Council of the
European Union

Brussels, 7 December 2023
(OR. en)

16048/1/23
REV 1

Interinstitutional File:
2022/0140(COD)

SAN 703
PHARM 161
COMPET 1179
MI 1049
DATAPROTECT 335
CODEC 2285
IA 331

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
No. Cion doc.:	8751/22 + ADD 1 - ADD 7
Subject:	Proposal for a Regulation on the European Health Data Space *- Mandate for negotiations with the European Parliament*

Delegations will find in Annex the revised Presidency compromise text proposed with a view to obtain a mandate for negotiations with the European Parliament on the above-mentioned proposal.

Changes compared to the Commission proposal are marked in ***bold/underline/italics*** for additions and in ~~strikethrough~~ for deletions.

ANNEX

2022/0140 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the European Health Data Space

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The aim of this Regulation is to establish the European Health Data Space ('EHDS') in order to improve access to and control by natural persons over their personal electronic health data in the context of healthcare (primary use of electronic health data), as well as for other purposes that would benefit the society such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities

[1] OJ C , , p. .
[2] OJ C , , p. .

(secondary use of electronic health data). In addition, the goal is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of electronic health record systems ('EHR systems') in conformity with Union values.

(2) The COVID-19 pandemic has highlighted the imperative of having timely access to electronic health data for health threats preparedness and response, as well as for diagnosis and treatment and secondary use of health data. Such timely access would have contributed, through efficient public health surveillance and monitoring, to a more effective management of the pandemic, and ultimately would have helped to save lives. In 2020, the Commission urgently adapted its Clinical Patient Management System, established by Commission Implementing Decision (EU) 2019/1269[3], to allow Member States to share electronic health data of COVID-19 patients moving between healthcare providers and Member States during the peak of the pandemic, but this was only an emergency solution, showing the need for a structural approach at Member States and Union level.

(3) The COVID-19 crisis strongly anchored the work of the eHealth Network, a voluntary network of digital health authorities, as the main pillar for the development of mobile contact tracing and warning applications and the technical aspects of the EU Digital COVID Certificates. It also highlighted the need for sharing electronic health data that are findable, accessible, interoperable and reusable ('FAIR principles'), and ensuring that electronic health data are as open as possible and as closed as necessary. Synergies between the EHDS, the European Open Science Cloud[4] and the European Research Infrastructures should be ensured, as well as lessons learned from data sharing solutions developed under the European COVID-19 Data Platform.

---

[3] Commission Implementing Decision (EU) 2019/1269 of 26 July 2019 amending Implementing Decision 2014/287/EU setting out criteria for establishing and evaluating European Reference Networks and their Members and for facilitating the exchange of information and expertise on establishing and evaluating such Networks (OJ L 200, 29.7.2019, p. 35).

[4] EOSC Portal (eosc-portal.eu).

(4) The processing of personal electronic health data is subject to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council[5] and, for Union institutions and bodies, Regulation (EU) 2018/1725 of the European Parliament and of the Council[6]. References to the provisions of Regulation (EU) 2016/679 should be understood also as references to the corresponding provisions of Regulation (EU) 2018/1725 for Union institutions and bodies, where relevant.

(5) More and more Europeans cross national borders to work, study, visit relatives or to travel. To facilitate the exchange of health data, and in line with the need for empowering citizens, they should be able to access their health data in an electronic format that can be recognised and accepted across the Union. Such personal electronic health data could include personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status, personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, as well as data determinants of health, such as behaviour, environmental, physical influences, medical care, social or educational factors. Electronic health data also includes data that has been initially collected for research, statistics, policy making or regulatory purposes and may be made available according to the rules in Chapter IV. The electronic health data concern all categories of those data, irrespective to the fact that such data is provided by the data subject or other natural or legal persons, such as health professionals, or is processed in relation to a natural person's health or well-being and should also include inferred and derived data, such as diagnostics, tests and medical examinations, as well as data observed and recorded by automatic means.

---

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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) (OJ L 119, 4.5.2016, p. 1).

6 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(5a) ***In health systems, personal electronic health data is usually gathered in electronic health records, which typically contain a natural person's medical history, diagnoses and treatment, medications, allergies, immunisations, as well as radiology images and laboratory results, spread between different entities from the health system (general practitioners, hospitals, pharmacies, care services). In order to enable that electronic health data be accessed, shared and changed by the natural persons or health professionals, some Member States have taken the necessary legal and technical measures and set up centralised infrastructures connecting EHR systems used by healthcare providers and natural persons. Alternatively, some Member States support public and private healthcare providers to set up personal health data spaces to enable interoperability between different healthcare providers. Several Member States have also supported or provided health data access services for patients and health professionals (for instance through patients or health professional portals). They have also taken measures to ensure the EHR systems or wellness applications are able to transmit electronic health data with the central EHR system (some Member States do this by ensuring, for instance, a system of certification). However, not all Member States have put in place such systems, and the Member States that have implemented them have done so in a fragmented manner. In order to facilitate the free movement of personal health data across the Union and avoid negative consequences for patients when receiving healthcare in cross-border context, Union action is needed in order to ensure individuals have improved access to their own personal electronic health data and are empowered to share it.***

(6) Chapter III of Regulation (EU) 2016/679 sets out specific provisions concerning the rights of natural persons in relation to the processing of their personal data. ***The*** EHDS builds upon these rights and ~~further develops~~ ***complements*** some of them~~. The EHDS should support the coherent implementation of those rights~~ as applied to ***personal*** electronic health data~~.~~ ***These rights apply*** regardless of the Member State in which the personal electronic health data are processed, type of healthcare provider, sources of data or Member State of affiliation of the natural person. The rights and rules related to the primary use of personal electronic health data under Chapter II and III of this Regulation concern all categories of those data, irrespective of how they have been collected or who has provided ~~hem~~ ***them***, of the legal ground for the processing under Regulation (EU) 2016/679 or the status of the controller as a public or private organisation***. The enhanced***

rights of access and portability of personal electronic health data should be without prejudice to the rights of access and portability as established under Regulation (EU) 2016/679. Natural persons continue to have those rights under the conditions set out in that regulation ~~of the legal ground for their processing~~.

(7) In health systems, personal electronic health data is usually gathered in electronic health records, which typically contain a natural person's medical history, diagnoses and treatment, medications, allergies, immunisations, as well as radiology images and laboratory results, spread between different entities from the health system (general practitioners, hospitals, pharmacies, care services). In order to enable that electronic health data to be accessed, shared and changed by the natural persons or health professionals, some Member States have taken the necessary legal and technical measures and set up centralised infrastructures connecting EHR systems used by healthcare providers and natural persons. Alternatively, some Member States support public and private healthcare providers to set up personal health data spaces to enable interoperability between different healthcare providers. Several Member States have also supported or provided health data access services for patients and health professionals (for instance through patients or health professional portals). They have also taken measures to ensure that EHR systems or wellness applications are able to transmit electronic health data with the central EHR system (some Member States do this by ensuring, for instance, a system of certification). However, not all Member States have put in place such systems, and the Member States that have implemented them have done so in a fragmented manner. In order to facilitate the free movement of personal health data across the Union and avoid negative consequences for patients when receiving healthcare in cross-border context, Union action is needed in order to ensure individuals have improved ac**c**ess to their own personal electronic health data and are empowered to share it.

(8) The right of access to data by a natural person, established by Article 15 of Regulation (EU) 2016/679, should be further ~~developed~~ ***complemented*** in the health sector. Under Regulation (EU) 2016/679, controllers do not have to provide access immediately. While patient portals, mobile applications and other personal health data access services exist in many places, including national solutions in some Member States, the right of access to health data is still commonly implemented in many places through the provision of the requested health data in paper format or as scanned documents, which is time-consuming~~.~~ ~~This may severely impair timely~~ ***for the controller, such as a hospital or other healthcare***

provider providing access. This slows down access to health data by natural persons, and may have a negative impact on natural persons ***if they*** ~~who~~ need such access immediately due to urgent circumstances pertaining to their health condition. ***For that reason, it is necessary to provide a more efficient way for natural persons to access their own personal electronic health data. They should have the right to have free of charge, immediate access, adhering to technological practicability, to certain defined priority categories of personal electronic health data, such as the patient summary, through an electronic health data access service. The scope of this complementary right established under this Regulation and the conditions for exercising it differ in certain ways from the right of access under Article 15 of Regulation (EU) 2016/679. The latter covers all personal data held by a controller and is exercised against an individual controller, which then has up to a month to reply to a request. The right to access personal electronic health data under this Regulation is limited to the categories of data falling within its scope, is exercised via an electronic health data access service, and provides an immediate answer.***

(9) At the same time, it should be considered that immediate access to certain types of personal electronic health data may be harmful for the safety of natural persons~~,~~ ***or*** unethical ~~or inappropriate~~. For example, it could be unethical to inform a patient through an electronic channel about a diagnosis with an incurable disease that is likely to lead to their swift passing instead of providing this information in a consultation with the patient first. Therefore, ~~a possibility for limited exceptions in the implementation~~ ***it should be possible to delay the provision*** of this ~~right should be ensured. Such an exception may be imposed by the~~ ***access in such situations for a limited amount of time.*** Member States ~~where this~~ ***should be able to define such an*** exception ***where it*** constitutes a necessary and proportionate measure in a democratic society, in line with the requirements of Article 23 of Regulation (EU) 2016/679. ~~Such restrictions should be implemented by delaying the display of the concerned personal electronic health data to the natural person for a limited period.~~ Where health data is only available on paper, if the effort to make data available electronically is disproportionate, there should be no obligation that such health data is converted into electronic format by Member States. Any digital transformation in the healthcare sector should aim to be inclusive and benefit also natural persons with limited ability to access and use digital services. ~~Natural persons should be able to provide an authorisation to the natural persons of their choice, such as to their relatives or other close~~

~~natural persons, enabling them to access or control access to their personal electronic health data or to use digital health services on their behalf. Such authorisations may also be useful for convenience reasons in other situations. Proxy services should be established by Member States to implement these authorisations, and they should be linked to personal health data access services, such as patient portals on patient-facing mobile applications. The proxy services should also enable guardians to act on behalf of their dependent children; in such situations, authorisations could be automatic. In order to take into account cases in which the display of some personal electronic health data of minors to their guardians could be contrary to the interests or will of the minor, Member States should be able to provide for such limitations and safeguards in national law, as well as the necessary technical implementation. Personal health data access services, such as patient portals or mobile applications, should make use of such authorisations and thus enable authorised natural persons to access personal electronic health data falling within the remit of the authorisation, in order for them to produce the desired effect.~~

(10) Some Member States allow natural persons to add electronic health data to their EHRs or to store additional information in their separate personal health record that can be accessed by health professionals***, to complement the information available to them***. However, this is not a common practice in all Member States and therefore should be ***left to Member States***. ~~established by the EHDS across the EU~~. Information inserted by natural persons may not be as reliable as electronic health data entered and verified by health professionals***. T***therefore, ***where Member States provide for this right,*** it should be clearly ***distinguishable from data provided by health professionals. This possibility for*** ~~marked to indicate the source of such additional data. Enabling~~ natural persons to ~~more easily and quickly access their~~ ***add and complement personal*** electronic health data ~~also further enables~~ ***should not entitle*** them to ~~notice possible errors such as incorrect information or incorrectly attributed patient records and have them rectified using their rights under Regulation (EU) 2016/679. In such cases, natural person should be enabled to request rectification of the incorrect~~ ***change personal*** electronic health data ~~online, immediately and free of charge, for example through the personal health data access service. Data rectification requests should be assessed and, where relevant, implemented by the data controllers on case by case basis, if necessary involving~~ ***provided by*** health professionals.

(10a) Enabling natural persons to more easily and quickly access their personal electronic health data also further enables them to notice possible errors such as incorrect

information or incorrectly attributed patient records. In such cases, natural persons should be enabled to request rectification of the incorrect electronic health data online, immediately and free of charge, for example through a personal health data access service. Such rectification requests should then be treated by the relevant data controllers in line with Regulation (EU) 2016/679. In this situation, the health data access service forwards the request for rectification under Regulation (EU) 2016/679 to the competent controller. This facilitates the exercise of this right for the natural person, who can submit requests through the health data access service instead of contacting controllers individually. It also helps the controller, who will receive assurance that the requester is in fact the data subject, as the requester will be reliably identified and authenticated by the health data access service. To further facilitate the exercise of existing data subject rights under Regulation (EU) 2016/679, Member States may also provide possibilities to submit requests to exercise them through their health data access services, complementing the possibility to contact the controller directly.

(11) Natural persons should be further empowered to exchange and to provide access to personal electronic health data to the health professionals of their choice, going beyond ***and complementing*** the right to data portability as established in Article 20 of Regulation (EU) 2016/679. ~~This is necessary to tackle objective difficulties and obstacles in the current state of play.~~ Under Regulation (EU) 2016/679, portability is limited only to data processed based on consent or contract~~,~~ which ~~excludes data processed under other legal bases, such as when the processing is based on law, for example when their processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It only concerns data~~ ***were*** provided by the data subject to a controller~~, excluding many inferred or indirect data, such as diagnoses, or tests~~. Finally, under Regulation (EU) 2016/679, the natural person has the right to have the personal data transmitted directly from one controller to another only where technically feasible. That Regulation, however, does not impose an obligation to make this direct transmission technically feasible. ~~All these elements limit the data portability and may limit its benefits for provision of high-quality, safe and efficient healthcare services to the natural person.~~

(12) ~~Natural persons should be able to exercise control over the transmission of personal electronic health data to other healthcare providers. Healthcare providers and other organisations providing EHRs should facilitate the exercise of this right. Stakeholders such~~

~~as healthcare providers, digital health service providers, manufacturers of EHR systems or medical devices should not limit or block the exercise of the right of portability because of the use of proprietary standards or other measures taken to limit the portability.~~ For these reasons, the framework laid down by this Regulation ~~builds on~~ ***extends*** the right to data portability established in Regulation (EU) 2016/679 by ensuring that natural persons as data subjects can transmit their electronic health data, including inferred data ***in the European electronic health record exchange format***, irrespective of the legal basis for processing the electronic health data. ***Health professionals*** ~~This right~~ should ~~apply to electronic health data processed by public or private controllers, irrespective of the legal basis for processing the data under in accordance with the Regulation (EU) 2016/679. This right should apply to all~~ ***refrain from hindering the implementation of the rights of natural persons, such as refusing to take into account electronic health data originating from another Member State and provided in the interoperable and reliable European*** electronic health ~~data~~ ***record exchange format***.

(12a) Moreover, the access to personal health records should be transparent to natural persons. The health data access services should provide detailed information on accesses to data, such as when and which healthcare providers or other individuals accessed which data. To ensure uniform implementation, the Commission should be empowered to lay down detailed elements in an implementing act.

(13) Natural persons may not want to allow access to some parts of their personal electronic health data while enabling access to other parts. Such selective sharing of personal electronic health data should be supported. However, such restrictions may have life threatening consequences and, therefore, access to personal electronic health data should be possible to protect vital interests as an emergency override. According to Regulation (EU) 2016/679, vital interests refer to situations in which it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal electronic health data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. More specific legal provisions on the mechanisms of restrictions placed by the natural person on parts of their personal electronic health data ~~should~~ ***may*** be provided by Member States in national law. ***In particular, this right may be restricted in a justified and proportionate manner, for purposes such as the preservation of public health in the case of highly contagious and hazardous diseases.*** Because the

unavailability of the restricted personal electronic health data may impact the provision or quality of health services provided to the natural person, ~~he/she~~ ***they*** should assume responsibility for the fact that the healthcare provider cannot take the data into account when providing health services.

(13a) ***In addition, due to the different sensitivities in the Member States on the degree of patients' control over their health data, Member States should be able to provide for an absolute right to object without an emergency override, both for cross-border access and for access internal to that Member State. If they choose to do so, they should establish the rules and specific safeguards regarding such mechanisms.*** **Such rules and specific safeguards may also relate to specific categories of personal electronic health data, for example genetic data**. ***Such a right to object means that personal electronic health data relating to the persons who made use of it would not be made available through the services set up under the EHDS beyond the healthcare provider that provided the treatment. If a natural person has exercised this right to object, healthcare providers will still document treatment provided in accordance with the applicable rules, and will be able to access the data registered by them. Natural persons who made use of such a right to object should be able to reverse their decision. Should they do so, personal electronic health data generated during the period of the objection might not be available via the access services and MyHealth@EU.***

~~(14) In the context of the EHDS, natural persons should be able to exercise their rights as they are enshrined in Regulation (EU) 2016/679. The supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679 should remain competent, in particular to monitor the processing of personal electronic health data and to address any complaints lodged by the natural persons. In order to carry out their tasks in the health sector and uphold the natural persons' rights, digital health authorities should cooperate with the supervisory authorities under Regulation (EU) 2016/679.~~

(15) ~~Article 9(2), point (h), of Regulation (EU) 2016/679 provides for exceptions where the processing of senstitive data is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee,~~***Timely and full access of health professionals to the medical records of patients is fundamental for ensuring continuity of care and avoiding duplications and errors. However, due to a lack of interoperability, in many cases, health professionals cannot access the complete medical records of their patients and cannot make optimal*** medical ***decisions for their*** diagnosis ***and treatment, which adds considerable costs for both health systems and natural persons and may lead to worse***~~, the provision of~~ health ~~care or treatment or the management of~~ ***outcomes for natural persons. Electronic health data made available in interoperable format, which can be transmitted between healthcare providers can also reduce the administrative burden on health professionals of manually entering or copying*** health ~~care~~***data between electronic*** systems***. Therefore, health professionals should be provided with appropriate electronic means, such as health professional portals or other health professional access*** ~~and~~ services***, to use personal electronic health data for the exercise of their duties. Providing this service to health professionals is a task in the public interest assigned by*** ~~on the basis of Union or Member State law.~~ this Regulation ~~should provide~~ ***whose performance requires the processing of personal data in the sense of Article 6(1)(e) of Regulation (EU) 2016/679. This Regulation provides*** conditions and safeguards for the processing of electronic health data ~~by healthcare providers and health professionals~~ ***in the health professional access service*** in line with Article 9(2), point (h)~~,~~ of Regulation (EU) 2016/679***, such as detailed provisions on logging to provide transparency towards data subjects*** ~~with the purpose of accessing personal electronic health data provided by the natural person or transmitted from other healthcare providers.~~ ***.*** However, this Regulation should be without prejudice to the national laws concerning the processing of health data ***for the delivery of healthcare***, including the legislation establishing categories of health professionals that can process different categories of electronic health data.

(15aa) In accordance with the general principles of European Union law, which include the fundamental rights guaranteed by Articles 7 and 8 of the Charter, a particular high level of protection and security should be ensured when processing personal electronic health data for primary use, by means of appropriate technical and organisational measures. In this respect, this Regulation is without prejudice to a requirement under national law,

with regards to the national context, according to which, where personal electronic health data are processed by healthcare providers for the provision of healthcare or by the national contact point for digital health connected to MyHealth@EU, the storage of personal electronic health data referred to in Article 5 for the purpose of primary use is located within the European Union in line with Union law and international commitments.

(15a) In order to facilitate the exercise of the complementary access and portability rights established under this Regulation, Member States should establish one or more electronic health data access services. These services may be provided as an online patient portal, via a mobile application or other means. They should be designed in an accessible way, including for persons with disabilities. Proving such a service to enable natural persons with easy access to their personal electronic health data is a substantial public interest. The processing of personal electronic health data in these services is necessary for the performance of that task assigned by this Regulation in the sense of Articles 6(1)(e) and 9(2) of Regulation (EU) 2016/679.

(15b) Natural persons should be able to provide an authorisation to the natural persons of their choice, such as to their relatives or other close natural persons, enabling them to access or control access to their personal electronic health data or to use digital health services on their behalf. Such authorisations may also be useful for convenience reasons in other situations. Proxy services for enabling such authorisations should be established by Member States to implement these authorisations, and they should be linked to personal health data access services, such as patient portals or patient-facing mobile applications. The proxy services should also enable guardians to act on behalf of their dependent children; in such situations, authorisations could be automatic. In order to take into account cases in which the display of some personal electronic health data of minors to their guardians could be contrary to the interests or the will of the minor, Member States should be able to provide for such limitations and safeguards in national law, as well as the necessary technical implementation. Personal health data access services, such as patient portals or mobile applications, should make use of such authorisations and thus enable authorised natural persons to access personal electronic health data falling within the remit of the authorisation, in order for them to produce the desired effect. Digital proxy solutions should be aligned with Regulation […] [eID regulation COM/2021/281 final] and the technical specifications of the European

Digital Identity Wallet to ensure a horizontal solution with increased user-friendliness. This should contribute to reduce both administrative and financial burdens for Member States by lowering the risk of developing parallel systems that are not interoperable across the Union.

(15c) ***In some Member States, health care is provided by primary care management teams, defined as groups of healthcare professionals centred on primary care (general practitioners), who carry out their primary care activities based on a healthcare plan drawn up by them. Also, other types of healthcare teams exist in several Member States for other care purposes. In the context of primary use of health data in the European Health Data Space, access should be provided to the healthcare professional of such teams.***

~~(16) Timely and full access of health professionals to the medical records of patients is fundamental for ensuring continuity of care and avoiding duplications and errors. However, due to a lack of interoperability, in many cases, health professionals cannot access the complete medical records of their patients and cannot make optimal medical decisions for their diagnosis and treatment, which adds considerable costs for both health systems and natural persons and may lead to worse health outcomes for natural persons. Electronic health data made available in interoperable format, which can be transmitted between healthcare providers can also reduce the administrative burden on health professionals of manually entering or copying health data between electronic systems. Therefore, health professionals should be provided with appropriate electronic means, such as health professional portals, to use personal electronic health data for the exercise of their duties. Moreover, the access to personal health records should be transparent to the natural persons and natural persons should be able to exercise full control over such access, including by limiting access to all or part of the personal electronic health data in their records. Health professionals should refrain from hindering the implementation of the rights of natural persons, such as refusing to take into account electronic health data originating from another Member State and provided in the interoperable and reliable European electronic health record exchange format.~~

(16a) ***The supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679 are competent for the monitoring and enforcement of that Regulation, in particular to monitor the processing of personal electronic health data and to address any complaints lodged by the natural persons. This notably includes the forwarding of complaints that falls within the other authorities' competences. The EHDS establishes additional rights for natural persons in primary use, going beyond the access and portability rights enshrined in Regulation (EU) 2016/679, complementing those rights. These additional rights should also be enforced by the supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679. Digital health authorities should cooperate with the supervisory authorities established pursuant to Regulation (EU) 2016/679. The supervisory authority or authorities responsible for monitoring and enforcement of the processing of personal electronic health data for primary use in compliance with the regulation should be competent to impose administrative fines. The legal system of Denmark and Ireland does not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark and Ireland the fines are imposed by the competent national courts as a criminal penalty, provided that such an application of the rules has an equivalent effect to administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive.***

(16b) ***Recognising the importance of ethical principles and the principle of doctor-patient confidentiality, Member States should strive to adhere to ethical principles and to respect the principle of doctor-patient confidentiality in the application of this Regulation. In particular, the European ethical principles for digital health provide guidance to practitioners, researchers, innovators, policy-makers and regulators at Union and Member State level for the application of the Regulation. The possibilities offered by the Regulation in terms of, inter alia, the promotion of better diagnosis, treatment and well-being of natural persons, should be attained without prejudice to the observance of ethical imperatives and the principle of doctor-patient confidentiality.***

(16c) ***The processing of health data for the purpose of law enforcement should not fall within the scope of primary or secondary use of electronic health data in the meaning of this Regulation.***

(17) The relevance of different categories of electronic health data for different healthcare scenarios varies. Different categories have also achieved different levels of maturity in standardisation, and therefore the implementation of mechanisms for their exchange may be more or less complex depending on the category. Therefore, the improvement of interoperability and data sharing should be gradual and prioritisation of categories of electronic health data is needed. Categories of electronic health data such as patient summary, electronic prescription and dispensation, laboratory results and reports, hospital discharge reports, medical images and reports have been selected by the eHealth Network as most relevant for the majority of healthcare situations and should be considered as priority categories for Member States to implement access to them and their transmission. When further needs for the exchange of more categories of electronic health data are identified for healthcare purposes, the list of priority categories should be expanded. The Commission should be empowered to extend the list of priority categories, after analysing relevant aspects related to the necessity and possibility for the exchange of new datasets, such as their support by systems established nationally or regionally by the Member States. Particular attention should be given to the data exchange in border regions of neighbouring Member States where the provision of cross-border health services is more frequent and needs even quicker procedures than across the Union in general.

(18) Access and sharing of electronic health data should be enabled for all the data that exist in the EHR of a natural person, when technically feasible. However, some electronic health data may not be structured or coded, and the transmission between healthcare providers may be limited or only possible in formats that do not allow for translation (when data is shared cross-borders). In order to provide enough time to prepare for implementation, dates of deferred application should be determined to allow for achieving legal, organisational, semantic and technical readiness for the transmission of different categories of electronic health data. When need for the exchange of new categories of electronic health data is identified, related dates of application should be determined in order to allow for the implementation of this exchange.

(19) The level of availability of personal health and genetic data in an electronic format varies between Member States. The EHDS should make it easier for natural persons to have those data available in electronic format. This would also contribute to the achievement of the target of 100% of Union citizens having access to their electronic health records by 2030, as referred to in the Policy Programme “Path to the Digital Decade”. In order to make

electronic health data accessible and transmissible, such data should be accessed and transmitted in an interoperable common European electronic health record exchange format, at least for certain categories of electronic health data, such as patient summaries, electronic prescriptions and dispensations, medical images and image reports, laboratory results and discharge reports, subject to transition periods. Where personal electronic health data is made available to a healthcare provider or a pharmacy by a natural person, or is transmitted by another data controller in the European electronic health record exchange format, the electronic health data should be read and accepted for the provision of healthcare or for dispensation of a medicinal product, thus supporting the provision of the health care services or the dispensation of the electronic prescription. Commission Recommendation (EU) 2019/243[7] provides the foundations for such a common European electronic health record exchange format. The use of European electronic health record exchange format should become more generalised at EU and national level. While the eHealth Network under Article 14 of Directive 2011/24/EU of the European Parliament and of the Council[8] recommended Member States to use the European electronic health record exchange format in procurements, in order to improve interoperability, uptake was limited in practice, resulting in fragmented landscape and uneven access to and portability of electronic health data.

(20) While EHR systems are widely spread, the level of digitalisation of health data varies in Member States depending on data categories and on the coverage of healthcare providers that register health data in electronic format. In order to support the implementation of data subjects' rights of access to and exchange of electronic health data, Union action is needed to avoid further fragmentation. In order to contribute to a high quality and continuity of healthcare, certain categories of health data should be registered in electronic format systematically and according to specific data quality requirements. The European electronic health record exchange format should form the basis for specifications related to the registration and exchange of electronic health data. The Commission should be empowered to adopt implementing acts for determining additional aspects related to the registration of electronic health data, such as categories of healthcare providers that are to register health data electronically, categories of data to be registered electronically, or data

---

7 Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format (OJ L 39, 11.2.2019, p. 18).

8 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

quality requirements. ***The European electronic health record exchange format may have two profiles: a simple technical specification for use applicable to EHR systems and a detailed technical specification for cross-border use, which should only apply to the national contact points for MyHealth@EU. At the national level, the European electronic health record exchange format should include the technical specifications for the 'European interoperability component for EHR systems'. Also, harmonised technical specifications for the 'European logging component for EHR systems' should be defined by means of implementing acts. These two components are mainly focused on data transformation, although they may imply indirect requirements for data registry and data presentation in EHR systems at the national level. Given the purposes of these components and the wide scope of the definition of EHR systems in this Regulation, conformance assessment of the harmonised components should be by means of self-certification. The Commission should establish a testing environment to facilitate such self-certification. Member States should retain the competence to define requirements relating to any other components of EHR systems and the terms and conditions for connection of healthcare providers to their respective national infrastructures, which may be subject to third-party assessment at the national level. The cross-border specifications of the European electronic health record exchange format should be complemented by further cybersecurity, technical and semantic interoperability, operations and service management specifications for cross-border use in the MyHealth@EU infrastructure, defined by means of implementing acts.***

(21) Under Article 168 of the Treaty Member States are responsible for their health policy, in particular for decisions on the services (including telemedicine) that they provide and reimburse. Different reimbursement policies should, however, not constitute barriers to the free movement of digital health services such as telemedicine, including online pharmacy services. When digital services accompany the physical provision of a healthcare service, the digital service should be included in the overall care provision.

(22) Regulation (EU) No 910/2014 of the European Parliament and of the Council[9] lays down the conditions under which Members States perform identification of natural persons in cross-border situations using identification means issued by another Member State,

[9] Regulation (EU) No 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 (OJ L 257, 28.8.2014, p. 73).

establishing rules for the mutual recognition of such electronic identification means. The EHDS requires a secure access to electronic health data, including in cross-border scenarios where the health professional and the natural person are from different Member States, to avoid cases of unauthorised access. At the same time, the existence of different means of electronic identification should not be a barrier for exercising the rights of natural persons and health professionals. The rollout of interoperable, cross-border identification and authentication mechanisms for natural persons and health professionals across the EHDS requires strengthening cooperation at Union level in the European Health Data Space Board ('EHDS Board').~~As the rights of the natural persons in relation to the access and transmission of personal electronic health data should be implemented uniformly across the Union, a strong governance and coordination is necessary at both Union and Member State level. Member States should establish relevant digital health authorities for the planning and implementation of standards for electronic health data access, transmission and enforcement of rights of natural persons and health professionals. In addition, governance elements are needed in Member States to facilitate the participation of national actors in the cooperation at Union level, channelling expertise and advising the design of solutions necessary to achieve the goals of the EHDS. Digital health authorities exist in most of the Member States and they deal with EHRs, interoperability, security or standardisation. Digital health authorities should be established in all Member States, as separate organisations or as part of the currently existing authorities.~~

(22a) ***Natural persons should be provided with sufficient tools for exercising their rights related to the personal electronic health data. Member States should therefore ensure that electronic health data access services are made available for natural persons and their representatives. Such services may be implemented for instance through online portals or mobile applications, at national or regional level, or by healthcare providers. Electronic health data access services should implement the rights of natural persons regardless of their Member State of affiliation, and should therefore support the identification of natural persons using any electronic identification means recognised pursuant to Article 6 of Regulation (EU) No 910/2014. Considering the possibility of identity matching challenges in cross-border situations, supplementary access tokens or codes may need to be issued by Member States to natural persons who arrive from other Member States and receive healthcare. The Commission should be empowered to adopt implementing acts for the interoperable, cross-border identification and authentication***

of natural persons and health professionals, including any supplementary mechanisms that are necessary for ensuring the possibility for natural persons to exercise their rights to personal electronic health data in cross-border situations.

(22b) ***As the rights of the natural persons in relation to the access and transmission of personal electronic health data should be implemented uniformly across the Union, a strong governance and coordination is necessary at both Union and Member State level. Member States should establish relevant digital health authorities for the planning and implementation of standards for electronic health data access, transmission and enforcement of rights of natural persons and health professionals. In addition, governance elements are needed in Member States to facilitate the participation of national actors in the cooperation at Union level, channelling expertise and advising the design of solutions necessary to achieve the goals of the EHDS. Digital health authorities exist in most of the Member States and they deal with EHRs, interoperability, security or standardisation. Digital health authorities should be established in all Member States, as separate organisations or as part of the currently existing authorities.***

(23) Digital health authorities should have sufficient technical skills, possibly bringing together experts from different organisations. The activities of digital health authorities should be well-planned and monitored in order to ensure their efficiency. Digital health authorities should take necessary measures to ensuring rights of natural persons by setting up national, regional, and local technical solutions such as national EHR, patient portals, data intermediation systems. When doing so, they should apply common standards and specifications in such solutions, promote the application of the standards and specifications in procurements and use other innovative means including reimbursement of solutions that are compliant with interoperability and security requirements of the EHDS. To carry out their tasks, the digital health authorities should cooperate at national and Union level with other entities, including with insurance bodies, healthcare providers, manufacturers of EHR systems and wellness applications, as well as stakeholders from health or information technology sector, entities handling reimbursement schemes, health technology assessment bodies, medicinal products regulatory authorities and agencies, medical devices authorities, procurers and cybersecurity or e-ID authorities.

(24) Access to and transmission of electronic health data is relevant in cross-border healthcare situations, as it may support continuity of healthcare when natural persons travel to other

Member States or change their place of residence. Continuity of care and rapid access to personal electronic health data is even more important for residents in border regions, crossing the border frequently to get health care. In many border regions, some specialised health care services may be available closer across the border rather than in the same Member State. An infrastructure is needed for the transmission of personal electronic health data across borders, in situations where a natural person is using services of a healthcare provider established in another Member State. A voluntary infrastructure for that purpose, MyHealth@EU, has been established as part of the actions provided for in Article 14 of Directive 2011/24/EU. Through MyHealth@EU, Member States started to provide natural persons with the possibility to share their personal electronic health data with healthcare providers when travelling abroad. To further support such possibilities, the participation of Member States in the digital infrastructure MyHealth@EU should become mandatory. All Member States should join the infrastructure and connect healthcare providers ~~and~~ ***including*** pharmacies to it, as this is necessary for the implementation of the rights of natural persons ***established under this Regulation*** to access and make use of their personal electronic health data regardless of the Member State. The infrastructure should be gradually expanded to support further categories of electronic health data.

(25) ~~In the context of~~ MyHealth@EU~~, a central platform should provide~~ ***provides*** a common infrastructure for the Member States to ensure connectivity and interoperability in an efficient and secure way ***to support cross-border healthcare. The Commission should, as a processor on behalf of the Member States, provide this infrastructure***. In order to guarantee compliance with data protection rules and to provide a risk management framework for the transmission of personal electronic health data, ***specific responsibilities of the Member States, as controllers, and the*** ~~the~~ Commission***'s obligations*** should~~, by means of~~ ***be laid down in detail in*** implementing acts~~, allocate specific responsibilities among the Member States, as joint controllers, and prescribe its own obligations, as processor~~***. This Regulation provides the legal basis for the processing of personal electronic health data in this infrastructure as a task carried out in the public interest assigned by Union law in the sense of Article 6(1)(e) of Regulation (EU) 2016/679. This processing is necessary for the provision of healthcare, as mentioned in Article 9(2)(h) of that Regulation, in cross-border situations***.

(26) In addition to services in MyHealth@EU for the exchange of personal electronic health data based on the European electronic health record exchange format, other services or

supplementary infrastructures may be needed for example in cases of public health emergencies or where the architecture of MyHealth@EU is not suitable for the implementation of some use cases. Examples of such use cases include support for vaccination card functionalities, including the exchange of information on vaccination plans, or verification of vaccination certificates or other health-related certificates. This would be also important for introducing additional functionality for handling public health crises, such as support for contact tracing for the purposes of containing infectious diseases. Connection of national contact points for digital health of third countries or interoperability with digital systems established at international level should be subject to a check ensuring the compliance of the national contact point with the technical specifications, data protection rules and other requirements of MyHealth@EU. A decision to connect a national contact point of a third country should be taken by data controllers in the joint controllership group for MyHealth@EU.

(27) In order to ~~ensure~~***enable seamless exchange of electronic health and contribute to ensuring*** respect for the rights of natural persons and health professionals, EHR systems marketed in the ~~internal~~***Single*** Market of the Union should be able to store and transmit, in a secure way, high quality electronic health data. ~~This~~***It*** is a key ~~principle~~***objective*** of the EHDS to ensure the secure and free movement of electronic health data across the Union. To that end, a mandatory ~~self-certification scheme~~***scheme of self-conformity assessment*** for EHR systems processing one or more priority categories of electronic health data should be established to overcome market fragmentation while ensuring a proportionate approach. Through this ~~self-certification~~ ***self-assessment***, EHR systems ~~should~~ ***will*** prove compliance with ~~essential~~ ***the*** requirements~~-~~ on interoperability***, security and logging for communication of personal electronic health data established by the two mandatory EHR components harmonised by this Regulation, namely the 'European EHR systems exchange interoperability component' and the 'European logging component for EHR systems'*** ~~and security, set at Union level~~. In relation to security ***of those components, these***~~,~~ ~~essential~~ requirements should cover elements specific to EHR systems, as more general security properties should be supported by other mechanisms such as ~~cybersecurity schemes under~~ Regulation ~~(EU)~~ 2019/881 ~~of the European Parliament and of the Council~~[10]***[…]… [Cyber-Resilience Act COM/2022/454 final]***.

[10] ~~Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and~~

(28) While EHR systems specifically intended by the manufacturer to be used for processing one or more specific categories of electronic health data should be subject to mandatory self-certification, software for general purposes should not be considered as EHR systems, even when used in a healthcare setting, and should therefore not be required to comply with the provisions of Chapter III.

(28a) This Regulation imposes a mandatory self-conformity assessment scheme for the two mandatory harmonised EHR components of EHR systems, to ensure that EHR systems placed on the Union market are able to exchange data in the European electronic health record exchange format and that they have the required logging capabilities. The declaration of conformity by the manufacturer is justified by ensuring that these requirements are guaranteed in a proportionate way, without imposing an undue burden on Member States and manufacturers.

(28b) In order to promote the smooth functioning of the internal market for electronic health data, digital health products and services, as much transparency as possible should be ensured as regards national regulations establishing requirements for EHR systems and provisions on their conformity assessment in relation to aspects other than the harmonised components of EHR systems under the regulation. It is essential for the Commission to have the necessary information regarding those national requirements in order to ensure that they do not impede or adversely interact with the harmonised components of EHR systems.

(29) Software or module(s) of software which falls within the definition of a medical device, ***in vitro diagnostic medical devices*** or high-risk artificial intelligence (AI) system should be certified in accordance with Regulation (EU) 2017/745, ***Regulation (EU) 2017/746*** ~~of the European Parliament and of the Council~~[11] and Regulation […] of the European Parliament and of the Council [AI Act COM/2021/206 final], as applicable. The essential requirements on interoperability of this Regulation should only apply to the extent that the manufacturer of a medical device***, in vitro diagnostic medical devices,*** or high-risk AI

~~communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).~~

[11] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 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 (OJ L 117, 5.5.2017, p. 1).

system, which is providing electronic health data to be processed as part of the EHR system, claims interoperability with such EHR system. In such case, the provisions on common specifications for EHR systems should be applicable to those medical devices***, in vitro diagnostic medical devices*** and high-risk AI systems.

(30) To further support interoperability and security, Member States may maintain or define specific rules for the procurement, reimbursement, financing or use of EHR systems at national level in the context of the organisation, delivery or financing of health services. Such specific rules should not impede the free movement of EHR systems in the Union. Some Member States have introduced mandatory certification of EHR systems or mandatory interoperability testing for their connection to national digital health services. Such requirements are commonly reflected in procurements organised by healthcare providers, national or regional authorities. Mandatory certification of EHR systems at Union level should establish a baseline that can be used in procurements at national level.

(31) In order to guarantee effective exercise by patients of their rights under this Regulation, where healthcare providers develop and use an EHR system 'in house' to carry out internal activities without placing it on the market in return of payment or remuneration, they should also comply with this Regulation. In that context, such healthcare providers should comply with all requirements applicable to the manufacturers ***for such 'in house'-developed system that they put into service. However, such healthcare providers may need additional time to prepare. For that reason, these requirements should only apply to such systems after an extended transition period.***

(32) It is necessary to provide for a clear and proportionate division of obligations corresponding to the role of each operator in the supply and distribution process of EHR systems. Economic operators should be responsible for compliance in relation to their respective roles in such process and should ensure that they make available on the market only EHR systems which comply with relevant requirements.

(33) Compliance with essential requirements on interoperability and security should be demonstrated by the manufacturers of EHR systems through the implementation of common specifications. To that end, implementing powers should be conferred on the Commission to determine such common specifications regarding datasets, coding systems, technical specifications, including standards, specifications and profiles for data exchange,

as well as requirements and principles related to security, confidentiality, integrity, patient safety and protection of personal data as well as specifications and requirements related to identification management and the use of electronic identification. Digital health authorities should contribute to the development of such common specifications.

(34) In order to ensure an appropriate and effective enforcement of the requirements and obligations laid down in Chapter III of this Regulation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply. Depending on the organisation defined at national level, such market surveillance activities could be carried out by the digital health authorities ensuring the proper implementation of Chapter II or a separate market surveillance authority responsible for EHR systems. While designating digital health authorities as market surveillance authorities could have important practical advantages for the implementation of health and care, any conflicts of interest should be avoided, for instance by separating different tasks.

(35) Users of wellness applications, such as mobile applications, should be informed about the capacity of such applications to be connected and to supply data to EHR systems or to national electronic health solutions, in cases where data produced by wellness applications is useful for healthcare purposes. The capability of those applications to export data in an interoperable format is also relevant for data portability purposes. Where applicable, users should be informed about the compliance of such applications with interoperability and security requirements. However, given the large number of wellness applications and the limited relevance for healthcare purposes of the data produced by many of them, a certification scheme for these applications would not be proportionate. A voluntary labelling scheme should therefore be established as an appropriate mechanism for enabling the transparency for the users of wellness applications regarding compliance with the requirements, thereby supporting users in their choice of appropriate wellness applications with high standards of interoperability and security. The Commission may set out in implementing acts the details regarding the format and content of such label.

(35a) ***Member States should remain free to regulate the use of wellness applications as referred to in Article 31 in the context of the provision of healthcare, provided that such rules are in compliance with Union law.***

(36) The distribution of information on certified EHR systems and labelled wellness applications is necessary to enable procurers and users of such products to find interoperable solutions for their specific needs. A database of interoperable EHR systems and wellness applications, which are not falling within the scope of Regulations (EU) 2017/745 and […] [AI act COM/2021/206 final] should therefore be established at Union level, similar to the European database on medical devices (Eudamed) established by Regulation (EU) 2017/745. The objectives of the EU database of interoperable EHR systems and wellness applications should be to enhance overall transparency, to avoid multiple reporting requirements and to streamline and facilitate the flow of information. For medical devices and AI systems, the registration should be maintained under the existing databases established respectively under Regulations (EU) 2017/745 and […] [AI act COM/2021/206 final], but the compliance with interoperability requirements should be indicated when claimed by manufacturers, to provide information to procurers.

(37) ***Without hindering or replacing contractual or other voluntary mechanisms in place, this Regulation is aimed at establishing a common mechanism to access electronic health data for secondary use, which makes it mandatory for data holders to make the data they hold available on the basis of a data permit or a data request.*** For the secondary use of ~~the clinical~~ ***electronic health*** data for research, innovation, policy making, regulatory purposes, patient safety or the treatment of other natural persons, the possibilities offered by ~~Regulation~~***Regulations*** (EU) 2016/679 ~~for a~~ ***and (EU) 2018/1725 for*** Union ~~law~~***laws*** should be used as a basis ~~and rules and mechanisms and providing~~***for the processing as well as*** suitable and specific measures to safeguard the rights and freedoms of ~~the~~ natural persons. This Regulation provides ~~the~~***a*** legal basis in accordance with ***Regulation (EU) 2016/679 and (EU) 2018/1725 for the secondary use of personal electronic health data including the safeguards to permit the processing of special categories of data, in accordance with*** Articles 9(2) (g), (h), (i) and (j) of Regulation (EU) 2016/679 ***and Articles 10(2) (g), (h), (i) and (j) of (EU) 2018/1725***, ~~for the secondary use of health data, establishing~~ the ~~safeguards for processing~~, in terms of lawful purposes, trusted governance for providing access to health data (through health data access bodies) and processing in a secure environment, as well as ***the*** modalities for data processing, set out in the data permit. ***Consequently, Member States may no longer maintain or introduce under Article 9(4) of Regulation (EU) 2016/679 further conditions, including limitations and specific provisions requesting the consent of natural persons, with regard to the***

processing for secondary use of personal electronic health data under this Regulation. At the same time~~, the data applicant~~ ***data applicants*** should demonstrate a legal basis pursuant to Article 6 of Regulation (EU) 2016/679 ***or Article 5 of Regulation (EU) 2018/1725, where applicable***, based on which they could request access to ***electronic health*** data pursuant to this Regulation and should fulfil the conditions set out in Chapter IV. More specifically~~:~~ ***,*** for processing of electronic health data held by the ~~data holder pursuant to this Regulation,~~***health data holders*** this Regulation creates the legal obligation in the sense of Article 6(1) point (c) of Regulation (EU) 2016/679***, in accordance with Article 9(2)(i) and (j) of the same Regulation for making available the personal electronic health*** ~~for disclosing the~~ data by the ***health*** data holder to health data access bodies, while the legal basis for the purpose of the initial processing (e.g. ***providing*** delivery of ~~care~~***healthcare***) is unaffected. This Regulation also ~~meets the conditions for such processing pursuant to Articles 9(2) (h),(i),(j) of the Regulation (EU) 2016/679. This Regulation~~ assigns tasks in the public interest ~~to the health data access bodies (running the secure processing environment, processing data before they are used, etc.)~~ in the sense of Article 6(1)(e) of Regulation (EU) 2016/679 to the health data access bodies, and meets the requirements of Article 9(2)(h),(i),(j) of the Regulation (EU) 2016/679~~. Therefore, in this case, this Regulation provides the legal basis under Article 6 and meets the requirements of Article 9 of that Regulation~~ ***for the health data access body's processing of personal electronic health data when the body is fulfilling its tasks of gathering, combining, preparing, including pseudonymisation and anonymisation of the data, and makes those data available to the health data user for secondary use*** on the ~~conditions under which electronic health data can be processed~~ ***basis of a data permit or a data request***. In the case where the ***health data*** user has access to ***personal*** electronic health data (for secondary use of data for one of the purposes defined in this Regulation), the ***health*** data user should demonstrate its legal basis pursuant to Articles 6(1), points (e) or (f), of Regulation (EU) 2016/679 ***or pursuant to Article 5(1), point (a) of Regulation (EU) 2018/1725*** and explain the specific legal basis on which it relies as part of the application for access to electronic health data pursuant to this Regulation.: ~~on the basis of the applicable legislation, where the legal basis under Regulation (EU) 2016/679 is Article 6(1), point (e), or on~~***. If the health data user relies upon a legal basis offered by*** Article 6(1), point ~~(f),~~***(e)*** of Regulation (EU) 2016/679~~. If the user relies upon a legal basis offered by Article 6(1), point (e)~~ ***or Article 5(1), point (a) of Regulation (EU) 2018/1725***, it should make reference to another ~~EU~~***Union*** or national law, different from this Regulation, mandating the ***health***

data user to process personal health data for the compliance of its tasks. If the lawful ground for processing by the ***health data*** user is Article 6(1), point (f), of Regulation (EU) 2016/679, in this case it is this Regulation that provides the safeguards. In this context, the data permits issued by the health data access bodies are an administrative decision defining the conditions for the access to the data.

(37a) ***The secondary use of electronic health data can bring great societal benefits. To achieve this goal, it is important that data sets made available for secondary use by the present Regulation are as complete as possible. This Regulation provides the necessary safeguards to mitigate certain risks involved in the realisation of those benefits. The secondary use of electronic health data is based on pseudonymised or anonymised data, in order to preclude the identification of the data subjects. However, to balance the need of data users to have exhaustive and representative datasets with the autonomy of natural persons over data that are considered particularly sensitive, Member State should be able to allow natural persons to indicate that they do not wish for their personal electronic health data to be made available for secondary use pursuant to this Regulation. To do so, Member States may introduce a specific right to object from the processing of personal electronic health data for secondary use which complements the right to object set out by article 21 of Regulation (EU) 2016/679. It is appropriate to leave Member States free to decide to introduce and modulate such a right as it involves a balance between individual autonomy and the availability of health data for secondary use purposes, which is best made at national level, taking into account Member States' specific situations and historical experiences. Should a Member State choose to provide for such a right, it should also define how and where to exercise it and facilitate its exercise. This right can be implemented at the level of the health data holder that is subject to a legal obligation to make data available to the health data access body, at the level of the health data intermediary entity, or at the level of the health data access body, or at several levels. As such a right can affect the representativity of datasets, statistics providing sufficient information for data users shall be available at Member State level to assess the impact of the exercise of this right on the utility of the dataset. Where a Member State does not introduce a specific right to object in accordance with article 35F of this regulation, solely Article 21 of Regulation (EU) 2016/679 will apply.***

(38) In the context of the EHDS, the electronic health data already exists and is being collected by healthcare providers, professional associations, public institutions, regulators,

researchers, insurers etc. in the course of their activities. Some categories of data are collected primarily for the provisions of healthcare (e.g. electronic health records, genetic data, claims data, etc.), others are collected also for other purposes such as research, statistics, patient safety, regulatory activities or policy making (e.g. disease registries, policy making registries, registries concerning the side effects of medicinal products or medical devices, etc.). For instance, European databases that facilitate data (re)use are available in some areas, such as cancer (European Cancer Information System) or rare diseases (European Platform on Rare Disease Registration, ERN registries, etc.). These data should also be made available for secondary use. However, much of the existing health-related data is not made available for purposes other than that for which they were collected. This limits the ability of researchers, innovators, policy-makers, regulators and doctors to use those data for different purposes, including research, innovation, policy-making, regulatory purposes, patient safety or personalised medicine. In order to fully unleash the benefits of the secondary use of electronic health data, all data holders should contribute to this effort in making different categories of electronic health data they are holding available for secondary use.

(39) The categories of electronic health data that can be processed for secondary use should be broad and flexible enough to accommodate the evolving needs of data users, while remaining limited to data related to health or known to influence health. It can also include relevant data from the health system (electronic health records, claims data, disease registries, genomic data etc.), as well as data with an impact on health (for example consumption of different substances, homelessness, health insurance, minimum income, professional status, behaviour, including environmental factors (for example, pollution, radiation, use of certain chemical substances). They can also include person-generated data, such as data from medical devices, wellness applications or other wearables and digital health applications. The data user who benefits from access to datasets provided under this Regulation could enrich the data with various corrections, annotations and other improvements, for instance by supplementing missing or incomplete data, thus improving the accuracy, completeness or quality of data in the dataset. To support the improvement of the original database and further use of the enriched dataset, the dataset with such improvements and a description of the changes should be made available free of charge to the original data holder. The data holder should make available the new dataset, unless it provides a justified notification against it to the health data access body, for instance in

cases of low quality of the enrichment. Secondary use of non-personal electronic data should also be ensured. In particular, pathogen genomic data hold significant value for human health, as proven during the COVID-19 pandemic. Timely access to and sharing of such data has proven to be essential for the rapid development of detection tools, medical countermeasures and responses to public health threats. The greatest benefit from pathogen genomics effort will be achieved when public health and research processes share datasets and work mutually to inform and improve each other.

(39a) ***In order to increase the effectiveness of the secondary use of personal electronic health data, and to fully benefit from the possibilities offered by this Regulation in terms of, among others, health research, innovation, policy-making, and regulatory purposes, personal electronic health data for secondary use should be made available prioritising the datasets according to their usefulness, quality and readiness. This Regulation aims to ensure the availability in the EHDS of electronic health data described in Chapter IV that are accessible, ready and suitable for the purpose of creating scientific, innovative and societal value.***

(40) The data holders can be public, non for profit or private health or care providers, public, non for profit and private organisations, associations or other entities, public and private entities that carry out research with regards to the ~~health sector~~***healthcare or care sectors, entities developing products and services intended for the healthcare or care sectors and Union institutions, bodies, offices or agencies*** that process the categories of health and ~~health~~***healthcare data mentioned above, as well as mortality registries. Also included in the category of data holders are entities in the care sector such as nursing homes, day-care centres, entities providing services for people with disabilities, business and technological activities*** related ***to care such as orthopaedics and companies providing care services. Legal persons developing products and services intended for the healthcare or care sectors, and wellness applications should also be data holders. This consideration applies both if these entities or bodies are developing new products or services, or if they already have products on the market*** ~~data mentioned above~~. In order to avoid a disproportionate burden***, natural persons and*** ~~on small entities,~~ micro-enterprises are***, as a general rule,*** excluded from the ~~obligation to make their data available~~ ***obligations as data holders*** for secondary use in the framework of EHDS. ***Member States should, however, be able to extend the obligations of data holders to natural persons and micro-enterprises in their national legislation. Due to the diversity in the structure of***

healthcare systems of the Member States and the administrative burden the inclusion of the care sector may entail at the national level, it should be possible to exclude the care sector from the obligations of data holders by way of national legislation. In order to reduce the administrative burden, and in the light of the effectiveness and efficiency principles, Member States should be able to decide , by way of national legislation that for certain categories of data holders their duties as data holders are to be carried out by health data intermediation entities. The public or private entities often receive public funding, from national or Union funds to collect and process electronic health data for research, statistics (official or not) or other similar purposes, including in ~~area~~ ***areas*** where the collection of such data is fragmented of difficult, such as rare diseases, cancer etc. Such data, collected and processed by data holders with the support of Union or national public funding, should be made available by data holders to health data access bodies, in order to maximise the impact of the public investment and support research, innovation, patient safety or policy making benefitting the society. In some Member States, private entities, including private healthcare providers and professional associations, play a pivotal role in the health sector. The health data held by such providers should also be made available for secondary use. At the same time, data benefiting from specific legal protection such as intellectual property from medical device companies or pharmaceutical companies often enjoy copyright protection or similar types of protection. However, public authorities and regulators should have access to such data, for instance in the event of pandemics, to verify defective devices and protect human health. In times of severe public health concerns (for example, PIP breast implants fraud) it appeared very difficult for public authorities to get access to such data to understand the causes and knowledge of ~~manufacturer~~ ***manufacturers*** concerning the defects of some devices. The COVID-19 pandemic also revealed the difficulty for policy makers to have access to health data and other data related to health. Such data should be made available for public and regulatory activities, supporting public bodies to carry out their legal mandate, while complying with, where relevant and possible, the protection enjoyed by commercial data. Specific rules in relation to the secondary use of health data should be provided. Data altruism activities may be carried out by different entities, in the context of Regulation […] [Data Governance Act COM/2020/767 final] and taking into account the specificities of the health sector.

(40a) Electronic health data protected by intellectual property rights or trade secrets can be very useful for secondary use. While they should be made available to the extent

possible, however, this Regulation should not be used to reduce or circumvent such protection. It is for the Health Data Access Body to assess how to preserve this protection while also enabling access to such data for health data users to the extent possible. If it is unable to do so, it should inform the health data user and explain why it is not possible to provide access to such data. Legal, organisational and technical measures to preserve intellectual property rights or trade secrets could include common electronic health data access contractual arrangements, specific obligations in relation to such rights within the data permit, pre-processing the data to generate derived data that protects a trade secret but still has utility for the user or configuration of the secure processing environment so that such data is not accessible by the health data user.

(40b) Taking into account the specific purposes of the processing, data should be anonymised or pseudonymised as early as possible in the chain of making data available for secondary use. Pseudonymisation and anonymisation can be carried out by the health data access bodies or by the health data holders. As data controllers, health data access bodies and health data holders may delegate these tasks to data processors.

(41) The secondary use of health data under EHDS should enable the public, private, not for profit entities, as well as individual researchers to have access to health data for research, innovation, policy making, educational activities, patient safety, regulatory activities or personalised medicine, in line with the purposes set out in this Regulation. Access to data for secondary use should contribute to the general interest of the society. Activities for which access in the context of this Regulation is lawful may include using the electronic health data for tasks carried out by public bodies, such as exercise of public duty, including public health surveillance, planning and reporting duties, health policy making, ensuring patient safety, quality of care, and the sustainability of health care systems. Public bodies and Union institutions, bodies, offices and agencies may require to have regular access to electronic health data for an extended period of time, including in order to fulfil their mandate, which is provided by this Regulation. Public sector bodies may carry out such research activities by using third parties, including sub-contractors, as long as the public sector body remain at all ~~time~~***times*** the supervisor of these activities. The provision of the data should also support activities related to scientific research (including private research), development and innovation, producing goods and services for the health or care sectors, such as innovation activities or training of AI algorithms that could protect the health or care of natural persons. In some cases, the information of some natural persons (such as

genomic information of natural persons with a certain disease) could support the diagnosis or treatment of other natural persons. There is a need for public bodies to go beyond the emergency scope of Chapter V of Regulation […] [Data Act COM/2022/68 final]. However, the public sector bodies may request the support of health data access bodies for processing or linking data. This Regulation provides a channel for public sector bodies to obtain access to information that they require for fulfilling their tasks assigned to them by law, but does not extend the mandate of such public sector bodies. Any attempt to use the data for any measures detrimental to the natural person, to increase insurance premiums, to ***engage in activities potentially detrimental to the natural persons related to employment, pension and banking, including mortgaging of properties, to*** advertise products or treatments, or develop harmful products should be prohibited. ***This prohibition applies to the activities contrary to ethical provisions according to national law, with the exception of ethical provisions related to consent the right to object to the processing of personal data and the right to object, which in application of the general principle of primacy of Union law, this Regulation takes precedence over national law.***

(41a) ***This Regulation does not create an empowerment for the secondary use of health data for the purpose of law enforcement. The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties by competent authorities is not among the secondary use purposes covered under this Regulation. Therefore, courts and other entities of the justice system cannot be considered data users in the secondary use of health data under this Regulation. In addition, courts and other entities of the justice system are not covered under the definition of data holders, and are therefore not addressees of obligations on data holders under this Regulation.***

(42) The establishment of one or more health data access bodies, supporting access to electronic health data in Member States, is an essential component for promoting the secondary use of health-related data. Member States should therefore establish one or more health data access body, for instance to reflect their constitutional, organisational and administrative structure. However, one of these health data access bodies should be designated as a coordinator in case there are more than one data access body. Where a Member State establishes several bodies, it should lay down rules at national level to ensure the coordinated participation of those bodies in the EHDS Board. That Member State should in particular designate one health data access body to function as a single contact point for the effective participation of those bodies, and ensure swift and smooth cooperation with other

health data access bodies, the EHDS Board and the Commission. Health data access bodies may vary in terms of organisation and size (spanning from a dedicated full-fledged organization to a unit or department in an existing organization) but should have the same functions, responsibilities and capabilities. Health data access bodies should not be influenced in their decisions on access to electronic data for secondary use. However, their independence should not mean that the health data access body cannot be subject to control or monitoring mechanisms regarding its financial expenditure or to judicial review. Each health data access body should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of its tasks, including those related to cooperation with other health data access bodies throughout the Union. Each health data access body should have a separate, public annual budget, which may be part of the overall state or national budget. In order to enable better access to health data and complementing Article 7(3) of Regulation […] of the European Parliament and of the Council [Data Governance Act COM/2020/767 final], Member States should entrust health data access bodies with powers to take decisions on access to and secondary use of health data. This could consist in allocating new tasks to the competent bodies designated by Member States under Article 7(1) of Regulation […] [Data Governance Act COM/2020/767 final] or in designating existing or new sectoral bodies responsible for such tasks in relation to access to health data.

(43) The health data access bodies should monitor the application of Chapter IV of this Regulation and contribute to its consistent application throughout the Union. For that purpose, the health data access bodies should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation. The health data access bodies should also cooperate with stakeholders, including patient organisations. Since the secondary use of health data involves the processing of personal data concerning health, the relevant provisions of Regulation (EU) 2016/679 apply and the supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 should be tasked with enforcing these rules. Moreover, given that health data are sensitive data and in a duty of loyal cooperation, the health data access bodies should inform the data protection authorities of any issues related to the data processing for secondary use, including penalties. In addition to the tasks necessary to ensure effective secondary use of health data, the health data access body should strive to expand the availability of additional

health datasets, support the development of AI in health and promote the development of common standards. They should apply tested techniques that ensure electronic health data is processed in a manner that preserves the privacy of the information contained in the data for which secondary use is allowed, including techniques for pseudonymisation, anonymisation, generalisation, suppression and randomisation of personal data. Health data access bodies can prepare datasets to the data user requirement linked to the issued data permit. This includes rules for anonymization of microdata sets.

(44) Considering the administrative burden for health data access bodies to inform the natural persons whose data are used in data projects within a secure processing environment, the exceptions provided for in Article 14(5) of Regulation (EU) 2016/679 should apply. Therefore, health data access bodies should provide general information concerning the conditions for the secondary use of their health data containing the information items listed in Article 14(1) and, where necessary to ensure fair and transparent processing, Article 14(2) of Regulation (EU) 2016/679, e.g. information on the purpose and the data categories processed. Exceptions from this rule should be made when the results of the research could assist in the treatment of the natural person concerned. In this case, the data user should inform the health data access body, which should inform the data subject or his health professional. Natural persons should be able to access the results of different research projects on the website of the health data access body, ideally in an easily searchable manner. The list of the data permits should also be made public. In order to promote transparency in their operation, each health data access body should publish an annual activity report providing an overview of its activities.

(45) Regulation […] [Data Governance Act COM/2020/767 final] sets out the general rules for the management of data altruism. At the same time, given that the health sector manages sensitive data, additional criteria should be established through the rulebook foreseen in Regulation […] [Data Governance Act COM/2020/767 final]. Where such a rulebook foresees the use of a secure processing environment for this sector, this should comply with the criteria established in this Regulation. The health data access bodies should cooperate with the bodies designated under Regulation […] [Data Governance Act COM/2020/767 final] to supervise the activity of data altruism organisations in the health or care sector.

(46) In order to support the secondary use of electronic health data, the data holders should refrain from withholding the data, requesting unjustified fees that are not transparent nor proportionate with the costs for making data available (and, where relevant, with marginal costs for data collection), requesting the data users to co-publish the research or other practices that could dissuade the data users from requesting the data. Where ethical approval is necessary for providing a data permit, its evaluation should be based on its own merits. On the other hand, Union institutions, bodies, offices and agencies, including EMA, ECDC and the Commission, have very important and insightful data. Access to data of such institutions, bodies, offices and agencies should be granted through the health data access body where the controller is located.

(47) Health data access bodies and single data holders should be allowed to charge fees ~~based on the provisions of Regulation […] [Data Governance Act COM/2020/767 final]~~ in relation to their tasks. Such fees may take into account the situation and interest of SMEs, individual researchers or public bodies. ***In particular, Member States may establish policies for health data access bodies in their jurisdiction allowing to charge reduced fees to certain categories of data users. On the other hand, health data access bodies should be able to cover the costs of their operation with fees, and this may lead to higher fees charged to certain categories of data users, established in a proportionate, justified and transparent manner, if servicing their data access applications and data requests requires more work in aspects such as compliance with Chapter V of the GDPR.*** Data holders should be allowed to also charge fees for making data available. Such fees should reflect the costs for providing such services. Private data holders may also charge fees for the collection of data. In order to ensure a harmonised approach concerning fee policies and structure***s***, the Commission may ~~adopt implementing acts. Provisions in Article 10 of the Regulation [Data Act COM/2022/68 final] should apply for fees charged under this Regulation~~ ***issue guidelines on fee policies and fee structures***.

(48) In order to strengthen the enforcement of the rules on the secondary use of electronic health data, appropriate measures that can lead to penalties or temporary or definitive exclusions from the EHDS framework of the data users or data holders that do not comply with their obligations. The health data access body should be empowered to verify compliance and give data users and holders the opportunity to reply to any findings and to remedy any infringement. The imposition of penalties should be subject to appropriate

procedural safeguards in accordance with the general principles of law of the relevant Member State, including effective judicial protection and due process.

(49) Given the sensitivity of electronic health data, it is necessary to reduce risks on the privacy of natural persons by applying the data minimisation principle as set out in Article 5 (1), point (c) of Regulation (EU) 2016/679. Therefore, the use of anonymised electronic health data which is devoid of any personal data should be made available when possible and if the data user asks it. If the data user needs to use personal electronic health data, it should clearly indicate in its request the justification for the use of this type of data for the planned data processing activity. The personal electronic health data should only be made available in pseudonymised format and the encryption key can only be held by the health data access body. Data users should not attempt to re-identify natural persons from the dataset provided under this Regulation, subject to administrative or possible criminal penalties, where the national laws foresee this. However, this should not prevent, in cases where the results of a project carried out based on a data permit has a health benefit or impact to a concerned natural person (for instance, discovering treatments or risk factors to develop a certain disease), the data users would inform the health data access body, which in turn would inform the concerned natural person(s). Moreover, the applicant can request the health data access bodies to provide the answer to a data request, including in statistical form. In this case, the data users would not process health data and the health data access body would remain sole controller for the data necessary to provide the answer to the data request.

(50) In order to ensure that all health data access bodies issue permits in a similar way, it is necessary to establish a standard common process for the issuance of data permits, with similar requests in different Member States. The applicant should provide health data access bodies with several information elements that would help the body evaluate the request and decide if the applicant may receive a data permit for secondary use of data, also ensuring coherence between different health data access bodies. Such information include: the legal basis under Regulation (EU) 2016/679 to request access to data (exercise of a task in the public interest assigned by law or legitimate interest), purposes for which the data would be used, description of the needed data and possible data sources, a description of the tools needed to process the data, as well as characteristics of the secure environment that are needed. Where data is requested in pseudonymised format, the data applicant should explain why this is necessary and why anonymous data would not suffice.

An ethical assessment may be requested based on national law. The health data access bodies and, where relevant data holders, should assist data users in the selection of the suitable datasets or data sources for the intended purpose of secondary use. Where the applicant needs anonymised statistical data, it should submit a data request application, requiring the health data access body to provide directly the result. In order to ensure a harmonised approach between health data access bodies, the Commission should support the harmonisation of data application, as well as data request.

(51) As the resources of health data access bodies are limited, they can apply prioritisation rules, for instance prioritising public institutions before private entities, but they should not make any discrimination between the national or from organisations from other Member States within the same category of priorities. The data user should be able to extend the duration of the data permit in order, for example, to allow access to the datasets to reviewers of scientific publication or to enable additional analysis of the dataset based on the initial findings. This would require an amendment of the data permit and may be subject to an additional fee. However, in all the cases, the data permit should reflect theses additionals uses of the dataset. Preferably, the data user should mention them in their initial request for the issuance of the data permit. In order to ensure a harmonised approach between health data access bodies, the Commission should support the harmonisation of data permit.

(52) As the COVID-19 crisis has shown, the Union institutions, bodies, offices and agencies, especially the Commission, need access to health data for a longer period and on a recurring basis. This is may be the case not only in specific circumstances in times of crisis but also to provide scientific evidence and technical support for Union policies on a regular basis. Access to such data may be required in specific Member States or throughout the whole territory of the Union.

(53) For requests to access electronic health data from a single data holder in a single Member State and in order to alieviate the administrative burden for heath data access bodies of managing such request, the data user should be able to request this data directly from the data holder and the data holder should be able to issue a data permit while complying with all the requirements and safeguards linked to such request and permit. Multi-country requests and requests requiring combination of datasets from several data holders should

always be channelled through health data access bodies. The data holder should report to the health data access bodies about any data permits or data requests they provide.

(54) Given the sensitivity of electronic health data, data users should not have an unrestricted access to such data. All secondary use access to the requested electronic health data should be done through a secure processing environment. In order to ensure strong technical and security safeguards for the electronic health data, the health data access body or, where relevant, single data holder should provide access to such data in a secure processing environment, complying with the high technical and security standards set out pursuant to this Regulation. Some Member States took measures to locate such secure environments in Europe. The processing of personal data in such a secure environment should comply with Regulation (EU) 2016/679, including, where the secure environment is managed by a third party, the requirements of Article 28 and, where applicable, Chapter V. Such secure processing environment should reduce the privacy risks related to such processing activities and prevent the electronic health data from being transmitted directly to the data users. The health data access body or the data holder providing this service should remain at all time in control of the access to the electronic health data with access granted to the data users determined by the conditions of the issued data permit. Only non-personal electronic health data which do not contain any electronic health data should be extracted by the data users from such secure processing environment. Thus, it is an essential safeguard to preserve the rights and freedoms of natural persons in relation to the processing of their electronic health data for secondary use. The Commission should assist the Member State in developing common security standards in order to promote the security and interoperability of the various secure environments.

(55) For the processing of electronic health data in the scope of a granted permit, the health data access bodies and the data users should be joint controllers in the sense of Article 26 of Regulation (EU) 2016/679, meaning that the obligations of joint controllers under that Regulation will apply. To support health data access bodies and data users, the Commission should, by means of an implementing act, provide a template for the joint controller arrangements health data access bodies and data users will have to enter into. In order to achieve an inclusive and sustainable framework for multi-country secondary use of electronic health data, a cross-border infrastructure should be established. HealthData@EU should accelerate the secondary use of electronic health data while increasing legal certainty, respecting the privacy of natural persons and being

interoperable. Due to the sensitivity of health data, principles such as "privacy by design" and "bring questions to data instead of moving data" should be respected whenever possible. Authorised participants in HealthData@EU could be health data access bodies, research infrastructures established as an European Research Infrastructure Consortium ('ERIC') under Council Regulation (EC) No 723/2009[12] or similar structures established under another Union legislation, as well as other types of entities, including infrastructures under the European Strategy Forum on Research Infrastructures (ESFRI), infrastructures federated under the European Open Science Cloud (EOSC). Other authorised participants should obtain the approval of the joint controllership group for joining HealthData@EU. On the other hand, HealthData@EU should enable the secondary use of different categories of electronic health data, including linking of the health data with data from other data spaces such as environment, agriculture, social etc. The Commission could provide a number of services within HealthData@EU, including supporting the exchange of information amongst health data access bodies and authorised participants for the handling of cross-border access requests, maintaining catalogues of electronic health data available through the infrastructure, network discoverability and metadata queries, connectivity and compliance services. The Commission may also set up a secure environment, allowing data from different national infrastructures to be transmitted and analysed, at the request of the controllers. The Commission digital strategy promote the linking of the various common European data spaces. For the health sector, interoperability with the sectors such as the environmental, social, agricultural sectors may be relevant for additional insights on health determinants. For the sake of IT efficiency, rationalisation and interoperability of data exchanges, existing systems for data sharing should be reused as much as possible, like those being built for the exchange of evidences under the once only technical system of Regulation (EU) 2018/1724 of the European Parliament and of the Council[13].

(56) In case of cross-border registries or databases, such as the registries of European Reference Networks for Rare Diseases, which receive data from different healthcare providers in

---

12 Council Regulation (EC) No 723/2009 of 25 June 2009 on the Community legal framework for a European Research Infrastructure Consortium (ERIC) (OJ L 206, 8.8.2009, p. 1).

13 Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, p. 1).

several Member States, the health data access body where the coordinator of the registry is located should be responsible for providing access to data.

(57) The authorisation process to gain access to personal health data in different Member States can be repetitive and cumbersome for data users. Whenever possible, synergies should be established to reduce the burden and barriers for data users. One way to achieve this aim is to adhere to the "single application" principle whereby, with one application, the data user obtain authorisation from multiple health data access bodies in different Member States.

(58) The health data access bodies should provide information about the available datasets and their characteristics so that data users can be informed of elementary facts about the dataset and assess their possible relevance to them. For this reason, each dataset should include, at least, information concerning the source, nature of data and conditions for making data available. Therefore, an EU datasets catalogue should be established to facilitate the discoverability of datasets available in the EHDS; to help data holders to publish their datasets; to provide all stakeholders, including the general public, also taking into account people with disabilities, with information about datasets placed on the EHDS (such as quality and utility labels, dataset information sheets); to provide the data users with up-to-date data quality and utility information about datasets.

(59) Information on the quality and utility of datasets increases the value of outcomes from data intensive research and innovation significantly, while, at the same time, promoting evidence-based regulatory and policy decision-making. Improving the quality and utility of datasets through informed customer choice and harmonising related requirements at Union level, taking into account existing Union and international standards, guidelines, recommendations for data collection and data exchange (i.e. FAIR principles: Findable, Accessible, Interoperable and Reusable), benefits also data holders, health professionals, natural persons and the Union economy overall. A data quality and utility label for datasets would inform data users about the quality and utility characteristics of a dataset and enable them to choose the datasets that best fit their needs. The data quality and utility label should not prevent datasets from being made available through the EHDS, but provide a transparency mechanism between data holders and data users. For example, a dataset that does not fulfil any requirement of data quality and utility should be labelled with the class representing the poorest quality and utility, but should still be made available. Expectations set in frameworks described in Article 10 of Regulation […] [AI Act COM/2021/206 final]

and its relevant documentation specified in Annex IV should be taken into account when developing the data quality and utility framework. Member States should raise awareness about the data quality and utility label through communication activities. The Commission could support these activities.

(60) The EU datasets catalogue should minimise the administrative burden for the data holders and other database users; be user-friendly, accessible and cost-effective, connect national data catalogues and avoid redundant registration of datasets. The EU datasets catalogue could be aligned with the data.europa.eu initiative and without prejudice to the requirements set out in the Regulation […] [Data Governance Act COM/2020/767 final]. Member states should ensure that national data catalogues are interoperable with existing dataset catalogues from European research infrastructures and other relevant data sharing infrastructures.

(61) Cooperation and work is ongoing between different professional organisations, the Commission and other institutions to set up minimum data fields and other characteristics of different datasets (registries for instance). This work is more advanced in areas such as cancer, rare diseases, and statistics and ~~shall~~***should*** be taken into account when defining new standards. However, many datasets are not harmonised, raising comparability issues and making cross-border research difficult. Therefore, more detailed rules should be set out in implementing acts to ensure a harmonised ~~provision,~~ coding and registration of electronic health data***. Such datasets may include data from registries of rare diseases, orphan drugs databases, cancer registries and registries of highly relevant infectious diseases***. Member States should work towards delivering sustainable economic and social benefits of European electronic health systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of healthcare and ensuring access to safe and high-quality healthcare.

(62) The Commission should support Member States in building capacity and effectiveness in the area of digital health systems for primary and secondary use of electronic health data. Member States should be supported to strengthen their capacity. Activities at Union level, such as benchmarking and exchange of best practices are relevant measures in this respect.

(63) The use of funds should also contribute to attaining the objectives of the EHDS. Public procurers, national competent authorities in the Member States, including digital health

authorities and health data access bodies, as well as the Commission should make references to applicable technical specifications, standards and profiles on interoperability, security and data quality, as well as other requirements developed under this Regulation when defining the conditions for public procurement, calls for proposals and allocation of Union funds, including structural and cohesion funds.

(63a) ***Any judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a digital health authority, a health data access body or a health data user to transfer or give access to anonymous non-personal electronic health data within the scope of this Regulation held in the Union should be recognised or enforceable in any manner only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State,* compliant with Union law.**

(64) Certain categories of electronic health data can remain particularly sensitive even when they are in anonymised format and thus non-personal, as already specifically foreseen in the Data Governance Act. Even in situations of the use of state of the art anonymization techniques, there remains a residual risk that the capacity to re-identify could be or become available, beyond the means reasonably likely to be used. Such residual risk is present in relation to rare diseases (a life-threatening or chronically debilitating condition affecting not more than five in 10 thousand persons in the Union), where the limited numbers of case reduce the possibility to fully aggregate the published data in order to preserve the privacy of natural persons while also maintaining an appropriate level of granularity in order to remain meaningful. It can affect different types of health data depending on the level of granularity and description of the characteristics of data subjects, the number of people affected or and for instance in cases of data included in electronic health records, disease registries, biobanks, person generated data etc. where the identification characteristics are broader and where, in combination with other information (e.g. in very small geographical areas) or through the technological evolution of methods which had not been available at the moment of anonymisation, can lead to the re-identification of the data subjects using means that are beyond those reasonably likely to be used. The realisation of such risk of re-identification of natural persons would present a major concern and is likely to put the acceptance of the policy and rules on secondary use provided for in this Regulation at risk. Furthermore, aggregation techniques are less tested for non-personal data containing for example trade secrets, as in the reporting on clinical trials, and enforcement of breaches of trade secrets outside the Union is more difficult in the absence of a sufficient international protection standard. Therefore, for these types of health data, there remains a risk for re-identification after the anonymisation or aggregation, which could not be reasonably mitigated initially. This falls within the criteria indicated in Article

5(13) of Regulation […] [Data Governance Act COM/2020/767 final]. These types of health data would thus fall within the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final] for transfer to third countries. The protective measures, proportional to the risk of re-identification, would need to take into account the specificities of different data categories or of different anonymization or aggregation techniques and will be detailed in the context of the Delegated Act under the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final].

(64a) ***The processing of large amounts of personal health data for the purposes foreseen in the EHDS, as part of data processing activities in the context of servicing data access applications, data permits and data requests entails higher risks of unauthorised access to such personal data, as well as the possibility of cybersecurity incidents. Personal health data are particularly sensitive as they often constitute intimate information, covered by medical secrecy, the disclosure of which to unauthorised third parties can cause significant distress. Taking fully into consideration the principles outlined in the case law of the Court of Justice of the European Union, this Regulation ensures full respect for fundamental rights, for the right to privacy and for the principle of proportionality. In order to ensure the full integrity and confidentiality of personal electronic health data under the Regulation, to guarantee a particularly high level of protection and security, and to reduce the risk of unlawful access to that personal electronic health data, the Regulation makes provision for personal electronic health data to be stored and processed within the Union for the purpose of carrying out the tasks foreseen by this Regulation, unless an adequacy decision pursuant to article 45 of Regulation (EU) 2016/679 applies.***

(65) In order to promote the consistent application of this Regulation, a European Health Data Space Board (EHDS Board) should be set up. The Commission should participate in its activities and chair it. It should contribute to the consistent application of this Regulation throughout the Union, including by helping Member State to coordinate the use of electronic health data for healthcare, certification, but also concerning the secondary use of electronic health data. Given that, at national level, digital health authorities dealing with the primary use of electronic health data may be different to the health data access bodies dealing with the secondary use of electronic health data, the functions are different and there is a need for distinct cooperation in each of these areas, the EHDS Board should be

able to set up subgroups dealing with these two functions, as well as other subgroups, as needed. For an efficient working method, the digital health authorities and health data access bodies should create networks and links at national level with different other bodies and authorities, but also at Union level. Such bodies could comprise data protection authorities, cybersecurity, eID and standardisation bodies, as well as bodies and expert groups under Regulations […], […], […] and […] [Data Governance Act, Data Act, AI Act and Cybersecurity Act].

(66) In order to manage the cross-border infrastructures for primary and secondary use of electronic health data, it is necessary to create the Joint controllership group for authorised participants (e.g. to ensure the compliance with data protection rules and this Regulation for the processing operations performed in such infrastructures).

(67) Since the objectives of this Regulation: to empower natural persons through increased control of their personal health data and support their free movement by ensuring that health data follows them; to foster a genuine single market for digital health services and products; to ensure a consistent and efficient framework for the reuse of natural persons' health data for research, innovation, policy-making and regulatory activities cannot be sufficiently achieved by the Member States, through coordination measures alone, as shown by the evaluation of the digital aspects of the Directive 2011/24/EU but can rather, by reason of harmonising measures for rights of natural persons in relation to their electronic health data, interoperability of electronic health data and a common framework and safeguards for the primary and secondary use of electronic health data, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(68) In order to ensure that EHDS fulfils its objectives, the power to adopt acts in accordance with Article 290 Treaty on the Functioning of the European Union should be delegated to the Commission in respect of different provisions of primary and secondary use of electronic health data. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-

institutional Agreement of 13 April 2016 on Better Law-Making[14]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(69) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[15].

(70) Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement. For certain specific infringements, Member States should take into account the margins and criteria set out in this Regulation.

(71) In order to assess whether this Regulation reaches its objectives effectively and efficiently, is coherent and still relevant and provides added value at Union level the Commission should carry out an evaluation of this Regulation. The Commission should carry out a partial evaluation of this Regulation 5 years after its entry into force, on the self-certification of EHR systems, and an overall evaluation 7 years after the entry into force of this Regulation. The Commission should submit reports on its main findings following each evaluation to the European Parliament and to the Council, the European Economic and Social Committee and the Committee of the Regions.

(72) For a successful cross-border implementation of EHDS, the European Interoperability Framework[16] to ensure legal, organisational, semantic and technical interoperability should be considered as common reference.

(73) The evaluation of the digital aspects of Directive 2011/24/EU shows limited effectiveness of eHealth Network, but also strong potential for EU work in this area, as shown by the

---

14 OJ L 123, 12.5.2016, p. 1.

15 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

16 European Commission, European Interoperability Framework.

work during pandemic. Therefore, the article 14 of the Directive will be repealed and replaced by the current Regulation and the Directive will be amended accordingly.

(74) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42 of Regulation (EU) 2018/1725 and delivered an opinion on […].

(75) This Regulation should not affect the application of the rules of competition, and in particular Articles 101 and 102 of the Treaty. The measures provided for in this Regulation should not be used to restrict competition in a manner contrary to the Treaty.

(76) Given the need for technical preparation, this Regulation should apply from [12 months after entry into force],

HAVE ADOPTED THIS REGULATION:

Chapter I
General provisions

Article 1

Subject matter and scope

1. This Regulation establishes the European Health Data Space ('EHDS') by providing for ***common*** rules, ~~common~~ standards ~~and practices~~, infrastructures and a governance framework ***with a view to facilitating access to electronic health data*** for the ***purposes of*** primary and secondary use of ~~electronic health~~ ***these*** data.

2. This Regulation:

   (a) ~~strengthens~~***specifies and complements*** the rights ***laid down in the Regulation (EU) 2016/679*** of natural persons in relation to the ~~availability and control~~***primary and secondary use*** of their ***personal*** electronic health data;

   (b) lays down ***common*** rules for ***electronic health records systems ('EHR systems') in relation to two mandatory software components, namely the 'European***

interoperability component for EHR ~~the placing on the market, making available on the market or putting into service of electronic health records~~ systems***' and the***~~('~~***'European logging component for*** EHR systems' ***as defined in Article 2(2), subparagraphs (nc*** ~~)~~ ***and (nd) and wellness applications that claim interoperability with EHR systems in relation to those two components*** in the Union ***for primary use***;

(c) lays down ***common*** rules and mechanisms ~~supporting the~~***for primary and*** secondary use of electronic health data;

(d) establishes a ~~mandatory~~ cross-border infrastructure enabling the primary use of ***personal*** electronic health data across the Union;

(e) establishes a ~~mandatory~~ cross-border infrastructure for the secondary use of electronic health data~~.~~**;**

(f) establishes governance and coordination on national and European level for both primary and secondary use of electronic health data.

~~3.~~ ~~This Regulation applies to:~~

~~(a) manufacturers and suppliers of EHR systems and wellness applications placed on the market and put into service in the Union and the users of such products;~~

~~(b) controllers and processors established in the Union processing electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States;~~

~~(c) controllers and processors established in a third country that has been connected to or are interoperable with MyHealth@EU, pursuant to Article 12(5);~~

~~(d) data users to whom electronic health data are made available by data holders in the Union.~~

3a. This Regulation shall be without prejudice to Regulations (EU) 2016/679, (EU) 2018/1725, (EU) No 536/2014 and (EC) No 223/2009.

4. This Regulation ~~shall be without prejudice to~~ ***complements*** other Union legal acts regarding access to, sharing of or secondary use of electronic health data, or requirements related to the processing of data in relation to electronic health data, in particular Regulations (EU) ~~2016/679, (EU) 2018/1725,~~***2022/868 and*** […] [Data ~~Governance Act COM/2020/767~~***Act COM/2022/68*** final]***. In the event of a specific conflict with these Regulations, the rules set out in this Regulation shall prevail*** ~~and […] [Data Act COM/2022/68 final]~~.

5. This Regulation shall be without prejudice to Regulations (EU) 2017/745***, (EU) 2017/746*** and […] [AI Act COM/2021/206 final], as regards the security– of medical devices***, in vitro diagnostic medical devices*** and AI systems that interact with EHR systems.

6. This Regulation shall ~~not affect the rights and obligations laid down in~~ ***be without prejudice to*** Union or national law ~~concerning~~ ***regarding electronic health*** data processing for the purposes of reporting, complying with ***access to*** information requests or demonstrating or verifying compliance with legal obligations ***or Union or national law regarding the granting of access to and disclosure of official documents***.

6a. This Regulation shall be without prejudice to specific provisions in Union or national law providing for access to electronic health data for further processing by public bodies of the Member States, Union institutions, bodies and agencies, or by private entities entrusted under Union or national law with a task of public interest, for the purpose of carrying out such task. Further, this Regulation shall not affect access to electronic health data for secondary use agreed in the framework of contractual or administrative arrangements between public or private entities.

7. This Regulation shall not apply to the processing of electronic health data for purposes of public security, national security, defence and law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. The powers of competent authorities for the prevention, investigation, detection and prosecution of criminal offences established by law to obtain electronic health data are unaffected. Likewise, electronic health data held by courts for the purpose of judicial proceedings are out of scope of this Regulation.

Article 2

Definitions

1. For the purposes of this Regulation, following definitions shall apply:

(a) the definitions ~~in~~ ***of 'personal data', 'processing', 'pseudonymisation', 'controller', 'processor', 'third party', 'consent', 'genetic data', 'data concerning health', 'international organisation' pursuant to Article 4(1), (2), (5), (7), (8), (10), (11), (13), (15) and (26) of the*** Regulation (EU) 2016/679;

(b) the definitions of 'healthcare', 'Member State of affiliation', 'Member State of treatment', 'health professional', 'healthcare provider', 'medicinal product' and 'prescription', pursuant to Article 3 (a), (c), (d), (f), (g), (i) and (k) ~~of Article 3~~ of the Directive 2011/24/EU;

(c) the definitions of 'data', 'access', 'data altruism', 'public sector body' and 'secure processing environment', pursuant to Article 2 (1), ~~(8), (10~~***(13), (16***), (~~11~~***17***) and (~~14~~***20***) of ~~[Data Governance Act COM/2020/767 final]~~ ***Regulation (EU) 2022/868***;

(d) the definitions of 'making available on the market', 'placing on the market', 'market surveillance', 'market surveillance authority', 'non-compliance', 'manufacturer', 'importer', 'distributor', 'economic operator', 'corrective action', ~~'risk'~~, 'recall' and 'withdrawal', pursuant to Article 2 (1), (2), (3), (4), (7), (8), (9), (10), (13), (16), ~~(18),~~ (22) and (23) of the Regulation (EU) 2019/1020;

(e) the definitions of 'medical device', 'intended purpose', 'instructions for use', 'performance', 'health institution' and 'common specifications', pursuant to Article 2 (1), (12), (14), (22), (36) and (71) of the Regulation (EU) 2017/745;

(f) the definitions of 'electronic identification', 'electronic identification means' and 'person identification data' pursuant to Article 3 (1), (2) and (3) of the Regulation (EU) No 910/2014~~.~~**;**

(g) the definition of 'contracting authorities' pursuant to Article 2(1)(1) of the Directive 2014/24/EU;

(h) the definition of 'public health' pursuant to Article 38(c) of the Regulation (EC) No 1338/2008.

2. In addition, for the purposes of this Regulation the following definitions shall apply:

(a) 'personal electronic health data' means ***personal*** data concerning health and ***personal*** genetic data as defined in ~~Regulation (EU) 2016/679, as well as data referring to determinants of health, or data processed in relation to the provision of healthcare services~~ ***Article 4, (13) and (15) of Regulation (EU) 2016/679*** , processed in an electronic form;

(b) '~~non-personal~~ ***anonymous*** electronic health data' means data ~~concerning~~ ***related to*** health***, processed in an electronic form, which does not relate to an identified or identifiable natural person or*** ~~and genetic data in electronic format that falls outside the definition of~~ personal data ~~provided in Article 4(1) of Regulation (EU) 2016/679~~;~~**data**~~ ***concerning health processed in a such manner that the data subject is not or no longer identifiable.***

(c) 'electronic health data' means personal ***electronic health data or anonymous*** ~~or non-personal~~ electronic health data~~;~~

(d) 'primary use of electronic health data' means the processing of personal electronic health data for the provision of ~~health services~~ ***healthcare*** to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social ~~security~~, administrative or reimbursement services;

(e) 'secondary use of electronic health data' means the processing of electronic health data for purposes set out in ~~Chapter IV~~ ***Article 34*** of this Regulation, **other than the initial purposes for which they were collected or produced**. ~~The data used may include personal electronic health data initially collected in the context of primary use, but also electronic health data collected for the purpose of the secondary use;~~

(f) ‘interoperability’ means the ability of organisations as well as software applications or devices from the same manufacturer or different manufacturers to interact ~~towards mutually beneficial goals~~, involving the exchange of information and knowledge without changing the content of the data between these organisations, software applications or devices, through the processes they support;

~~(g) ‘European electronic health record exchange format’ means a structured, commonly used and machine-readable format that allows transmission of personal electronic health data between different software applications, devices and healthcare providers;~~

(h) ‘registration of electronic health data’ means the recording of health data in an electronic format, through manual entry of data, through the collection of data by a device, or through the conversion of non-electronic health data into an electronic format, to be processed in an EHR system or a wellness application;

(i) ‘electronic health data access service’ means an online service, such as a portal or a mobile application, that enables natural persons not acting in their professional role to access their own electronic health data or electronic health data of those natural persons whose electronic health data they are legally authorised to access;

(j) ‘health professional access service’ means a service, supported by an EHR system, that enables health professionals to access data of natural persons under their treatment;

~~(k) ‘data recipient’ means a natural or legal person that receives data from another controller in the context of the primary use of electronic health data;~~

~~(l) ‘telemedicine’ means the provision of healthcare services, including remote care and online pharmacies, through the use of information and communication technologies, in situations where the health professional and the patient (or several health professionals) are not in the same location;~~

(m) ‘EHR’ (electronic health record) means a collection of ***personal*** electronic health data related to a natural person and collected in the health system, processed for ***the provision of*** healthcare ~~purposes~~;

(n) ‘EHR system’ (electronic health record system) means any ***system where the*** appliance or software ***allows to store, intermediate, export, import, convert, edit or view personal electronic health data that belongs to the priority categories of personal electronic health data as referred to in Article 5(1) of this Regulation and is*** intended by the manufacturer to be used ~~for storing, intermediating, importing, exporting, converting, editing or viewing electronic~~ ***by healthcare providers in providing patient care or by patient to access to their*** health ~~records~~ ***data***

(na) ‘putting into service’ means the first use, for its intended purpose, in the Union, of an EHR system covered by this Regulation;

(nb) ‘software component’ or ‘component’ means a discrete part of software which provides specific functionality or performs specific procedures and which can operate in conjunction with other components. Components are designed to be reusable and to integrate seamlessly with other components within a larger software system;

(nc) ‘European interoperability component for EHR systems’ (or ‘the interoperability component’) means a software component of the EHR system which provides and receives the **personal electronic health data referred to in Article 5** ***in the format referred to in Article 6 of this Regulation; The European interoperability component is independent of the European logging component;***

(nd) ‘European logging component for EHR systems’ (or ‘the logging component’) means a software component of the EHR system which provides logging information relating to accesses of health professionals or other individuals to personal electronic health data **referred to in Article 5,** ***in the format defined in Annex II.3.4 of this Regulation; The European logging component is independent of the European interoperability component;***

(ne) ‘harmonised components of EHR systems’ means the European interoperability component for EHR systems and the European logging component for EHR systems;

(o) ‘wellness application’ means any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data for other purposes than healthcare, such as well-being and pursuing healthy life-styles;

(p) ‘CE marking of conformity’ means a marking by which the manufacturer indicates that the EHR system is in conformity with the applicable requirements set out in this Regulation and other applicable Union legislation providing for its affixing ***pursuant to Regulation (EC) No 765/2008***;

(pa) ‘risk’ means the combination of the degree of severity of a harm and the probability of an occurrence of hazard causing the harm to health, safety and information security;

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

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

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

~~(r) ‘national contact point for digital health’ means an organisational and technical gateway for the provision of cross-border digital health information services for primary use of electronic health data, under the responsibility of the Member States;~~

~~(s) ‘central platform for digital health’ means an interoperability platform providing services to support and facilitate the exchange of electronic health data between national contact points for digital health;~~

~~(t) ‘MyHealth@EU’ means the cross-border infrastructure for primary use of electronic health data formed by the combination of national contact points for digital health and the central platform for digital health;~~

~~(u) ‘national contact point for secondary use of electronic health data’ means an organisational and technical gateway enabling the cross-border secondary use of electronic health data, under the responsibility of the Member States;~~

~~(v) 'central platform for secondary use of electronic health data' means an interoperability platform established by the Commission, providing services to support and facilitate the exchange of information between national contact points for secondary use of electronic health data;~~

~~(x) 'HealthData@EU' means the infrastructure connecting national contact points for secondary use of electronic health data and the central platform;~~

(qa) 'care' means a professional service the purpose of which is to address the specific needs of a person who, on account of impairment or other physical or mental conditions requires assistance to carry out essential activities of daily living in order to support their personal autonomy.

(xb) '***health*** data holder' means any natural or legal person, ~~which is an entity or a~~ ***public authority, agency or other*** body in the ~~health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data;~~ ***healthcare or the care sectors; as well as any natural o legal person developing products or services intended for the health, healthcare or care sectors; developing or manufacturing wellness applications; performing research in relation to the health, healthcare or care sectors; or acting as a mortality registry; as well as any Union institution, body, office or agency; who has either:***

(a) the right or obligation, in accordance with applicable Union law or national legislation, to process personal electronic health data for the provision of healthcare or care or for public health, reimbursement, research, innovation, policy making, official statistics, patient safety or regulatory purposes, in its capacity as a controller or joint controller; or

(b) the ability to make available, including to register, provide, restrict access or exchange anonymous electronic health data, through control of the technical design of a product and related services.

(ya) 'health data intermediation entity' means a legal person able to make available, including to register, provide, process, restrict access or exchange electronic health data provided by data holders for secondary use.

(z) '***health*** data user' means a natural or legal person who has lawful access to ~~personal or non-personal~~ electronic health data for secondary use ***based on a data permit or a data request pursuant to this Regulation***;

(aa) ~~'~~data permit' means an administrative decision issued to a ***health*** data user by a health data access body or ***a single health*** data holder to process ***certain*** ~~the~~ electronic health data ~~specified in the data permit~~ for ***specific*** ~~the~~ secondary use purposes ~~specified in the data permit~~ based on conditions laid down in ***Chapter IV of*** this Regulation;

(ab) 'dataset' means a structured collection of electronic health data;

(aba) 'datasets of high impact for the secondary use of electronic health data' means datasets the re-use of which is associated with important benefits because of their relevance for health research;

(ac) 'dataset catalogue' means a collection of datasets descriptions, which is arranged in a systematic manner and consists of a user-oriented public part, where information concerning individual dataset parameters is accessible by electronic means through an online portal;

(ad) 'data quality' means the degree to which ~~characteristics~~ ***the elements*** of electronic health data are ***assessed and considered*** suitable for ***their intended primary and*** secondary use;

(ae) 'data quality and utility label' means a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset.

Chapter II

Primary use of electronic health data

SECTION 1

ACCESS TO AND TRANSMISSION OF PERSONAL ELECTRONIC HEALTH DATA FOR PRIMARY USE

Article 2A

Registration of personal electronic health data

1. ***Member States shall ensure that, where data is processed in electronic format for the provision of healthcare, healthcare providers shall register the relevant personal health data falling fully or partially under at least the priority categories referred to in Article 5 in the electronic format in an EHR system.***

1a. ***Where they process data in an electronic format, healthcare providers shall ensure that the personal electronic health data of the natural persons they treat are updated with information related to the healthcare provided.***

2. ***Where personal electronic health data is registered in a Member State of treatment that is not the Member State of affiliation of the person concerned, the Member State of treatment shall ensure that the registration is performed under the identification data of the natural person in the Member State of affiliation.***

3. ***The Commission shall, by means of implementing acts, determine data quality requirements, including semantics, uniformity, consistency of data registration, accuracy and completeness, for the registration of personal electronic health data in EHR system,as relevant.***

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

Article 3

Rights of natural persons in relation to the primary use of their personal electronic health data

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

2. Natural persons shall have the right to receive an electronic copy, in the European electronic health record exchange format referred to in Article 6, of at least their electronic health data in the priority categories referred to in Article 5.

3. In accordance with Article 23 of Regulation (EU) 2016/679, Member States may restrict the scope of this right whenever necessary for the protection of the natural person based on patient safety and ethics by delaying their access to their personal electronic health data for a limited period of time until a health professional can properly communicate and explain to the natural person information that can have a significant impact on his or her health.

4. Where the personal health data have not been registered electronically prior to the application of this Regulation, Member States may require that such data is made available in electronic format pursuant to this Article. This shall not affect the obligation to make personal electronic health data registered after the application of this Regulation available in electronic format pursuant to this Article.

5. Member States shall:

(a) establish one or more electronic health data access services at national, regional or local level enabling the exercise of rights referred to in paragraphs 1 and 2;

(b) establish one or more proxy services enabling a natural person to authorise other natural persons of their choice to access their electronic health data on their behalf.

The proxy services shall provide authorisations free of charge, electronically or on paper. They shall enable guardians or other representatives to be authorised, either automatically or upon request, to access electronic health data of the natural persons whose affairs they administer. Member States may provide that authorisations do not apply whenever necessary

for reasons related to the protection of the natural person, and in particular based on patient safety and ethics. The proxy services shall be interoperable among Member States.

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

7. Member States shall ensure that, when exercising the right to rectification under Article 16 of Regulation (EU) 2016/679, natural persons can easily request rectification online through the electronic health data access services referred to in paragraph 5, point (a), of this Article.

8. Natural persons shall have the right to give access to or request a data holder from the health or social security sector to transmit their electronic health data to a data recipient of their choice from the health or social security sector, immediately, free of charge and without hindrance from the data holder or from the manufacturers of the systems used by that holder.

Natural persons shall have the right that, where the data holder and the data recipient are located in different Member States and such electronic health data belongs to the categories referred to in Article 5, the data holder shall transmit the data in the European electronic health record exchange format referred to in Article 6 and the data recipient shall read and accept it.

By way of derogation from Article 9 of Regulation […] [Data Act COM/2022/68 final], the data recipient shall not be required to compensate the data holder for making electronic heath data available.

Natural persons shall have the right that, where priority categories of personal electronic health data referred to in Article 5 are transmitted or made available by the natural person according to the European electronic health record exchange format referred to in Article 6, such data shall be read and accepted by other healthcare providers.

9. Notwithstanding Article 6(1), point (d), of Regulation (EU) 2016/679, natural persons shall have the right to restrict access of health professionals to all or part of their electronic

health data. Member States shall establish the rules and specific safeguards regarding such restriction mechanisms.

10. Natural persons shall have the right to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare. The information shall be provided immediately and free of charge through electronic health data access services.

11. The supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Article, in accordance with the relevant provisions in Chapters VI, VII and VIII of Regulation (EU) 2016/679. They shall be competent to impose administrative fines up to the amount referred to in Article 83(5) of that Regulation. Those supervisory authorities and the digital health authorities referred to in Article 10 of this Regulation shall, where relevant, cooperate in the enforcement of this Regulation, within the remit of their respective competences.

12. The Commission shall, by means of implementing acts, determine the requirements concerning the technical implementation of the rights set out in this Article. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

Article 4

Access by health professionals to personal electronic health data

1. Where they process data in an electronic format, health professionals shall:

(a) have access to the electronic health data of natural persons under their treatment, irrespective of the Member State of affiliation and the Member State of treatment;

(b) ensure that the personal electronic health data of the natural persons they treat are updated with information related to the health services provided.

2. In line with the data minimisation principle provided for in Regulation (EU) 2016/679, Member States may establish rules providing for the categories of personal electronic

~~health data required by different health professions. Such rules shall not be based on the source of electronic health data.~~

~~3.~~ ~~Member States shall ensure that access to at least the priority categories of electronic health data referred to in Article 5 is made available to health professionals through health professional access services. Health professionals who are in possession of recognised electronic identification means shall have the right to use those health professional access services, free of charge.~~

~~4.~~ ~~Where access to electronic health data has been restricted by the natural person, the healthcare provider or health professionals shall not be informed of the content of the electronic health data without prior authorisation by the natural person, including where the provider or professional is informed of the existence and nature of the restricted electronic health data. In cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person, the healthcare provider or health professional may get access to the restricted electronic health data. Following such access, the healthcare provider or health professional shall inform the data holder and the natural person concerned or his/her guardians that access to electronic health data had been granted. Member States' law may add additional safeguards.~~

Article 5

Priority categories of personal electronic health data for primary use

1. ~~Where data is processed in electronic format, Member States shall implement access to and exchange~~ ***For the purposes of this Chapter, where data is processed in electronic format, the priority categories*** of personal electronic health data ~~for primary use fully or partially falling under~~ ***shall be*** the following***:*** ~~categories:~~

   (a) patient summaries;

   (b) electronic prescriptions;

   (c) electronic dispensations;

   (d) medical images and ***related*** image reports;

(e) laboratory results ***and related laboratory reports***;

(f) ***hospital*** discharge reports.

The main characteristics of the ***priority*** categories of ***personal*** electronic health data ~~in the first subparagraph~~ shall be as set out in Annex I.

1A. Member States may provide by virtue of national law that additional categories of personal electronic health data shall be accessed and exchanged for primary use pursuant to this Chapter. The Commission may, by means of implementing acts, lay down cross-border specifications for these data categories pursuant to Article 6(1A) and Article 12(8).

2. The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend ~~the list of priority categories of electronic health data in paragraph 1. Such delegated acts may also amend~~ Annex I by adding, modifying or removing the main characteristics of the priority categories of ***personal*** electronic health data ~~and indicating, where relevant, deferred application date. The categories of electronic health data added through such delegated acts~~ ***as referred to in paragraph 1. The amendments*** shall satisfy the following ***cumulative*** criteria:

(a) the ~~category~~***characteristic*** is relevant for ~~health services~~ ***healthcare*** provided to natural persons;

(b) ~~according to the most recent information, the category~~ ***the characteristic as modified*** is used in ***the majority of Member States according to the most recent information*** ~~a significant number of EHR systems used in Member States~~;

(c) ~~international standards exist for the category that have been examined for the possibility of their application in the Union~~***the changes are aimed to adapt the priority categories to the technical evolution and international standards***.

Article 6

European electronic health record exchange format

1. The Commission shall, by means of implementing acts, lay down the technical specifications for the priority categories of personal electronic health data referred to in Article 5 **(1),** setting out the European electronic health record exchange format. ***Such format shall be commonly used, machine-readable and allow transmission of personal electronic health data between different software applications, devices and healthcare providers. The format should support transmission of structured and unstructured health data.*** The format shall include the following elements:

   (a) datasets containing electronic health data and defining structures, such as data fields and data groups for the ~~content~~ representation of clinical content and other parts of the electronic health data;

   (b) coding systems and values to be used in datasets containing electronic health data;

   (c) technical specifications for the exchange of electronic health data, including its content representation, standards and profiles.

   Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2). ~~Member States shall ensure that where the priority categories of personal electronic health data referred to in Article 5 are provided by a natural person directly or transmitted to a healthcare provider by automatic means in the format referred to in paragraph 1, such data shall be read and accepted by the data recipient.~~

-1a. The Commission may, by means of implementing acts, lay down technical specifications that extend the European electronic health record exchange format to additional categories of electronic health data referred to in Article 5(1A). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

~~3~~**2**. Member States shall ensure that the priority categories of personal electronic health data referred to in Article 5 areissued in the ***European electronic health record exchange*** format referred to in paragraph 1***. Where*** ~~and~~ such data ~~shall be read and accepted by~~***are***

transmitted by automatic means for primary use the receiving provider shall accept the format of the data ~~recipient~~***and be able to read it***.

~~*Article 7*~~

~~Registration of personal electronic health data~~

~~1.~~ ~~Member States shall ensure that, where data is processed in electronic format, health professionals systematically register the relevant health data falling under at least the priority categories referred to in Article 5 concerning the health services provided by them to natural persons, in the electronic format in an EHR system.~~

~~2.~~ ~~Where electronic health data of a natural person is registered in a Member State that is not the Member State of affiliation of that person, the Member State of treatment shall ensure that the registration is performed under the person identification data of the natural person in the Member State of affiliation.~~

~~3.~~

~~The Commission shall, by means of implementing acts, determine the requirements for the registration of electronic health data by healthcare providers and natural persons, as relevant. Those implementing acts shall establish the following:~~

~~(a) categories of healthcare providers that are to register health data electronically;~~

~~(b) categories of health data that are to be registered systematically in electronic format by healthcare providers referred to in point (a);~~

~~(c) data quality requirements pertaining to the electronic registration of health data.~~

~~Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).~~

Article 7A

Access by health professionals to personal electronic health data

1. Member States shall ensure that where health professionals process personal health data in an electronic format, they shall have access to the personal electronic health data of natural persons under their treatment, through the health professional access services

referred to in Article 7B, irrespective of the Member State of affiliation and the Member State of treatment.

1A. ***Where the Member States of affiliation of the natural person under treatment and the Member States of treatment differ, cross-border access to the electronic health data of the natural person under treatment shall be provided through the infrastructure referred to in Article 12.***

2. ***The access referred to in paragraphs 1 and 1A shall include at least the priority categories in Article 5. In line with the principles provided for in Article 5 of the Regulation (EU) 2016/679, Member States may also establish rules providing for the categories of personal electronic health data accessible by different health professionals. Such rules shall take into account the possibility of restrictions imposed in according to Article 8E.***

3. ***Where access to electronic health data has been restricted by the natural person pursuant to Article 8E, the healthcare provider or health professional shall not be informed of the content of the electronic health data without prior authorisation by the natural personThe healthcare provider or health professional shall be informed exclusively about the existence of restricted electronic health data. In cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person as referred to in Article 9(2)(c) of the Regulation (EU) 2016/679, the healthcare provider or health professional may get access to the restricted electronic health data. Such events shall be logged in a clear and understandable format and shall be easily accessible for the natural persons. Member States' law may set out additional safeguards.***

Article 7B

Health professional access services

For the provision of healthcare, Member States shall ensure that access to the priority categories of electronic health data referred to in Article 5 is made available to health professionals through health professional access services. Those services shall be accessible only to health professionals who are in possession of electronic identification means recognised pursuant to Article 6 of Regulation (EU) No 910/2014 or other

electronic identification means compliant with common specifications referred to in Article 23 and the access shall be free of charge.

~~*Article 8*~~

~~*Telemedicine in the context of cross-border healthcare*~~

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

Article 8A

Right of natural persons to access their personal electronic health data

1. ***Natural persons shall have the right to access their personal electronic health data, at a minimum data that belongs in the priority categories in Article 5, processed for the provision of healthcare through the electronic health data access services referred to in Article 8G. The access shall be provided immediately after the personal electronic health data has been registered in an EHR system, adhering to technological practicability, free of charge and in an easily readable, consolidated and accessible form.***

2. ***Natural persons shall have the right to receive an electronic copy, free of charge, through the electronic health data access services referred to in Article 8G, in the European electronic health record exchange format referred to in Article 6, of at least their personal electronic health data in the priority categories referred to in Article 5.***

3. ***In accordance with Article 23 of Regulation (EU) 2016/679, Member States may restrict the scope of the rights referred to in paragraphs 1 and 2, in particular whenever necessary for the protection of the natural person based on patient safety and ethics by delaying their access to their personal electronic health data for a limited period of time until a health professional can properly communicate and explain to the natural person information that can have a significant impact on their health.***

Article 8B

Right of natural persons to insert information in their own EHR

Member States law may provide that natural persons or their representatives as referred to in Article 8G(2) have the right to insert information in their own EHR through electronic health data access services or applications linked to these services as referred to in Article 8G. That information shall in such cases be clearly distinguishable as inserted by the natural person or by his or her representative. Natural persons shall not have the possibility to directly alter the electronic health data and related information inserted by health professionals.

Article 8C

Right of natural persons to rectification

When exercising the right to rectification under Article 16 of Regulation (EU) 2016/679, natural persons shall be able to easily request, online through the electronic health data access services referred to in Article 8G, the controller of the personal electronic health data, to rectify their personal electronic health data.

Member States law may also enable natural persons to exercise other rights pursuant to Chapter III of Regulation (EU) 2016/679 online through the electronic health data access services referred to in Article 8G.

Article 8D

Right to data portability for natural persons

1. Natural persons shall have the right to give access to or request a healthcare provider to transmit, all or part of their electronic health data that belongs to the priority categories as referred to in Article 5 to another provider of their choice from the healthcare sector, without delay, free of charge and without hindrance from the transmitting provider or from the manufacturers of the systems used by that provider.

2. ***Natural persons shall have the right that, where healthcare providers are located in different Member States and such electronic health data belongs to the priority categories referred to in Article 5, the transmitting provider transmits the data in the European electronic health record exchange format referred to in Article 6 through the cross border infrastructure as referred to in Article 12. The receiving healthcare provider shall accept such data and shall be able to read it.***

3. ***Where natural persons have received an electronic copy of their priority categories of personal electronic health data as referred to in Article 8A(2), they shall be able to transmit that data to healthcare providers of their choice in the European electronic health record exchange format referred to in Article 6 The receiving provider shall accept such data and be able to read it, as appropriate.***

4. ***The Commission shall, by means of implementing acts, determine the requirements concerning the technical implementation of the rights set out in this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).***

Article 8E

Right to restrict access and information on access

1. ***Natural persons shall have the right to restrict access of health professionals and healthcare providers to their personal electronic health data referred to in Article 8A. Member States laws may provide that such restriction of access may be derogated under the same conditions as those laid down in Article 7A (3).***

Member States shall establish the rules and specific safeguards regarding such restriction mechanisms, including the restriction of this right in a justified and proportionate manner.

2. ***Natural persons shall have the right to obtain information on any access to their personal electronic health data through the health professional access service made in the context of healthcare. The information shall be provided without delay and free of charge through electronic health data access services. The information shall include, at least, the following:***

(a) the healthcare provider or other individuals who accessed the personal electronic health data;

(b) the date and time of access;

(c) the personal electronic health data that was accessed.

3. The Commission shall, by means of implementing acts, determine the requirements for the technical implementation of the rights set out in this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

Article 8F

Right of natural person to object

1. Member States laws may provide that natural persons have the right to object to the access to their personal electronic health data registered in an EHR system through the electronic health data access services referred to in Articles 7B and 8G. In such cases, Member States should ensure that the exercise of this right is reversible.

If a Member State provides for such a right, it shall establish the rules and specific safeguards regarding such objection mechanism. In particular, Member States may allow for the possibility of the healthcare provider or health professional to get access to the personal electronic health data in cases where processing is necessary in order to protect the vital interests of the data subject or of another natural person as referred to in Article 9(2)(c) of the Regulation (EU 2016/679, even if the patient has exercised the right to object.

2. With regard to cross-border access to personal electronic health data referred to in Article 5, Member States laws may provide for natural persons to have the right to object to their personal electronic health data being made available for cross-border access and exchange through the cross-border infrastructure as referred to in Article 12.

If a Member State provides for such a right, it shall establish the rules and specific safeguards regarding such objection mechanism.

Article 8G

Electronic health data access services for natural persons and their representatives

1. Member States shall ensure that one or more electronic health data access services at national, regional or local level are established, enabling natural persons access to their personal electronic health data and the exercise of rights referred to in Articles 8A to 8F.

2. Member States shall ensure that one or more proxy services are established as a functionality of health data access services enabling natural persons to:

(a) authorise other natural persons of their choice to access their personal electronic health data, or part thereof, on their behalf; and;

(b) have access to the personal electronic health data of natural persons whose affairs they administer as legal guardians

in an equivalent manner as they access their personal electronic health data and to manage those authorisations.

The proxy services shall provide authorisations free of charge, electronically or on paper.

Member States shall establish rules regarding such authorisations, actions of guardians and representatives. The proxy services shall be interoperable among Member States.

(2a) For the purposes of paragraph 2, the Commission shall, by means of implementing acts, lay down the technical specifications to ensure the interoperability of the proxy services of the Member States. These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

3. The access to the electronic health data services as referred to in paragraph 1 shall be free of charge for the natural persons and their representatives.

Article 9

Identification management

1. Where a natural person uses ~~telemedicine services or~~ personal health data access services referred to in Article ~~3(5), point (a)~~ ***8G***, that natural person shall have the right to identify electronically using any electronic identification means which is recognised pursuant to Article 6 of Regulation (EU) No 910/2014. ***Member States may provide complementary mechanisms to ensure appropriate identity matching in cross-border situations.***

2. The Commission shall, by means of implementing acts, determine the requirements for the interoperable, cross-border identification and authentication mechanism for natural persons and health professionals~~, in accordance with Regulation (EU) No 910/2014 as amended by [COM(2021) 281 final].~~ The mechanism shall facilitate the transferability of ***personal*** electronic health data in a cross-border context. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

3. The Commission shall implement services required by the interoperable, cross-border identification and authentication mechanism referred to in paragraph 2 of this Article at Union level, as part of the cross-border ~~digital health~~ infrastructure referred to in Article 12(3).

4. The ~~digital health authorities~~ ***Member States*** and the Commission shall implement the cross-border identification and authentication mechanism at ~~Union and~~ Member States' ***and Union*** -level, respectively.

Article 9A

Compensation for making personal electronic health data available

By way of derogation from Article 9 of Regulation […] [Data Act COM/2022/68 final], where personal electronic health data is transmitted in accordance with Article 8D, the receiving provider shall not be required to compensate the transmitting provider for making electronic heath data available.

SECTION 1A

GOVERNANCE FOR PRIMARY USE OF ELECTRONIC HEALTH DATA

Article 10

Digital health authority

1. Each Member State shall designate ***one or more*** ~~a~~ digital health ~~authority~~ ***authorities*** responsible for the implementation and enforcement of this Chapter at national level. The Member State shall ~~communicate the~~ ***inform the Commission of the*** identity of the digital health authority ~~to the Commission~~ by the date of application of this Regulation. Where a ***Member State*** designated ***more than one*** digital health authority ~~is an entity consisting~~ ***and where the digital health authority consists*** of multiple organisations, the Member State shall communicate to the Commission a description of the separation of tasks between the organisations. The Commission shall make this information publicly available.

2. ~~Each~~ ***The*** digital health authority shall be entrusted with the following tasks:

   (a) ensure the implementation of the rights and obligations provided for in Chapters II and III by adopting necessary national, regional or local technical solutions and by establishing relevant rules and mechanisms;

   (b) ensure that complete and up to date information about the implementation of rights and obligations provided for in in Chapters II and III is made readily available to natural persons, health professionals and healthcare providers;

   (c) in the implementation of technical solutions referred to in point (a), enforce their compliance with Chapter II, III and Annex II;

   (d) contribute, at Union level, to the development of technical solutions enabling natural persons and health professionals to exercise their rights and obligations set out in this Chapter;

(e) facilitate for persons with disabilities to exercise their rights listed in Article 3 of this Regulation in accordance with Directive (EU) 2019/882 of the European Parliament and of the Council[17].

(f) supervise the national contact points for digital health and cooperate with other digital health authorities and the Commission on further development of MyHealth@EU;

(g) ensure the implementation, at national level, of the European electronic health record exchange format, in cooperation with national authorities and stakeholders;

(h) contribute, at Union level, to the development of the European electronic health record exchange format and to the elaboration of common specifications addressing interoperability, security, safety or fundamental right concerns in accordance with Article 23 and of the specifications of the EU database for EHR systems and wellness applications referred to in Article 32;

(i) where applicable, perform market surveillance activities in accordance with Article 28, while ensuring that any conflict of interest is avoided;

(j) build national capacity for implementing interoperability and security of the primary use of electronic health data and participate in information exchanges and capacity building activities at Union level;

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

(l) cooperate with market surveillance authorities, participate in the activities related to handling of risks posed by EHR systems and of serious incidents and supervise the implementation of corrective actions in accordance with Article 29;

---

17 Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance) (OJ L 151, 7.6.2019, p. 70)

(m) cooperate with other relevant entities and bodies at national or Union level, to ensure interoperability, data portability and security of electronic health data, as well as with stakeholders representatives, including patients' representatives, healthcare providers, health professionals~~,~~ ***and*** industry associations;

(n) cooperate with supervisory authorities in accordance with Regulation (EU) 910/2014, Regulation (EU) 2016/679 ~~and~~ **,** Directive (EU) ~~2016/1148 of the European Parliament and of the Council~~[18] ***2022/2555 and*** with other relevant authorities, including those competent for cybersecurity, electronic identification~~, the European Artificial Intelligence Board, the Medical Device Coordination Group, the European Data Innovation Board and the competent authorities under Regulation […] [Data Act COM/2022/68 final];~~**;**

~~(o) draw up, in collaboration where relevant with market surveillance authorities, an annual activity report, which shall contain a comprehensive overview of its activities. The report shall be transmitted to the Commission. The annual activity report shall follow a structure that is agreed at Union level within EHDS Board, to support benchmarking pursuant to Article 59. The report shall contain at least information concerning:~~

~~(i) measures taken to implement this Regulation;~~

~~(ii) percentage of natural persons having access to different data categories of their electronic health records;~~

~~(iii) information on the handling of requests from natural persons on the exercise of their rights pursuant to this Regulation;~~

~~(iv) number of healthcare providers of different types, including pharmacies, hospitals and other points of care, connected to MyHealth@EU calculated a) in absolute terms, b) as share of all healthcare providers of the same type and c) as share of natural persons that can use the services;~~

~~18~~ ~~Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).~~

~~(v) volumes of electronic health data of different categories shared across borders through MyHealth@EU;~~

~~(vi) level of natural person satisfaction with MyHealth@EU services;~~

~~(vii) number of certified EHR systems and labelled wellness applications enrolled in the EU database;~~

~~(viii) number of non-compliance cases with the mandatory requirements;~~

~~(ix) a description of its activities carried out in relation to engagement with and consultation of relevant stakeholders, including representatives of natural persons, patient organisations, health professionals, researchers, and ethical committees;~~

~~(x) information on cooperation with other competent bodies in particular in the area of data protection, cybersecurity, and artificial intelligence.~~

~~3. The Commission is empowered to adopt delegated acts in accordance with Article 67 to supplement this Regulation by entrusting the digital health authorities with additional tasks necessary to carry out the missions conferred on them by this Regulation and to modify the content of the annual report.~~

~~4. Each Member State shall ensure that each digital health authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers.~~

5. In the performance of its tasks, the digital health authority shall ~~actively cooperate with stakeholders' representatives, including patients' representatives. Members of the digital health authority shall~~ avoid any conflicts of interest.

Article 10A

Reporting by digital health authority

1. The digital health authority shall publish a biennial activity report, which shall contain a comprehensive overview of its activities. If a Member State designates more than one digital health authority, one of them shall be responsible for the report and request

necessary information from the other digital health authorities. The biennial activity report shall follow a structure that is agreed at Union level within EHDS Board. The report shall contain at least information concerning:

(a) measures taken to implement this Regulation;

(b) percentage of natural persons having access to different data categories of their electronic health records;

(c) formation on the handling of requests from natural persons on the exercise of their rights pursuant to this Regulation;

(d) number of healthcare providers of different types, including pharmacies, hospitals and other points of care, connected to MyHealth@EU calculated a) in absolute terms, b) as share of all healthcare providers of the same type and c) as share of natural persons that can use the services;

(e) volumes of electronic health data of different categories shared across borders through MyHealth@EU;

2. The report shall be drawn up in collaboration with market surveillance authorities as referred to in Article 28 of this Regulation, where relevant.

3. The report shall be sent to the Commission and the EHDS Board within 6 months after the end date of the 2 year reporting period.

Article 11

Right to lodge a complaint with a digital health authority

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the digital health authority***, related to the provisions in this Chapter***. Where the complaint concerns the rights of natural persons pursuant to ~~Article 3~~***Articles 8A to 8F*** of this Regulation, the digital health authority shall ~~inform~~ ***transmit the complaint to*** the supervisory authorities under Regulation (EU) 2016/679 ***and shall consult and cooperate with them in the handling of such complaints***.

2. The ***competent*** digital health authority with which the complaint has been lodged shall inform the complainant***, in accordance with national law,*** of the progress of the proceedings and of the decision taken.

3. Digital health authorities ***in different Member States*** shall cooperate to handle and resolve complaints ***related to the cross-border exchange and access to personal electronic health data***, including by exchanging all relevant information by electronic means, without undue delay.

Article 11A

Relationship with data protection supervisory authorities

1. The supervisory authority or authorities responsible for monitoring and enforcement of Regulation (EU) 2016/679 shall also be competent for monitoring and enforcement of the application of Articles 8A to 8F, in accordance with the relevant provisions of Regulation (EU) 2016/679. They shall be competent to impose administrative fines up to the amount referred to in Article 83(5) of that Regulation. Those supervisory authorities and the digital health authorities referred to in Article 10 of this Regulation shall, where relevant, cooperate in the enforcement of this Regulation, within the remit of their respective competences.

SECTION 2

CROSS-BORDER INFRASTRUCTURE FOR PRIMARY USE OF *PERSONAL* ELECTRONIC HEALTH DATA

Article 12

MyHealth@EU

1. The Commission shall establish a central ***and interoperability*** platform for digital health***, MyHealth@EU,*** to provide services to support and facilitate the exchange of ***personal*** electronic health data between national contact points for digital health of the Member States.

2. Each Member State shall designate one national contact point for digital health***. The national contact point shall be an organisational and technical gateway for the provision of cross-border digital health information services in the context of healthcare of personal electronic health data, enabling and ensuring*** ~~to ensure~~ the connection to all other national contact points for digital health and to the central platform for digital health ***in cross-border infrastructure MyHealth@EU***. Where a designated national contact point is an entity consisting of multiple organisations responsible for implementing different services, the Member State shall communicate to the Commission a description of the separation of tasks between the organisations. ~~The national contact point for digital health shall be considered an authorised participant in the infrastructure~~. Each Member State shall ~~communicate~~ ***inform of*** the identity of its national contact point to the Commission by [the date of application of this Regulation]. Such contact point may be established within the digital health authority established by Article 10 of this Regulation. Member States shall ~~communicate to~~ ***inform*** the Commission ***of*** any subsequent modification of the identity of those contact points. The Commission and the Member States shall make this information publicly available.

3. Each national contact point for digital health shall enable the exchange of the personal electronic health data referred to in Article ~~5 with all~~***5(1) with national contact points in*** other ~~national contact points~~***Member States through MyHealth@EU***. The exchange shall be based on the European electronic health record exchange format. ***National contact point for digital health may enable the exchange of additional categories of electronic health data referred to in Article 5(1A) insofar as Member State law has provided for these additional categories of personal electronic health to be accessed and exchanged, according to article 5 (1A).***4. The Commission shall, by means of implementing acts, adopt the necessary measures for the technical development of MyHealth@EU, detailed rules concerning the security, confidentiality and protection of ***personal*** electronic health data and the conditions and compliance checks necessary to join and remain connected to MyHealth@EU and conditions for temporary or definitive exclusion from MyHealth@EU. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

5. Member States shall ensure connection of all healthcare providers to their national contact points for digital health***. Member States*** ~~and~~ shall ensure that ***connected healthcare***

providers ~~those connected~~ are enabled to perform two-way exchange of electronic health data with the national contact point for digital health.

6. Member States shall ensure that pharmacies operating on their territories~~, including online pharmacies,~~ are enabled to dispense electronic prescriptions issued by other Member States, under the conditions laid down in Article 11 of Directive 2011/24/EU. The pharmacies shall access and accept electronic prescriptions transmitted to them from other Member States through MyHealth@EU. Following dispensation of medicinal products based on an electronic prescription from another Member State, pharmacies shall report the dispensation to the Member State that issued the prescription, through MyHealth@EU.

7. The national contact points for digital health shall act as ~~joint~~ controllers of the ***personal*** electronic health data communicated through 'MyHealth@EU' for the processing operations in which they are involved. The Commission shall act as processor.

8. ***By means of implementing acts,*** the Commission shall~~, by means of implementing acts, allocate responsibilities among controllers and as regards~~ ***lay down the rules regarding the requirements of cybersecurity, technical interoperability, semantic interoperability, operations and service management in relation to the processing by*** the processor referred to in paragraph 7 of this Article ***and its responsibilities towards the controllers***, in accordance with Chapter IV of Regulation (EU) 2016/679 ***and of Regulation (EU) 2018/1725***. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

9. ***The national contact points referred to in paragraph 2 shall be authorised participants in MyHealth@EU, provided that they fulfil the conditions to join and to remain connected to MyHealth@EU as laid down pursuant to paragraph 4.*** The approval for individual authorised participants to join MyHealth@EU for different services, or to disconnect a participant shall be issued by the ~~Joint Controllership group~~***Commission*** , based on the results of the compliance checks ***performed by the Commission***. ***Subject to the outcome of the compliance check, the Commission shall, by means of implementing act, take decisions to connect individual authorised participants to join the infrastructure or to disconnect them. These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).***

Article 13

Supplementary cross-border digital health services and infrastructures

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

2. The Commission and Member States may facilitate the exchange of ***personal*** electronic health data with other infrastructures, such as the Clinical Patient Management System or other services or infrastructures in the health, care or social security fields which may become authorised participants to MyHealth@EU. The Commission shall, by means of implementing acts, set out the technical aspects of such exchanges. Those implementing acts shall be adopted in accordance with the advisory ***examination*** procedure referred to in Article 68(2). ~~The~~ The connection of another infrastructure to the central platform for digital health***, as well as its disconnection,*** shall be subject to a decision***, by means of implementing acts,*** of the ~~joint controllership group for MyHealth@EU~~***Commission, based on the result of the compliance checks of the technical aspects of such exchanges as referred to in subparagraph 1. Those implementing acts shall be adopted in accordance with the examination procedure*** referred to in Article ~~66~~***68(2)***.

3. ~~Member States and the Commission shall seek to ensure interoperability of MyHealth@EU with technological systems~~***A national contact point of a third country or a system*** established at ***an*** international level ~~for the exchange of electronic health data. The Commission may adopt an implementing act establishing that a national contact point of a third country or a system established at an international level is compliant with requirements of MyHealth@EU for the purposes of the electronic health data exchange. Before adopting such an implementing act, a compliance check of the national contact~~

~~point~~***may become an authorised participant in MyHealth@EU provided that they fulfil the requirements of MyHealth@EU for the purposes of the personal electronic health data exchange as referred to in Article 12, that the transfer stemming from such connection complies with the rules in Chapter V of Regulation (EU) 2016/679, and that the requirements concerning the legal, organizational, operational, semantic, technical and cybersecurity measures are equivalent to those applicable to*** ~~of the third country or of the system established at an international level~~ ***Member States in the operation of MyHealth@EU services. The requirements in subparagraph 1*** shall be ~~performed under the control of~~ ***verified through compliance check performed by*** the Commission.

~~The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the procedure referred to in Article 68. The connection of~~ ***Based on the outcome of the compliance check, the Commission may, by means of implementing act, take the decision to connect as well as to disconnect*** the national contact point of the third country or of the system established at an international level to ~~the central platform for digital health, as well as the decision to be disconnected~~ ***MyHealth@EU. Member States national security interests shall be taken into account. These implementing acts*** shall be ~~subject to a decision of the joint controllership group for MyHealth@EU~~ ***adopted in accordance with the examination procedure*** referred to in Article ~~66~~***68(2)***.

The Commission shall ~~make~~ ***maintain*** the list of ~~implementing acts adopted~~ ***national contact points of a third country or of systems established at an international level connected to MyHealth@EU*** pursuant to this paragraph ***and shall make it*** publicly available.

CHAPTER III

EHR systems and wellness applications

SECTION 1

SCOPE AND GENERAL PROVISIONS FOR EHR SYSTEMS

Article 13A

EHR harmonised components

1. ***EHR systems shall include a 'European interoperability component for EHR systems' and a 'European logging component for EHR systems' (the 'harmonised components'), in accordance with the provisions laid down in this Chapter.***

2. ***This Chapter shall not apply to general purpose software used in a healthcare environment.***

Article 13B

Placing on the market and putting into service

1. ***EHR systems as referred to in Article 13A(1) may be placed on the market or put into service only if they comply with the provisions laid down in this Chapter.***

2. ***EHR systems that are manufactured and used within health institutions established in the Union and EHR systems offered as a service within the meaning of Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council[19] to a natural or legal person established in the Union shall be considered as having been put into service.***

---

19 ***[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).***

3. ***Member States may not, for considerations relating to aspects concerning the harmonised components regulated by this Regulation, prohibit or restrict the placing on the market of EHR systems which comply with this Regulation.***

Article 14

*Interplay with legislation governing medical devices**, in vitro diagnostic medical devices and** AI systems*

~~1.~~ ~~EHR systems intended by their manufacturer for primary use of priority categories of electronic health data referred to in Article 5 shall be subject to the provisions laid down in this Chapter.~~

~~2.~~ ~~This Chapter shall not apply to general software used in a healthcare environment.~~

~~3~~***1***. Manufacturers of medical devices as defined in Article 2(1) of Regulation (EU) 2017/745 ***and manufacturers of in vitro diagnostic medical devices as defined in Article 2(2) of Regulation (EU) 2017/746*** that claim interoperability of those medical devices with ***the harmonised components of*** EHR systems shall prove compliance with the essential requirements on ***the European*** interoperability ***component for EHR systems and the European logging component for EHR systems,*** laid down in Section 2 of Annex II of this Regulation. Article 23 of this Chapter shall be applicable to those medical devices.

~~4~~***2***. Providers of high-risk AI systems as defined in Article 6 of Regulation […] [AI act COM/2021/206 final], which does not fall -within the scope of Regulation (EU) 2017/745, that claim interoperability of those AI systems with ***the harmonised components of*** EHR systems will need to prove compliance with the essential requirements on ***the European*** interoperability ***component for EHR systems and the European logging component for EHR systems, as further*** laid down in Section 2 of Annex II of this Regulation. Article 23 of this Chapter shall be applicable to those high-risk AI systems.

~~5.~~ ~~Member States may maintain or define specific rules for the procurement, reimbursement or financing of EHR systems in the context of the organisation, delivery or financing of healthcare services.~~

~~*Article 15*~~

~~*Placing on the market and putting into service*~~

~~1. EHR systems may be placed on the market or put into service only if they comply with the provisions laid down in this Chapter.~~

~~2. EHR systems that are manufactured and used within health institutions established in the Union and EHR systems offered as a service within the meaning of Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council[20] to a natural or legal person established in the Union shall be considered as having been put into service.~~

Article 16

Claims

In the information sheet, instructions for use or other information accompanying EHR systems, and in the advertising of EHR systems, it shall be prohibited to use text, names, trademarks, pictures and figurative or other signs that may mislead the user with regard to its intended purpose, interoperability and security by:

(a) ascribing functions and properties to the EHR system which it does not have;

(b) failing to inform the user of likely limitations related to interoperability or security features of the EHR system in relation to its intended purpose;

(c) suggesting uses for the EHR system other than those stated in the technical documentation to form part of the intended purpose.

~~20 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).~~

Article 16A

Procurement, reimbursement and financing of EHR systems

Member States may maintain or define requirements for the procurement, reimbursement or financing of EHR systems in the context of the organisation, delivery or financing of healthcare services provided that such requirements are compliant with Union law and do not affect the harmonised components

SECTION 2

OBLIGATIONS OF ECONOMIC OPERATORS WITH REGARD TO EHR SYSTEMS

Article 17

Obligations of manufacturers of EHR systems

1. Manufacturers of EHR systems shall ***with regard to the harmonised components referred to in Article 13A(1)***:

(a) ensure that ***these harmonised components of*** their EHR systems are in conformity with the essential requirements laid down in Annex II and with the common specifications in accordance with Article 23;

(ab) ensure that these components of their EHR systems are not impeded or negatively affected by other components of the same EHR system;

(b) draw up the technical documentation of their EHR systems ***for these harmonised components*** in accordance with Article 24;

(c) ensure that ***these harmonised components of*** their EHR systems are accompanied, free of charge for the user, by the information sheet provided for in Article 25 and clear and complete instructions for use;

(d) draw up an EU declaration of conformity- as referred to in Article 26;

(e) affix the CE marking ***for those harmonised components*** in accordance with Article 27;

(f) comply with the registration obligations ***for these harmonised components*** in Article 32;

(g) take without undue delay any necessary corrective action in respect of ***these harmonised components of*** their EHR systems which are not in conformity with the essential requirements laid down in Annex II, or recall or withdraw such systems;

(h) inform the distributors of their EHR systems and, where applicable, the authorised representative***, importers and the users*** ~~and importers~~ of any ***mandatory preventive maintenance and its frequency,*** corrective action, recall or withdrawal ***in relation to these harmonised components***;

(i) inform the market surveillance authorities of the Member States in which they made their EHR systems available or put them into service of the non-conformity and of any corrective action taken***, including the timetable for implementation, when those harmonised components of their EHR system have been brought into conformity and been recalled or withdrawn***;

(j) upon request of a market surveillance authority, provide it with all the information and documentation necessary to demonstrate the conformity of ***these harmonised components of*** their EHR system with the essential requirements laid down in Annex II.

(k) cooperate with market surveillance authorities, at their request, on any action taken to bring ***these harmonised components of*** their EHR systems in conformity with the essential requirements laid down in Annex II.

2. Manufacturers of EHR systems shall ensure that procedures are in place to ensure that the design, development and deployment of ***the components of*** an EHR system ***defined in Article 2(2)(nc)-(nd)*** continues to comply with the essential requirements laid down in Annex II and the common specifications referred to in Article 23. ~~.~~ Changes in EHR system design or characteristics ***with regard to these harmonised components*** shall be adequately taken into account and reflected in the technical documentation.

3. Manufacturers of EHR systems shall keep the technical documentation and the EU declaration of conformity for 10 years after the last ***components of the*** EHR system

defined in Article 2(2)(nc)-(nd) covered by the EU declaration of conformity ~~has~~ ***have*** been placed on the market.

Article 18

Authorised representatives

1. Prior to making an EHR system available on the Union market, a manufacturer of an EHR system established outside of the Union shall, by written mandate, appoint an authorised representative which is established in the Union.

2. An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:

   (a) keep the EU declaration of conformity and the technical documentation at the disposal of market surveillance authorities for the period referred to in Article 17(3);

   (b) further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of an EHR system with ~~the~~ essential requirements laid down in Annex II ***as well as the common specifications in accordance with Article 23***;

   (c) cooperate with the market surveillance authorities, at their request, on any corrective action taken in relation to the ***components of the*** EHR systems ***defined in Article 2(2)(nc)-(nd)*** covered by their mandate.

(d) terminate the mandate if the manufacturer acts contrary to its obligations under this Regulation.

(e) ensure that the technical documentation can be made available to those authorities, upon request.

Article 19

Obligations of importers

1. Importers shall place on the Union market only EHR systems which are in conformity with the essential requirements ***in relation to the harmonised components of EHR systems as*** laid down in Annex II ***as well as the common specifications in accordance with Article 23***.

2. Before making an EHR system available on the market, importers shall ensure that:

   (a) the manufacturer has drawn up the technical documentation and the EU declaration of conformity;

   (b) the EHR system bears the CE marking of conformity;

   (c) the EHR system is accompanied by the information sheet referred to in Article 25 and appropriate instructions for use***, including maintenance actions***.

3. Importers shall indicate their name, registered trade name or registered trade mark and the address at which they can be contacted in a document accompanying the EHR system.

4. Importers shall ensure that, while an EHR system is under their responsibility, the EHR system is not altered in such a way that its conformity with the essential requirements laid down in Annex II is jeopardised.

5. Where an importer considers or has reason to believe that an EHR system is not in conformity with the essential requirements in Annex II, it shall not make that system available on the market until that system has been brought into conformity. The importer shall inform without undue delay the manufacturer of such EHR system***, the users*** and the market surveillance authorities of the Member State in which it made the EHR system available ***on the market where this situation occurs***, to that effect.

6. Importers shall keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities for the period referred to in Article 17(3) ~~and ensure that the technical documentation can be made available to those authorities, upon request~~.

7. Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation necessary to demonstrate the conformity of ***harmonised components of*** an EHR system in the official language of the Member State where the market surveillance authority is located. They shall cooperate with that authority, at its request, on any action taken to bring their EHR systems in conformity with the essential requirements ***in relation to those components as*** laid down in Annex II.

Article 20

Obligations of distributors

1. Before making an EHR system available on the market, distributors shall verify that: ***with regard to the harmonised components of EHR systems***

   (a) the manufacturer has drawn up the EU declaration of conformity;

   (b) the EHR system bears the CE marking of conformity;

   (c) the EHR system is accompanied by the information sheet referred to in Article 25 and appropriate instructions for use;

   (d) where applicable, the importer has complied with the requirements set out in Article 19(3).

2. Distributors shall ensure that, while an EHR system is under their responsibility, the EHR system is not altered in such a way that its conformity with the essential requirements ***with regards to the EHR harmonised components*** laid down in Annex II is jeopardised.

3. Where a distributor considers or has reason to believe that an EHR system is not in conformity with the essential requirements laid down in Annex II, it shall not make the EHR system available on the market until it has been brought into conformity ***with the harmonised components of EHR systems***. Furthermore, the distributor shall inform without undue delay the manufacturer or the importer ***and the users***, as well as the market surveillance authorities of the Member states where the EHR system has been made available on the market, to that effect.

4. Distributors shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation necessary to demonstrate the conformity of an EHR system ***with regard to the harmonised components of EHR systems***. They shall cooperate with that authority, at its request, on any action taken to bring their EHR systems in conformity with the essential requirements laid down in Annex II ***in relation to those two components***.

Article 21

Cases in which obligations of manufacturers of an EHR system apply to importers and distributors

An importer or ***a*** distributor shall be considered a manufacturer for the purposes of this Regulation and shall be subject to the obligations laid down in Article 17, where they made an EHR system available on the market under their own name or trademark or modify an EHR system already placed on the market in such a way that conformity with the applicable requirements may be affected.

Article 22

Identification of economic operators

Economic operators shall, on request, identify the following to the market surveillance authorities, for 10 years after the last EHR system covered by the EU declaration of conformity has been placed on the market:

(a) any economic operator who has supplied them with an EHR system;

(b) any economic operator to whom they have supplied an EHR system.

SECTION 3

CONFORMITY OF THE EHR SYSTEM

Article 23

Common specifications

1. The Commission shall, by means of implementing acts, adopt common specifications in respect of the essential requirements set out in Annex II, including a time limit for implementing those common specifications. ***Those common specifications shall be based on existing harmonised standards for the harmonised components of EHR systems, where applicable.*** Where relevant, the common specifications shall take into account the specificities ***and verify compatibility with sectorial legislation and harmonised standards*** of medical devices and high risk AI systems referred to in paragraphs ~~3 and 4~~***1 and 2*** of Article 14***, including the state-of-the-art standards for health informatics and the European electronic health record exchange format***.

   Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

2. The common specifications referred to in paragraph 1 shall include the following elements:

   (a) scope;

   (b) applicability to different categories of EHR systems or functions included in them;

   (c) version;

   (d) validity period;

   (e) normative part;

   (f) explanatory part, including any relevant implementation guidelines.

3. The common specifications may include elements related to the following:

(a) datasets containing electronic health data and defining structures, such as data fields and data groups for the representation of clinical content and other parts of the electronic health data;

(b) coding systems and values to be used in datasets containing electronic health data**,** ***taking due account of both the future harmonisation of terminologies and their compatibility with existing national terminologies***;

(c) other requirements related to data quality, such as the completeness and accuracy of electronic health data;

(d) technical specifications, standards and profiles for the exchange of electronic health data;

(e) requirements and principles related to security, confidentiality, integrity, patient safety and protection of electronic health data;

(f) specifications and requirements related to identification management and the use of electronic identification.

4. EHR systems, medical devices***, in vitro diagnostic medical devices*** and high risk AI systems referred to in ***Articles 13A and*** 14 that are in conformity with the common specifications referred to in paragraph 1 shall be considered to be in conformity with the essential requirements covered by those specifications or parts thereof, set out in Annex II covered by those common specifications or the relevant parts of those common specifications.

5. Where common specifications covering interoperability and security requirements of EHR systems affect medical devices***, in vitro diagnostic medical devices*** or high-risk AI systems falling under other acts, such as Regulations (EU) 2017/745 ***and (EU) 2017/746*** or […] [AI Act COM/2021/206 final], the ***Commission shall ensure that the*** adoption of those common specifications ***shall have been*** ~~may be~~ preceded by a consultation with the Medical Devices Coordination Group (MDCG) referred to in Article 103 of Regulation (EU) 2017/745 or the European Artificial Intelligence Board referred to in Article 56 of Regulation […] [AI Act COM/2021/206 final], as applicable.

6. Where common specifications covering interoperability and security requirements of medical devices***, in vitro diagnostic medical devices*** or high-risk AI systems falling under other acts such as ***Regulations*** (EU) 2017/745 ***and (EU) 2017/746*** or Regulation […] [AI Act COM/2021/206 final], impact EHR systems, the ***Commission shall ensure that the*** adoption of those common specifications shall ~~be~~***have been*** preceded by a consultation with the EHDS Board~~, especially its subgroup for Chapters II and III of this Regulation~~.

Article 24

Technical documentation

1. The technical documentation shall be drawn up before the EHR system is placed on the market or put into service and shall be kept up-to-date.

2. The technical documentation shall be drawn up in such a way as to demonstrate that the EHR system complies with the essential requirements laid down in Annex II and provide market surveillance authorities with all the necessary information to assess the conformity of the EHR system with those requirements. It shall contain, at a minimum, the elements set out in Annex III.

3. The technical documentation shall be drawn up in one of the official languages of the Union. Following a reasoned request from the market surveillance authority of a Member State, the manufacturer shall provide a translation of the relevant parts of the technical documentation into the official language of that Member State.

4. When a market surveillance authority requests the technical documentation or a translation of parts thereof from a manufacturer, it shall set a deadline of 30 days for receipt of such documentation or translation, unless a shorter deadline is justified because of a serious and immediate risk. If the manufacturer does not comply with the requirements of paragraphs 1, 2 and 3, the market surveillance authority may require it to have a test performed by an independent body at its own expense within a specified period in order to verify the conformity with the essential requirements laid down in Annex II and the common specifications referred to in Article 23.

Article 25

Information sheet accompanying the EHR system

1. ***The harmonised components of*** EHR systems shall be accompanied by an information sheet that includes concise, complete, correct and clear information that is relevant, accessible and comprehensible to users.

2. The information sheet referred to in paragraph 1 shall specify:

   (a) the identity, registered trade name or registered trademark, and the contact details of the manufacturer and, where applicable, of its authorised representative;

   (b) the name and version of the EHR system and date of its release;

   (c) its intended purpose;

   (d) the categories of electronic health data that the EHR system has been designed to process;

   (e) the standards, formats and specifications and versions thereof supported by the EHR system.

3. ~~The Commission is empowered to adopt delegated acts in accordance with Article 67 to supplement this Regulation by allowing~~ ***As an alternative to supplying the information sheet referred to in paragraph 1 with the EHR system,*** manufacturers ~~to~~ ***may*** enter the information referred to in paragraph 2 into the EU database ~~of EHR systems and wellness applications~~ referred to in Article 32~~, as an alternative to supplying the information sheet referred to in paragraph 1 with the EHR system.~~.

Article 26

EU declaration of conformity

1. The EU declaration of conformity shall state that the manufacturer of the EHR system has demonstrated that the essential requirements laid down in Annex II have been fulfilled.

2. Where EHR systems are subject to other Union legislation in respect of aspects not covered by this Regulation, which also requires an EU declaration of conformity by the manufacturer that fulfilment of the requirements of that legislation has been demonstrated, a single EU declaration of conformity shall be drawn up in respect of all Union acts applicable to the EHR system. The declaration shall contain all the information required for the identification of the Union legislation to which the declaration relates.

3. The EU declaration of conformity shall~~, as a minimum,~~ contain the information set out in Annex IV and shall be translated into one or more official Union languages determined by the Member State(s) in which the EHR system is made available.

4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the conformity of the EHR system ***when it is placed on the market or put into service***.

Article 26A

European digital testing environment

1. The Commission shall set up and operate a European digital testing environment to support the assessment of harmonised components of EHR systems

2. Member States may set up digital testing environment to support the assessment of harmonised components of EHR systems. Such environments shall comply with the common specifications for digital testing environments laid down pursuant paragraph 4 and shall be communicated to the Commission.

3. Manufacturers shall use the testing environments mentioned in paragraphs 1 and 2 as a supporting element for the assessment of harmonised components of EHR systems. The

results of the test shall be included in the documentation referred to in Article 24. The conformity to this regulation shall be presumed in respect of the elements tested with positive results.

4. The Commission shall, by means of implementing acts, lay down the common specifications for digital testing environments. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

Article 27

CE marking

1. The CE marking shall be affixed visibly, legibly and indelibly to the accompanying documents of the EHR system and, where applicable, to the packaging.

2. The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) 765/2008 of the European Parliament and of the Council[21].

Article 27A

National requirements and reporting to the Commission

1. Member States may introduce national requirements for EHR systems and provisions on their conformity assessment in relation to aspects other than the harmonised components of EHR systems.

2. National requirements or provisions on assessment referred to in paragraph 1 shall not impede or adversely interact with the harmonised components of EHR systems.

3. When Member States adopt regulations in accordance with paragraph 1, , they shall inform thereabout the Commission

[21] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

SECTION 4

MARKET SURVEILLANCE OF EHR SYSTEMS

Article 28

Market surveillance authorities

1. Regulation (EU) 2019/1020 shall apply to EHR systems ***in relation to the harmonised components of EHR systems*** covered by Chapter III of this Regulation.

2. Member States shall designate the market surveillance authority or authorities responsible for the implementation of this Chapter. They shall entrust their market surveillance authorities with the powers, resources, equipment and knowledge necessary for the proper performance of their tasks pursuant to this Regulation. ***Market surveillance authorities shall take the measures referred to in Article 16 of Regulation (EU) 2019/1020 to enforce this Chapter.*** Member States shall communicate the identity of the market surveillance authorities to the Commission ~~which shall publish a list of those authorities~~***The Commission and the Member States shall make this information publicly available***.

3. Market surveillance authorities designated pursuant to this Article may be the digital health authorities designated pursuant to Article 10. Where a digital health authority carries out tasks of market surveillance authority, ***Member States shall ensure that*** any conflict of interest ~~shall be~~ ***is*** avoided.

4. Market surveillance authorities shall report to the Commission on a ~~regular~~ ***yearly*** basis the outcomes of relevant market surveillance activities.

5. The market surveillance authorities of the Member States shall cooperate with each other and with the Commission. The Commission shall provide for the organisation of exchanges of information necessary to that effect.

6. For medical devices***, in vitro diagnostic medical devices*** or high-risk AI systems referred to in Article 14 (3) and (4), the responsible authorities for market surveillance shall be

those referred to in Article 93 of Regulation (EU) 2017/745***, Article 88 of Regulation (EU) 2017/746*** or Article 59 of Regulation […] [AI act COM/2021/206 final], as applicable.

Article 29

Handling of risks posed by EHR systems and of serious incidents

1. Where a market surveillance authority finds that an ***any of the harmonised components of EHR systems*** ~~EHR system~~ presents a risk to the health or safety of natural persons***, to the security of the EHR system*** or to other aspects of public interest protection, it shall require the manufacturer of the EHR system concerned, its authorised representative and all other relevant economic operators to take all appropriate measures to ensure that the EHR system concerned no longer presents that risk when placed on the market***. The measures may include withdrawal of*** ~~to withdraw~~ the EHR system from the market or to recall it within a reasonable period.

2. The economic operator referred to in paragraph 1 shall ensure that corrective action is taken in respect of all the EHR systems ***with regard to the harmonised components*** concerned that it has placed on market throughout the Union.

3. The market surveillance authority shall immediately inform the Commission and the market surveillance authorities of other Member States of the measures ordered pursuant to paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the EHR system concerned, the origin and the supply chain of the EHR system, the nature of the risk involved and the nature and duration of the national measures taken.

4. Manufacturers of EHR systems placed on the market ***or put into service*** shall report any serious incident involving an EHR system to the market surveillance authorities of the Member States where such serious incident occurred and ***to the market surveillance authorities of the Member States where such EHR systems is placed on the market or put into service. The report shall also contain a description of*** the corrective actions taken or envisaged by the manufacturer. ***Member States may provide for users of EHR systems placed on the market or put into service to report such incidents.***

Such notification shall be made, without prejudice to incident notification requirements under Directive (EU) ~~2016/1148~~***2022/2555*** , immediately after the manufacturer has established a causal link between the EHR system and the serious incident or the reasonable likelihood of such a link, and, in any event, not later than ~~15~~***3*** days after the manufacturer becomes aware of the serious incident involving the EHR system.

5. The market surveillance authorities referred to in paragraph 4 shall inform the other market surveillance authorities, without delay, of the serious incident and the corrective action taken or envisaged by the manufacturer or required of it to minimise the risk of recurrence of the serious incident.

6. Where the tasks of the market surveillance authority are not performed by the digital health authority, it shall cooperate with the digital health authority. It shall inform the digital health authority of any serious incidents and of EHR systems ***in relation to the harmonised components of EHR systems*** presenting a risk, including risks related to interoperability, security and patient safety, and of any corrective action, recall or withdrawal of such EHR systems.

7. Where the market surveillance authority becomes aware that the risk or the incident can entail a personal data breach, as defined in Article 4(12) of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation.

8. For incidents putting at risk patient safety or information security, the market surveillance authorities may take immediate actions and require immediate corrective actions.

Article 30

Handling of non-compliance

1. Where a market surveillance authority makes one of the following findings, it shall require the manufacturer of the EHR system concerned, its authorised representative and all other relevant economic operators***, within a deadline it establishes, to take appropriate measures*** to put an end to the non-compliance concerned:

(a) the ***harmonised components of EHR systems***~~EHR system~~ is not in conformity with ***the*** essential requirements laid down in Annex II;

(b) the technical documentation is either not available or not complete;

(c) the EU declaration of conformity has not been drawn up ***with regard to the harmonised components of EHR systems*** or has not been drawn up correctly;

(d) the CE marking has been affixed in violation of Article 27 or has not been affixed.

2. Where the non-compliance referred to in paragraph 1 persists, the ~~Member State~~ ***market surveillance authority*** concerned shall take all appropriate measures to restrict or prohibit the EHR system being placed on the market or ensure that it is recalled or withdrawn from the market.

SECTION 5

OTHER PROVISIONS ON INTEROPERABILITY

Article 31

~~Voluntary~~ Labelling of wellness applications

1. Where a manufacturer of a wellness application claims interoperability with an EHR system ***in relation to the harmonised components of EHR systems*** and therefore compliance with the essential requirements laid down in Annex II and common specifications in Article 23, such wellness application ~~may~~ ***shall*** be accompanied by a label, clearly indicating its compliance with those requirements. The label shall be issued by the manufacturer of the wellness application.

2. The label shall indicate the following information:

(a) categories of electronic health data for which compliance with essential requirements laid down in Annex II has been confirmed;

(b) reference to common specifications to demonstrate compliance;

(c) validity period of the label.

3. The Commission may, by means of implementing acts, determine the format and content of the label. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

4. The label shall be drawn-up in one or more official languages of the Union or languages determined by the Member State(s) in which the ~~in which the~~ wellness application is placed on the market ***or put into service***.

5. The validity of the label shall not exceed ~~5~~***3*** years.

6. If the wellness application is embedded in a device, the accompanying label shall be placed on the device. ***Two-dimensional, 2D,*** ~~2D~~ barcodes may also be used to display the label.

7. The market surveillance authorities shall check the compliance of wellness applications with the essential requirements laid down in Annex II.

8. Each supplier of a wellness application, for which a label has been issued, shall ensure that the wellness application that is placed on the market or put into service is accompanied with the label for each individual unit, free of charge.

9. Each distributor of a wellness application for which a label has been issued shall make the label available to customers at the point of sale in electronic form or, upon request, in physical form.

10. The requirements of this Article shall not apply to wellness applications which are high-risk AI systems as defined under Regulation […] [AI Act COM/2021/206 final].

SECTION 6

REGISTRATION OF EHR SYSTEM AND WELLNESS APPLICATION

Article 32

EU database for *registration of EHR systems and wellness applications*

1. The Commission shall establish and maintain a publicly available database with information on EHR systems for which an EU declaration of conformity has been issued

pursuant to Article 26 and wellness applications for which a label has been issued pursuant to Article 31.

2. Before placing on the market or putting into service an EHR system referred to in Article 14 or a wellness application referred to in Article 31, the manufacturer of such EHR system or wellness application or, where applicable, its authorised representative shall register the required data into the EU database referred to in paragraph 1.

3. ***Medical devices, in vitro diagnostic*** medical devices or high-risk AI systems referred to in paragraphs ~~3 and 4~~***1 and 2*** of Article 14 of this Regulation shall be registered in the database established pursuant to Regulations (EU) 2017/745**, *(EU) 2017/746*** or […] [AI Act COM/2021/206 final], as applicable. ***In such cases, the information shall also be forwarded to the EU database referred to in paragraph 1.***

4. The Commission is empowered to adopt delegated acts in accordance with Article 67 to determine the list of required data to be registered by the manufacturers of EHR systems and wellness applications pursuant to paragraph 2.

CHAPTER IV

Secondary use of electronic health data

SECTION 1

GENERAL CONDITIONS WITH REGARD TO THE SECONDARY USE OF ELECTRONIC HEALTH DATA

Article 32A

Applicability to health data holders

1. The following categories of health data holders shall be exempted from the obligations incumbent on health data holders laid down in this Chapter:

(a) individual researchers and natural persons;

(b) legal persons that qualify as micro-enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC.

2. Member States may, by virtue of national legislation, provide that the obligations of health data holders laid down in this Chapter shall apply to the health data holders referred to in paragraph 1 which fall under their jurisdiction.

3. Member States may provide, by virtue of national legislation, that the obligations of health data holders laid down in this Chapter shall not apply to health data holders in the care sector,), which fall under their jurisdiction, in order to avoid a disproportionate burden on the entities pertaining to this sector.

4. Member States may, by virtue of national legislation, provide that the duties of certain categories of data holders shall be fulfilled by health data intermediation entities.

5. National legislation defined under paragraphs 2, 3 and 4 of this Article shall be notified to the Commission by [date of applicability of chapter IV]. Any subsequent law or amendment affecting them shall be notified to the Commission without delay.

Article 33

Minimum categories of electronic data for secondary use

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

(a) ***health data from EHRs processed in a structured form***~~EHRs~~;

(b) ~~data impacting on health, including~~ ***data on*** ~~-~~social, environmental ***and*** behavioural determinants of health~~;~~

(ba) aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing;

(c) ~~relevant~~ pathogen ~~genomic~~ data, impacting on human health;

(d) ~~health-related~~***healthcare-related*** administrative data, including ***insurance status,*** claims and reimbursement data ***and other administrative data relating to an individual's socioeconomic status, in a structured form***;

(e) human genetic~~, genomic and proteomic~~ ***and genomic*** data;

(ea) other human molecular data such as proteomic transcriptomic, epigenomic, metabolomic, lipidomic and other omic data;

(f) person generated ~~electronic~~ health data~~, including~~ ***through*** medical devices, wellness applications or other digital health applications;

(g) ~~identification data related to~~ ***data on professional status, specialisation and institution of*** health professionals involved in the treatment of a natural person;

(h) ~~population wide~~ ***population-based*** health data registries (public health registries);

(i) ~~electronic health~~ data from medical registries ~~for specific diseases~~***and mortality registries*** ;

(j) ~~electronic health data from~~ ***data from clinical trials and*** clinical ~~trials~~***investigations that have ended in accordance with Article 37(4) of Regulation (EU) 536/2014 and Article 77(5) of Regulation (EU) 2017/745, respectively***;

(k) ~~electronic~~ health data from medical devices ~~and from registries for medicinal products and medical devices;~~

(ka) data from registries for medicinal products and medical devices;

(l) ***data from*** research cohorts, questionnaires and surveys related to health***, after the first publication of results***;

(m) ~~electronic~~ health data from biobanks and ~~dedicated~~ ***associated*** databases;

(n) ~~electronic~~ data related to ~~insurance status~~, professional status, education~~, lifestyle, wellness and behaviour data relevant to health~~;

~~(o) electronic health data containing various improvements such as correction, annotation, enrichment received by the data holder following a processing based on a data permit.~~

2. ~~The requirement in the first subparagraph shall not apply to data holders that qualify as micro enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC[22].~~

~~3. The electronic health data referred to in paragraph 1 shall cover data processed for the provision of health or care or for public health, research, innovation, policy making, official statistics, patient safety or regulatory purposes, collected by entities and bodies in the health or care sectors, including public and private providers of health or care, entities or bodies performing research in relation to these sectors, and Union institutions, bodies, offices and agencies.~~

~~4. Electronic health data entailing protected intellectual property and trade secrets from private enterprises shall be made available for secondary use. Where such data is made available for secondary use, all measures necessary to preserve the confidentiality of IP rights and trade secrets shall be taken.~~

~~5. Where the consent of the natural person is required by national law, health data access bodies shall rely on the obligations laid down in this Chapter to provide access to electronic health data.~~

~~6. Where a public sector body obtains data in emergency situations as defined in Article 15, point (a) or (b) of the Regulation […] [Data Act COM/2022/68 final], in accordance with the rules laid down in that Regulation, it may be supported by a health data access body to provide technical support to process the data or combing it with other data for joint analysis.~~

~~7. The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the list in paragraph 1 to adapt it to the evolution of available electronic health data.~~

~~8~~***3***. ~~Health data access bodies~~ ***Member States*** may provide ~~access to~~ ***by virtue of national law that*** additional categories of electronic health data ~~that they have been entrusted with~~

~~pursuant to national law or based on voluntary cooperation with the relevant data holders at national level, in particular to electronic health data held by private entities in the health sector.~~***shall be made available for secondary use pursuant to this Regulation.***

4. Member States may establish rules for the processing and use of electronic health data containing various improvements related to processing of electronic health data based on a data permit pursuant to Article 46, such as correction, annotation and enrichment.

5. ***Member States may introduce stricter measures at a national level aimed at safeguarding the sensitivity and value of the data referred to in Article 33 (1) points (e) and (ea). Member States shall notify the Commission of those rules and measures and shall notify the Commission without delay of any subsequent amendment affecting them.***

Article 34

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

1. Health data access bodies shall only ~~provide~~ ***grant*** access ***for secondary use*** to electronic health data referred to in Article 33 ~~where the intended purpose of processing pursued by the applicant complies with~~***to a health data user for the following categories of purposes*** :

(a) ~~activities for reasons of~~ public interest in the area of public and occupational health, such as ***activities for*** protection against serious cross-border threats to health~~,~~ ***and*** public health surveillance or ***activities*** ensuring high levels of quality and safety of healthcare***, including patient safety,*** and of medicinal products or medical devices;

(b) ***policy making and regulatory activities*** to support public sector bodies or Union institutions, agencies and bodies**,** including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates;

(c) ~~to produce~~ ***statistics, such as*** national, multi-national and Union level official statistics related to health or care sectors;

(d) education or teaching activities in health or care sectors ***at the level of vocational or higher education***;

(e) scientific research related to health or care sectors;

(f) development and innovation activities ***contributing to the public health or social security, or aimed at ensuring high levels of quality and safety of healthcare, of medicinal products or of medical devices, in particular***: ~~for products or services contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;~~,

(i) activities for the development of medicinal products or services or of medical devices;

(ii) training, testing and evaluating activities of algorithms, including in medical devices, AI systems and digital health applications;

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

(h) providing ~~personalised~~ healthcare ~~consisting in assessing, maintaining or restoring the state of health of natural persons~~, based on the ***electronic*** health data of other natural persons.

2. Access to electronic health data ~~referred to in Article 33 where the intended purpose of processing pursued by the applicant fulfils one of~~***for*** the purposes referred to in points (a) to (c) of paragraph ~~1 shall only be granted to~~ ***1is reserved for*** public sector bodies and Union institutions, bodies, offices and agencies exercising their tasks conferred to them by Union or national law, including where processing of data for carrying out these tasks is done by a third party on behalf of that public sector body or of Union institutions, agencies and bodies.

~~3. The access to privately held data for the purpose of preventing, responding to or assisting in the recovery from public emergencies shall be ensured in accordance with Article 15 of the Regulation […] [Data Act COM/2022/68 final].~~

~~4.~~ ~~Public sector bodies or Union institutions, agencies and bodies that obtain access to electronic health data entailing IP rights and trade secrets in the exercise of the tasks conferred to them by Union law or national law, shall take all specific measures necessary to preserve the confidentiality of such data.~~

Article 35

Prohibited secondary use of electronic health data

~~Seeking access to and processing~~ ***Health data users shall be prohibited to access, processor use*** electronic health data ~~obtained via a~~ ***outside the scope of the*** data permit ~~issued~~ ***pursuant to Article 46 or data request*** pursuant to Article ~~46~~***47. In particular, the following processing and using the electronic health data*** ~~for the following purposes~~ shall be prohibited:

(a) taking decisions detrimental to a natural person ***or a group of natural persons*** based on their electronic health data; in order to qualify as "decisions", they must produce legal***, social or economical,*** effects or similarly significantly affect those natural persons;

(b) taking decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract***, such as life assurance contract or a policy of health insurance or health-related insurance, or to modify their contributions or premiums contract*** or to modify their contributions and insurance premiums;

(ba) activities potentially detrimental to natural persons related to employment, pension and banking, including mortgaging of properties;

(c) advertising or marketing activities towards health professionals, organisations in health or natural persons***, with the exception of public health messaging by competent public sector bodies***;

~~(d) providing access to, or otherwise making available, the electronic health data to third parties not mentioned in the data permit;~~

(e) developing products or services that may harm individuals and societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco products, or goods or services***, services, included those for automated processing,*** which are designed or modified in such a way that they contravene public order or ~~morality.~~***cause a risk for human health;***

(f) activities in conflict with ethical provisions pursuant to national law;

Article 35A

Intellectual property rights and trade secrets

1. Where the health data access body or the Union data access service obtain access to electronic health data from health data holders entailing intellectual property rights and/or trade secrets in the exercise of the tasks conferred to them by this Regulation, they shall take all specific measures, including legal, organisational, and technical ones, necessary to preserve the confidentiality of such data. If the health data access body, by itself or in cooperation with other entities, is unable to preserve the confidentiality of intellectual property rights or trade secrets, it shall refuse access to the health data user in that respect. The health data access body shall inform the health data user of this refusal and explain why it is not possible to provide access.

2. The health data access body or the Union data access service shall make the legal, organisational and technical measures taken to preserve the confidentiality of electronic health data entailing intellectual property rights or trade secrets referred to in paragraph 1 available to the data holder. Generic information about these measures may be made publicly available.

Article 35B

Duties of health data holders

1. ***A health data holder is obliged to make the electronic health data under Article 33 they hold available upon request to the health data access body according to a data permit pursuant to Article 46 or data request pursuant to Article 47.***

1aa. ***Where such electronic health data entail intellectual property rights or trade secrets the health data holder shall inform the health data access body of such intellectual property rights and trade secrets when communicating to the health data access body the dataset descriptions pursuant to Article 35B(2) for the datasets it holds, or at the latest following a request received from the health data access body. If the requested electronic health data is protected by intellectual property rights and/or trade secrets, the health data holder shall justify to the health access body why the data needs specific protection.***

1a. ***The health data holder shall put the requested electronic health data referred to in paragraph 1 at the disposal of the health data access body within a reasonable time of up to 3 months determined by the health data access body. In justified cases, such as in complex and burdensome request, the health data access body may extend this period by up to 3 additional months.***

1b. ***The health data holder shall fulfil its obligations towards natural persons laid down in Article 35D.***

2. ***The health data holder shall communicate to the health data access body a description of the dataset it holds in accordance with Article 55. The health data holder shall, at a minimum, on an annual basis check that its dataset description in the national datasets catalogue is accurate and up to date.***

3. ***Where a data quality and utility label accompanies the dataset pursuant to Article 56, the health data holder shall provide sufficient documentation to the health data access body for that body to confirm the accuracy of the label.***

4. ***A health data holder shall cooperate with the health data access body when the body is carrying out its tasks.***

Article 35C

Duties of health data users

1. Health data users shall only access and process the electronic health data in accordance with a data permit pursuant to Article 46 or a data request pursuant to Article 47 . This includes a prohibition for health data users to try to re-identify the natural persons in the dataset made available to them or to process and use electronic health data outside the scope of the respectively data permit pursuant to Article 46 or data request pursuant to Article 47, in particular the prohibited purposes pursuant to Article 35 or any other misuse of electronic health data.

2. When processing electronic health data within the secure processing environments referred to in Article 50, the health data users are prohibited to provide access to or otherwise making the electronic health data available to third parties not mentioned in the data permit.

3. Health data users shall make public the results or output of the secondary use of electronic health data, including information relevant for the provision of healthcare, within 18 months after the completion of the electronic health data processing in the secure environment or after having received the answer to the data request referred to in Article 47. This period may in justified cases related to the permitted purposes of the processing of electronic health data be extended by the health data access body, in particular in cases where the result is published in a scientific journal or other scientific publication. Those results or output shall only contain anonymous data. The health data users shall inform the health data access bodies from which a data permit was obtained and support them to also make the information related to the results or output provided by the health data users public on health data access bodies' websites. Such publication on the health data access bodies website shall be without prejudice to publication rights in a scientific journal or other scientific publication. Whenever the health data users have used electronic health data in accordance with this Chapter, they shall acknowledge the electronic health data sources and the fact that electronic health data has been obtained in the context of the EHDS.

4. ***Where required by Member State's law, the health data users shall inform the health data access body of any clinically significant findings that may influence the health status of the natural persons whose data are included in the dataset as referred to in Article 35G.***

5. ***The health data users shall cooperate with the health data access body when the health data access body is carrying out its tasks.***

Article 35D

Information from the health data holder to natural persons

1. ***Where Member State law provides that health data holders, in addition to their information obligations under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725, health data holders shall inform natural persons about their processing of personal electronic health data pursuant to this Chapter, the information shall in particular include the following:***

(a) ***the health data holder's obligation to make personal electronic health data available for secondary use to the health data access body upon request or, in situations referred to in Article 49, the health data holder's role pursuant to that Article;***

(b) ***the categories of personal electronic health data it holds that may be made available and the purposes for which those data may be processed pursuant to Article 34;***

2. ***The information referred to in paragraph 1 shall be provided to the natural persons in an easily accessible, intelligible and clearly legible manner and within the timeframe set out respectively in Articles 13(1) and 14(3) of Regulation (EU) 2016/679 or, where applicable Articles 15(1) and 16(3) of Regulation (EU) 2018/1725. Where the health data holder has not obtained the personal electronic health data from the natural person concerned and if the provision of information to each person concerned proves impossible or would involve a disproportionate effort in the meaning of Article 14(5)(b) of Regulation (EU) 2016/679 or Article 16(5)(b) of Regulation (EU) 2018/1725***

respectively, the health data holder shall take appropriate measures and at the minimum make the information referred to in paragraph 1 publicly available.

3. ***The information referred to in paragraph 1 shall also be made publicly available.***

4.. ***Where a Member State has provided for the right to object pursuant to Article 35F,***

(a) ***if this right is to be exercised with the data holder, the data holder shall inform the data subject about the procedure to object.***

(b) ***if this right is to be exercised with the health data access bodies or with the health data intermediation entities, national legislation may define an obligation for the data holder or the health data intermediation entities to inform the data subject about the procedure to object.***

Article 35E

Obligations of health data access bodies towards natural persons

1. ***Health data access bodies shall make publicly available and easily searchable through electronic means the conditions under which electronic health data is made available for secondary use. This shall include information concerning:***

(a) ***the legal basis under which access is granted;***

(b) ***the technical and organisational measures taken to protect the rights of natural persons;***

(c) ***the applicable rights of natural persons in relation to secondary use of electronic health data;***

(d) ***the arrangements for natural persons to exercise their rights in accordance with Chapter III of Regulation (EU) 2016/679;***

(e) ***the results or outcomes of the projects for which the electronic health data were used.***

2 ***If a Member State has provided for the right to object pursuant to Article 35F to be exercised at the health data access bodies, the relevant health data access bodies shall provide public information about the procedure to object and facilitate the exercise of this right.***

Article 35F

Right to object to the processing of personal electronic health data for secondary use

1. ***Member States may provide, by way of national legislation, that natural persons falling under their jurisdiction shall have a specific right to object to the processing of their personal electronic health data for the purposes laid down in Article 34(1) under the conditions set out in paragraph 2.***

2*.* ***Where Member State law provides for the right to object referred to in paragraph 1, it shall lay down at least the following rules and specific safeguards:***

(a) ***Natural persons may exercise this right to object, at any time and without stating reasons, in a simple and accessible manner, including by electronic means;***

(b) ***Member State law shall lay down whether the right to object is to be exercised with either the health data access bodies, the health data intermediation entities, the health data holders or with more than one of them;***

(c) ***After a natural person has exercised the right to object referred to in paragraph 1, the personal electronic health data related to the natural person shall not be made available for secondary use under a data permits pursuant to Article 46 or be processed for secondary use following a data request for electronic health data in a statistical format pursuant to Article 47;***

(d) ***Member State law shall lay down the mechanisms to inform the applicant of, a data permit pursuant to Article 46 or a data request pursuant to Article 47 at the latest prior to the payment of any fees, about the anonymous statistics of natural persons who have exercised the right to object pursuant to this article.***

3. ***Member States may restrict the right to object referred to in paragraph 1 under the conditions set out in Article 23 of Regulation (EU) 2016/679, especially for purposes***

related to public interest in the area of public and occupational health, such as activities for protection against serious cross-border threats to health, and public health surveillance or activities ensuring high levels of quality and safety of healthcare, including patient safety, and of medicinal products or medical devices. In such case, Member States shall implement appropriate and effective measures to inform data subjects about restrictions to the right to object.

Article 35G

Information of findings related to a natural person's health status

Where Member States' law to which the health data access body is subject requires health data users to inform the health data access body of any clinically significant findings that may influence the health status of the natural persons whose data are included in the dataset pursuant to a data permit the health data access body may under the conditions laid down in national law inform the natural person or his or her treating health professional about that finding.

SECTION 2

GOVERNANCE AND MECHANISMS FOR THE SECONDARY USE OF ELECTRONIC HEALTH DATA

Article 36

Health data access bodies

1. Member States shall designate one or more health data access bodies responsible for ~~granting access to electronic health data for secondary use~~ ***carrying out the tasks set out in Articles 37 and 39***. Member States may either establish one or more new public sector bodies or rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions set out in this Article. ***The tasks laid down in Article 37 may be divided between different health data access bodies.*** Where a Member State

designates several health data access bodies, it shall designate one health data access body to act as coordinator, with responsibility for coordinating ~~requests~~ ***tasks*** with the other health data access bodies ***both within the Member State and towards health data access bodies in other Member States***.

2. Member States shall ensure that each health data access body is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and the exercise of its powers.

3. In the performance of their tasks, health data access bodies shall ~~actively cooperate with stakeholders' representatives, especially with representatives of patients, data holders and data users. Staff of health data access bodies shall~~ avoid any ~~conflicts~~***conflict*** of interest. ~~Health data access bodies shall not be bound by any instructions, when making their decisions~~.

4. Member States shall ~~communicate to~~***inform*** the Commission ***of*** the identity of the health data access bodies designated pursuant to paragraph 1 by the date of application of this Regulation. They shall also ~~communicate to~~***inform*** the Commission ***of*** any subsequent modification of the identity of those bodies. The Commission and the Member States shall make this information publicly available.

Article 36A

Union data access service

1. The Commission shall exercise the tasks set out in Articles 37 and 39 concerning health data holders which are Union institutions, bodies, offices or agencies.

2. The Commission shall ensure that the necessary human, technical and financial resources, premises and infrastructure are allocated to the effective performance of these tasks and the exercise of its duties.

3. Unless there is an explicit exclusion, references to the tasks and duties of health data access bodies in this regulation shall also apply to the Commission, where data holders which are Union institutions, bodies, offices, or agencies are concerned.

Article 37

Tasks of health data access bodies

1. Health data access bodies shall carry out the following tasks:

(a) decide on data access applications pursuant to Article 45, authorise and issue data permits pursuant to Article 46 to access electronic health data falling within their national remit for secondary use and decide on data requests ~~in accordance with Chapter II of Regulation […] [Data Governance Act COM/2020/767 final] and this Chapter~~***pursuant to Article 47 in accordance with this Chapter and Chapter II of Regulation (EU) 2022/868 including***;

(i) process electronic health data referred to in Article 33 such as the gathering, combination, preparation and compiling of necessary requested data from health data holders, the pseudonymisation or anonymisation of the data and the disclosure of those data for secondary use to health data users on the basis of a data permit or a data request;

(ii) take all measures necessary to preserve the confidentiality of IP rights and of trade secrets of electronic health data before those data are made available for secondary use pursuant to a data permit or a data request taking into account the relevant rights of both the health data holder and health data user;

(iii) provide access to electronic health data to health data users pursuant to a data permit in a secure processing environment in accordance with the requirements laid down in Article 50.

(ab) monitor and supervise compliance with the requirements laid down in this Regulation by health data users and health data holders.

~~(b) support public sector bodies in carrying out the tasks enshrined in their mandate, based on national or Union law;~~

~~(c) support Union institutions, bodies, offices and agencies in carrying out tasks enshrined in the mandate of Union institutions, bodies, offices and agencies, based on national or Union law;~~

~~(d) process electronic health data for the purposes set out in Article 34, including the collection, combination, preparation and disclosure of those data for secondary use on the basis of a data permit;~~

~~(e) process electronic health data from other relevant data holders based on a data permit or a data request for a purposes laid down in Article 34;~~

~~(f) take all measures necessary to preserve the confidentiality of IP rights and of trade secrets;~~

~~(g) gather and compile or provide access to the necessary electronic health data from the various data holders whose electronic health data fall within the scope of this Regulation and put those data at the disposal of data users in a secure processing environment in accordance with the requirements laid down in Article 50;~~

~~(h) contribute to data altruism activities in accordance with Article 40;~~

~~(i) support the development of AI systems, the training, testing and validating of AI systems and the development of harmonised standards and guidelines under Regulation […] [AI Act COM/2021/206 final] for the training, testing and validation of AI systems in health;~~

(j) cooperate with and supervise data holders to ensure the consistent and accurate implementation of the data quality and utility label set out in Article 56;

(k) maintain a management system to record and process data access applications, data requests***, the decisions on these*** and the data permits issued and data requests answered, providing at least information on the name of the data applicant, the purpose of access the date of issuance, duration of the data permit and a description of the data application or the data request;

~~(l) maintain a public information system to comply with the obligations laid down in Article 38;~~

(m) cooperate at Union and national level to lay down appropriate measures and requirements for accessing electronic health data in a secure processing environment;

(n) cooperate at Union and national level and provide advice to the Commission on techniques and best practices for ***secondary use of*** electronic health data ~~use~~ and management;

(o) facilitate cross-border access to electronic health data for secondary use hosted in other Member States through HealthData@EU and cooperate closely with each other and with the Commission.

~~(p) send to the data holder free of charge, by the expiry of the data permit, a copy of the corrected, annotated or enriched dataset, as applicable, and a description of the operations performed on the original dataset;~~

(q) make public, through electronic means:

(i) a ~~national~~ dataset catalogue ~~that shall include details about the source and nature of electronic health data, in accordance with Articles 56 and 58, and the conditions for making electronic health data available. The national dataset catalogue shall also be made available to single information points under~~ ***referred to in*** Article ~~8 of Regulation […] [Data Governance Act COM/2020/767 final];~~***55***

(ii) ~~all~~***data access applications and*** data permits, requests and ~~applications~~***answers, including the rejected applications ,*** on their websites within 30 working days after ~~issuance of the~~***deciding on a*** data permit or ~~reply to~~ a data request ;

(iii) ~~penalties applied~~ ***measures related to non-compliance*** pursuant to Article 43;

(iv) results communicated by ***health*** data users pursuant to Article ~~46(11)~~***35C(3)***;

(v) an information system to comply with the obligations laid down in Article 35E;

(vi) information of the connection of a national contact point of a third country or an international organisation, as soon as it becomes an authorised

participant in HealthData@EU, through electronic means, at minimum on an easily accessible website or web portal.

(r) fulfil obligations towards natural persons pursuant to ~~Article 38~~***Articles 35E to 35G***;

~~(s) request from data users and data holders all the relevant information to verify the implementation of this Chapter;~~

(t) fulfil any other tasks related to making available the secondary use of electronic health data in the context of this Regulation.

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

(a) cooperate with supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 in relation to personal electronic health data and the EHDS Board;

(b) inform the relevant supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 ~~where a health data access body has imposed penalties or other measures pursuant to Article 43 in relation to processing personal electronic health data and where such processing refers to an attempt to re-identify an individual or~~***of any suspected*** unlawful processing of personal electronic health data;

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

(d) cooperate with other national competent bodies, including the national competent bodies supervising data altruism organisations under Regulation ~~[…] [Data Governance Act COM/2020/767 final]~~***(EU) 2022/868*** , the competent authorities under Regulation […] [Data Act COM/2022/68 final] and the national competent authorities for Regulations (EU) 2017/745***, (EU) 2017/746*** and Regulation […] [AI Act COM/2021/206 final]***, where relevant*** ~~-~~.

3. The health data access bodies may provide assistance to public sector bodies where those public sector bodies access electronic health data on the basis of Article 14 of Regulation […] [Data Act COM/2022/68 final].

3a. ***The health data access body may provide support to a public sector body where it obtains data in emergency situations as defined in Article 15, point (a) or (b) of the Regulation […] [Data Act COM/2022/68 final], in accordance with the rules laid down in that Regulation, by providing technical support to process the data or combining it with other data for joint analysis.***

~~4.~~ ~~The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the list of tasks in paragraph 1 of this Article, to reflect the evolution of activities performed by health data access bodies.~~

5. ***Notwithstanding national laws requesting the data subject's consent pursuant to Article 9(4) of Regulation (EU) 2016/679, health data access bodies shall rely on the obligations laid down in this Chapter, when requesting and processing personal electronic health data from the health data holder and provide access to pseudonymised electronic health data to the health data user.***

~~*Article 38*~~

~~Obligations of health data access bodies towards natural persons~~

~~1.~~ ~~Health data access bodies shall make publicly available and easily searchable the conditions under which electronic health data is made available for secondary use, with information concerning:~~

~~(a) the legal basis under which access is granted;~~

~~(b) the technical and organisational measures taken to protect the rights of natural persons;~~

~~(c) the applicable rights of natural persons in relation to secondary use of electronic health data;~~

~~(d) the arrangements for natural persons to exercise their rights in accordance with Chapter III of Regulation (EU) 2016/679;~~

~~(e) the results or outcomes of the projects for which the electronic health data were used.~~

~~2. Health data access bodies shall not be obliged to provide the specific information under Article 14 of Regulation (EU) 2016/679 to each natural person concerning the use of their data for projects subject to a data permit and shall provide general public information on all the data permits issued pursuant to Article 46.~~

~~3. Where a health data access body is informed by a data user of a finding that may impact on the health of a natural person, the health data access body may inform the natural person and his or her treating health professional about that finding.~~

~~4. Member States shall regularly inform the public at large about the role and benefits of health data access bodies.~~

Article 39

Reporting by health data access bodies

1. Each health data access body shall publish ~~an annual~~***a biennial*** activity report***. If a Member States designates more than one health data access body, the coordinating body referred to in Article 37(1) shall be responsible for the report and request necessary information from the other health data access bodies. The activity report shall follow a structure agreed within EHDS Board. The activity report*** ~~which~~ shall contain at least the following:

(a) information relating to the data access applications for electronic health data access submitted, such as the types of applicants, number of data permits granted or refused, ***categories of*** purposes of access and categories of electronic health data accessed, and a summary of the results of the electronic health data uses, where applicable;

~~(b) a list of data permits involving access to electronic health data processed by the health data access body based on data altruism and a summary description of the general interests purposes pursued, where applicable, including the outcomes of the data permits granted;~~

(c) information on the fulfilment of regulatory and contractual commitments by ***health*** data users and ***health*** data holders, as well as penalties imposed;

(d) information on audits carried out on ***health*** data users to ensure compliance of the processing ~~with~~ ***in the secure processing environment pursuant to Article 50(1)(e) of*** this Regulation,

(e) information on ***third party*** audits on compliance of secure processing environments with the defined standards, specifications and requirements ***pursuant to Article 50(3) of this Regulation;*** ~~;~~

(f) information on the handling of requests from natural persons on the exercise of their data protection rights;

~~(g) a description of its activities carried out in relation to engagement with and consultation of relevant stakeholders, including representatives of natural persons, patient organisations, health professionals, researchers, and ethical committees;~~

~~(h) information on cooperation with other competent bodies in particular in the area of data protection, cybersecurity, data altruism, and artificial intelligence;~~

(i) revenues from data permits and data requests;

~~(j) satisfaction from applicants requesting access to data;~~

(k) average number of ***working*** days between application and access to data;

(l) number of data quality labels issued, disaggregated per quality category;

~~(m) number of peer-reviewed research publications, policy documents, regulatory procedures using data accessed via the EHDS;~~

(n) number of digital health products and services, including AI applications, developed using data accessed via EHDS.

2. The report shall be ~~transmitted~~ ***sent*** to the Commission ***and the EHDS Board within 6 months after the end date of the 2 year reporting period***.

~~3. The Commission is empowered to adopt delegated acts in accordance with Article 67 to modify the content of the annual activity report.~~

Article 40

Data altruism in health

1. When processing personal electronic health data, data altruism organisations shall comply with the rules set out in Chapter IV of Regulation […] [Data Governance Act COM/2020/767 final]. Where data altruism organisations process personal electronic health data using a secure processing environment, such environments shall also comply with the requirements set out in Article 50 of this Regulation.

2. Health data access bodies shall support the competent authorities designated in accordance with Article 23 of Regulation […] [Data Governance Act COM/2020/767 final] in the monitoring of entities carrying out data altruism activities.

Article 41

Duties of data holders

1. Where a data holder is obliged to make electronic health data available under Article 33 or under other Union law or national legislation implementing Union law, it shall cooperate in good faith with the health data access bodies, where relevant.

2. The data holder shall communicate to the health data access body a general description of the dataset it holds in accordance with Article 55.

3. Where a data quality and utility label accompanies the dataset pursuant to Article 56, the data holder shall provide sufficient documentation to the health data access body for that body to confirm the accuracy of the label.

4. The data holder shall put the electronic health data at the disposal of the health data access body within 2 months from receiving the request from the health data access body. In exceptional cases, that period may be extended by the health data access body for an additional period of 2 months.

5. Where a data holder has received enriched datasets following a processing based on a data permit, it shall make available the new dataset, unless it considers it unsuitable and notifies the health data access body in this respect.

~~6.~~ ~~Data holders of non-personal electronic health data shall ensure access to data through trusted open databases to ensure unrestricted access for all users and data storage and preservation. Trusted open public databases shall have in place a robust, transparent and sustainable governance and a transparent model of user access.~~

~~7.~~ ~~The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the duties of the data holders in this Article, to reflect the evolution of activities performed by data holders.~~

Article 42

Fees

1. Health data access bodies ~~and~~***or*** single ***health*** data holders ***referred to in Article 49*** may charge fees for making electronic health data available for secondary use. ~~Any~~***Such*** fees shall ~~include and be derived from the costs related to conducting the procedure for requests, including~~ ***be in proportion to the cost of making the data available and not restrict competition. Such fees shall cover all or part of costs related to the procedure*** for assessing a data ***permit*** application or a data request, granting, refusing or amending a data permit pursuant to ~~Articles~~***Article*** 45 and 46 or providing an answer to a data request pursuant to Article 47, ***as well as costs related to the gathering, preparation and provisioning of the electronic health data.*** ~~In accordance with~~ ***This provision prevails over*** Article 6 of Regulation ~~[…] [Data Governance Act COM/2020/767 final]~~***(EU)2022/868 for health data holders and single data holders from the public sector. Reduced fees may be established by the Member States for certain types of data users located in the Union, such as university researchers or micro-enterprises.***

2. Where the ***electronic health*** data in question are ~~not~~ held by ~~the data access body or a public sector~~***a health data holder or a data intermediation entity which is not a health data access*** body, the fees ***charged pursuant to paragraph 1*** may also include compensation for ~~part of the costs for collecting~~ ***costs incurred by the health data holder compiling and preparing*** the electronic health data ~~specifically under this Regulation in addition to the fees that may be charged pursuant to paragraph 1~~***to be made available for secondary use. When the health data holder is a public sector body, Article 6 of***

Regulation (EU)2022/868 shall not apply. The part of the fees linked to the ***health*** data holder's costs shall be paid to the ***health*** data holder.

~~3. The electronic health data referred to in Article 33(1), point (o), shall be made available to a new user free of charge or against a fee matching the compensation for the costs of the human and technical resources used to enrich the electronic health data. That fee shall be paid to the entity that enriched the electronic health data.~~

~~4. Any fees charged to data users pursuant to this Article by the health data access bodies or data holders shall be transparent and proportionate to the cost of collecting and making electronic health data available for secondary use, objectively justified and shall not restrict competition. The support received by the data holder from donations, public national or Union funds, to set up, develop or update tat dataset shall be excluded from this calculation. The specific interests and needs of SMEs, public bodies, Union institutions, bodies, offices and agencies involved in research, health policy or analysis, educational institutions and healthcare providers shall be taken into account when setting the fees, by reducing those fees proportionately to their size or budget.~~

~~5. Where data holders and data users do not agree on the level of the fees within 1 month of the data permit being granted, the health data access body may set the fees in proportion to the cost of making available electronic health data for secondary use. Where the data holder or the data user disagree with the fee set out by the health data access body, they shall have access to dispute settlement bodies set out in accordance with Article 10 of the Regulation […] [Data Act COM/2022/68 final].~~

5a. Before issuing a data permit pursuant to Article 46 or providing an answer to a data request pursuant to Article 47, the health data access body shall inform the applicant of the expected fees. The applicant shall be informed about the option to withdraw the application. If the applicant withdraw its application, the applicant shall only be charged the costs that have already been incurred.

6. The Commission may, ~~by means of implementing acts, lay down principles and rules for the~~***in close cooperation with the EHDS Board, issue guidelines on*** fee policies and fee structures~~. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2)~~ ***in order to support consistency and transparency between Member States***.

Article 43

*~~Penalties~~**Non-compliance** by health data ~~access bodies~~**holder and health data user***

~~1. Health data access bodies shall monitor and supervise compliance by data users and data holders with the requirements laid down in this Chapter.~~

2. When ~~requesting from data users and data holders the information that is necessary to verify compliance with this Chapter, the~~***health data access bodies perform their monitoring and supervising tasks the bodies have the right to request and receive from*** health data ~~access bodies shall be proportionate to the performance of the~~***users and health data holders all the necessary information to verify*** compliance ~~verification task~~***with this Chapter***.

3. Where ***a*** health data access ~~bodies find~~***body finds*** that a ***health*** data user or ***a health*** data holder does not comply with the requirements of this Chapter, ~~they~~ ***it*** shall immediately notify the ***health*** data user or ***health*** data holder of those findings and ***take appropriate measures. The health data access body*** shall give ~~it~~***the concerned health data user or the health data holder*** the opportunity to state its views within ***a reasonable time*** ~~2 months~~.

4. ***With regard to non-compliance by a health data user pursuant to a data permit,*** health data access bodies shall have the power to revoke the data permit issued pursuant to Article 46 and stop the affected electronic health data processing operation carried out by the ***health*** data user ~~in order to ensure the cessation of the non-compliance referred to in paragraph 3,~~ immediately or within a reasonable time limit, and shall take appropriate and proportionate measures aimed at ensuring compliant processing by the ***health*** data users~~.~~. In this regard, the health data access bodies shall ***also*** be able, where appropriate, ~~to revoke the data permit and~~ ***to exclude or initiate proceedings*** to exclude ***in accordance with national law the health*** ~~the~~ data user from any access to electronic health data ***within the EHDS in the context of secondary use*** for a period of up to 5 years.

4a. Where a health data access body finds that a health data user is processing or using the electronic health data outside the scope of the data permit for the prohibited uses laid down in Article 35 or a health data user does not respect the health data access body's measures ensuring pseudonymisation, it shall immediately revoke the data permit issued.

5. ***With regard to non-compliance by a health data holder,*** where ***health*** data holders withhold the electronic health data from health data access bodies with the manifest intention of obstructing the use of electronic health data, or do not respect the deadlines set out in Article ~~41~~***35B(1a)***, the health data access body shall have the power to fine the ***health*** data holder with ~~fines~~***periodic penalty payment in accordance with national law*** for each day of delay, which shall be transparent and proportionate. The amount of the fines shall be established by the health data access body. In case of repeated breaches by the ***health*** data holder of the obligation of ~~loyal~~ cooperation with the health data access body, that body ~~can~~ ***may*** exclude ~~the data holder from participation in the EHDS for a period of up to 5 years. Where a~~***or initiate proceedings to exclude in accordance with national law the health*** data holder ~~has been excluded from the~~***from*** participation in the EHDS ~~pursuant to this Article, following manifest intention of obstructing the~~ ***in the context of*** secondary use ~~of electronic health data, it shall not have the right to provide access to health data in accordance with Article 49.~~***for a period of up to 5 years.***

6. The health data access body shall communicate the measures imposed pursuant to paragraph 4 and the reasons on which they are based to the ***health*** data user or holder concerned, without delay, and shall lay down a reasonable period for the ***health*** data user or holder to comply with those measures.

7. Any ***measures imposed by the health data access body*** ~~penalties and measures imposed~~ pursuant to paragraph 4 shall be ~~made available~~ ***notified*** to other health data access bodies***, through the tool referred to in paragraph 8***.

8. The Commission ~~may~~***shall***, by means of implementing act, set out the architecture of an IT tool aimed to support and make transparent to other health data access bodies the ~~activities~~ ***measures related to non-compliance*** referred to in this Article, especially ~~penalties~~***periodic penalty payments, revoking of data permits*** and exclusions. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

9. Any natural or legal person affected by a decision of a health data access body shall have the right to an effective judicial remedy against such decision.

10. The Commission may ~~issues~~***issue*** guidelines***, in close cooperation with EHDS Board, on periodic penalty payments and other measures*** ~~on penalties~~ to be applied by the health data access bodies.

Article 43A

Relationship with data protection supervisory authorities

The supervisory authority or authorities responsible for monitoring and enforcement the application of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 shall also be responsible for monitoring and enforcement the processing of personal electronic health data for secondary use, in accordance with the relevant provisions of Regulation (EU) 2016/679 or of Regulation (EU) 2018/1725 respectively. They shall be competent to impose administrative fines up to the amount referred to in Article 83 and 52 respectively of those Regulations. Those supervisory authorities and the health data access bodies referred to in Article 36 of this Regulation shall, where relevant, cooperate in the enforcement of this Regulation, within the remit of their respective competences.

SECTION 3

~~DATA PERMIT FOR THE~~ *ACCESS TO ELECTRONIC HEALTH DATA FOR* SECONDARY USE ~~OF ELECTRONIC HEALTH DATA~~

Article 44

Data minimisation and purpose limitation

1. The health data access body shall ensure that access is only provided to requested electronic health data relevant for the purpose of processing indicated in the data ~~access~~ ***permit*** application by the ***health*** data user and in line with the data permit granted.

2. The health data access bodies shall provide ~~the~~ electronic health data in an anonymised ***or anonymised statistical*** format, where the purpose of processing by the ***health*** data user can be achieved with such data, taking into account the information provided by the ***health*** data user.

3. Where the purpose of the ***health*** data user's processing cannot be achieved with anonymised data, taking into account the information provided by the ***health*** data user, the health data access bodies shall provide access to electronic health data in pseudonymised format. The information necessary to reverse the pseudonymisation shall be available only to the health data access body~~. Data users shall not re-identify the electronic health data provided to them in pseudonymised format. The data user's failure to respect the health data access body's measures ensuring pseudonymisation shall be subject to appropriate penalties.~~ ***or a body that acts as trusted third party in accordance with national law.***

Article 45

Data access applications

1. ~~Any~~***A*** natural or legal person may submit a data access application for the purposes referred to in Article 34 ***to the health data access body***.

2. The data access application shall include ***a data utilisation plan with the following information***:

(aa) a description of the applicant's identity, professional function and activities, including the identity of the natural persons who will have access to the electronic health data;

(a) ~~a~~ detailed explanation of the intended ***use and expected benefit related to the*** use of the electronic health data, including for which of the purposes referred to in Article 34(1) access is sought;

(b) a description of the requested electronic health data, their format and data sources, where possible, including geographical coverage where data is requested from ***health data holder in*** several Member States ***or authorised participants in the cross-border infrastructure referred to in Article 52***;

(c) ~~an indication~~ ***a description*** whether electronic health data ***need to*** ~~should~~ be made available in ~~an~~***a pseudonymised or*** anonymised format;

~~(d) where applicable, an explanation of the reasons for seeking access to electronic health data in a pseudonymised format;~~

(e) a description of the safeguards planned to prevent any ~~other use~~ ***misuse*** of the electronic health data***, including re-identification of natural persons in the dataset***;

(ea) in case the applicant intends to bring datasets it already holds into the secure processing environment, a description of those datasets;

(f) a description of the safeguards planned to protect the rights and interests of the ***health*** data holder and of the natural persons concerned;

(g) an ~~estimation~~***indication*** of the period during which the electronic health data is needed for processing ***in a secure processing environment***;

(h) a description of the tools and computing resources needed for a secure environment.

(i) information on the assessment of ethical aspects of the processing, where applicable and in line with national law.

~~3.~~ ~~Data users seeking access to electronic health data from more than one Member State shall submit a single application to one of the concerned health data access bodies of their choice which shall be responsible for sharing the request with other health data access bodies and authorised participants in HealthData@EU referred to in Article 52, which have been identified in the data access application. For requests to access electronic health data from more than one Member States, the health data access body shall notify the other relevant health data access bodies of the receipt of an application relevant to them within 15 days from the date of receipt of the data access application.~~

3~~4~~. Where the applicant ~~intends to~~ ***seeks for*** access the personal electronic health data in a pseudonymised format ***in a secure processing environment***, the following additional information shall be provided together with the data access application:

(aa) a detailed justification on the reasons why access to electronic health data in an anonymised form is not sufficient for the intended use;

(a) a description of how the processing would comply with ~~Article 6(1)~~ ***Article 6(1)*** of Regulation (EU) 2016/679 ***or Article 5(1) of Regulation (EU) 2018/1725***;

(ba) a description of how the processing would comply with Chapter V of Regulations (EU) 2016/679 or (EU) 2018/1725 respectively, where applicable;

~~(b) information on the assessment of ethical aspects of the processing, where applicable and in line with national law.~~

(c) a documented data protection impact assessment required by Article 35 of Regulation (EU) 2016/679 or Article 39 of Regulation (EU) 2018/1725, where applicable.

4~~5~~. ~~For the implementation of the tasks referred to in Article 37(1), points (b) and (c),~~ The public sector bodies and the Union institutions, bodies, offices and agencies shall provide the same information as requested under Article 45(2) ***and 45(4)***, except for point (g) ***in 45(2)***, where they shall submit information concerning the period for which the ***electronic health*** data can be accessed, the frequency of that access or the frequency of the data updates.

~~Where the public sector bodies and the Union institutions, bodies, offices and agencies intend to access the electronic health data in pseudonymised format, a description of how the processing would comply with Article 6(1) of Regulation (EU) 2016/679 or Article 5(1) of Regulation (EU) 2018/1725, as applicable, shall also be provided.~~

5. Where an applicant seeks access to electronic health data from health data holders established in different Member State or from other authorised participants in the cross-border infrastructure referred to in Article 52, the applicant shall submit a single data access application through the Health Data Access Body of their main establishment or through the services provided by the Commission in the cross-border infrastructure HealthData@EU referred to in Article 52. The application shall be automatically forwarded to the authorised participants identified in the data access application and to the Health Data Access Bodies of the Member States where the data holders and the authorised participants identified in the data access application have their main establishment.

~~6. The Commission may, by means of implementing acts, set out the templates for the data access application referred to in this Article, the data permit referred to in Article 46 and the data request referred to in Article 47. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 68(2).~~

~~7.~~ ~~The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the list of information in paragraphs 2, 4, 5 and 6 of this Article, to ensure the adequacy of the list for processing a data access application at national or cross-border level.~~

Article 46

Data permit

1. ***The*** health data access bodies shall ~~assess if the application fulfils one of the purposes listed in Article 34(1) of this Regulation, if the requested data is necessary for the purpose listed in the application and if the requirements in this Chapter are fulfilled by the applicant. If that is the case, the health data access body shall issue a data permit.~~***decide to grant or refuse access to electronic health data on the basis of the following criteria:***

(a) the purposedescribed in the data permit application matches one or more of the purposes listed in Article 34(1) of this Regulation;

(b) the requested data is necessary for the purpose described in the data access application taking into account the provisions of data minimisation and purpose limitation in Article 44;

(c) the processing complies with Article 6(1) of Regulation (EU) 2016/679 or Article 5(1) of Regulation (EU) 2018/1725, in case of access to pseudonymised electronic health data, as well as Chapter V in those Regulations respectively, where applicable;

(d) the information provided in the application demonstrates sufficient safeguards to protect the rights and interests of the health data holder and of the natural persons concerned as well as to prevent misuse;

(e) the information on the assessment of ethical aspects of the processing, where applicable, complies with national law;

(f) other requirements in this Chapter.

The health data access body shall also take into account the following risks:

(a) risks for national defence, security, public security and public order;

(b) risks of undermining protected IP-rights and trade secrets and privacy of natural persons;

(c) risk of undermining confidential data in governmental databases of regulatory authorities;

(d) risk of misuse, including the prohibited use in Article 35.

2. ***If the*** health data access ~~bodies shall refuse all applications including one or more purposes listed in Article 35 or~~ ***body in its assessment comes to the conclusion that the requirements in paragraph 1 are met and the risks referred to in paragraph 2 are sufficiently mitigated, the health data access body shall issue a data permit. Health data access bodies shall refuse all applications*** where ***the*** requirements in this Chapter are not met. ***Alternatively, a health data access body may decide to provide an answer in an anonymous statistical format under article 47, if this approach mitigates the risks and if the purpose of the data access application can be fulfilled in this manner.***

3. ***By way of derogation from that Regulation (EU) 2022/868,*** a health data access body shall issue or refuse a data permit within ~~2~~***3*** months of receiving the data access application. ~~By way of derogation from that Regulation […] [Data Governance Act COM/2020/767 final],~~ The health data access body may extend the period for responding to a data access application by ~~2~~***3*** additional months where necessary, taking into account the ***urgency and*** complexity of the request ***and the volume of requests submitted for decision***. In such cases, the health data access body shall notify the applicant as soon as possible that more time is needed for examining the application, together with the reasons for the delay. ~~Where a health data access body fails to provide a decision within the time limit, the data permit shall be issued~~.

3A. When handling a data access application for cross-border access to electronic health data referred to in Article 45(5A), health data access bodies and relevant authorised participants in HealthData@EU referred to in Article 52, shall remain responsible for taking decisions to grant or refuse access to electronic health data within their remit in

accordance with the requirements in this Chapter. The concerned health data access bodies and authorised participants shall inform each other of their decisions and may take the information into consideration when deciding on granting or refusing access to electronic health data.

3AA. ***Member States may provide for an accelerated application procedure for public sector bodies and Union institutions, bodies, offices and agencies if the processing of the data s is to be carried out for the purposes in article 34(1), letters (a) to (c).***

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

4a. ***In situations referred to in paragraph 3A the concerned health data access bodies and authorised participants who issued a data permit, may decide to provide access to the electronic health data in the secure processing environment provided by the Commission as referred to in Article 52(10).***

5. When the health data access body refuses to issue a data permit, it shall provide a justification for the refusal to the applicant.

6. ***When the health data access body issues a*** ~~The~~ data permit***, it*** shall set out the general conditions applicable to the ***health*** data user~~, in particular~~ ***in the data permit. The data permit shall contain the following***:

(a) ~~types~~***categories, specification*** and format of electronic health data accessed, covered by the data permit, including their sources ***and if the electronic health data will be accessed in a pseudonymised format in the secure processing environment***;

(b) ***a detailed description of the*** purpose for which data are made available;

(ba) the identity of authorised persons who will have the right to access the electronic health data in the secure processing environment;

(c) duration of the data permit;

(d) information about the technical characteristics and tools available to the ***health*** data user within the secure processing environment;

(e) fees to be paid by the ***health*** data user;

(f) any additional specific conditions in the data permit granted.

~~7. Data users shall have the right to access and process the electronic health data in accordance with the data permit delivered to them on the basis of this Regulation.~~

~~8. The Commission is empowered to adopt delegated acts to amend the list of aspects to be covered by a data permit in paragraph 7 of this Article, in accordance with the procedure set out in Article 67.~~

9. A data permit shall be issued for the duration necessary to fulfil the requested purposes which shall not exceed ~~5~~ ***10*** years. This duration may be extended once, at the request of the ***health*** data user, based on arguments and documents to justify this extension provided, 1 month before the expiry of the data permit, for a period which cannot exceed ~~5~~ ***10*** years. ~~By way of derogation from Article 42, ~~ The health data access body may charge increasing fees to reflect the costs and risks of storing electronic health data for a longer period of time exceeding the initial ~~5 years~~***period*** . In order to reduce such costs and fees, the health data access body may also propose to the ***health*** data user to store the dataset in storage system with reduced capabilities. ***Such reduced capabilities shall not affect the security of the processed dataset. The electronic health*** ~~The~~ data within the secure processing environment shall be deleted within 6 months following the expiry of the data permit. Upon request of the ***health*** data user, the formula on the creation of the requested dataset ~~shall~~ ***may*** be stored by the health data access body.

10. If the data permit needs to be updated, the ***health*** data user shall submit a request for an amendment of the data permit.

~~11. Data users shall make public the results or output of the secondary use of electronic health data, including information relevant for the provision of healthcare, no later than 18 months after the completion of the electronic health data processing or after having received the answer to the data request referred to in Article 47. Those results or output shall only contain anonymised data. The data user shall inform the health data access bodies from which a data permit was obtained and support them to make the information~~

~~public on health data access bodies' websites. Whenever the data users have used electronic health data in accordance with this Chapter, they shall acknowledge the electronic health data sources and the fact that electronic health data has been obtained in the context of the EHDS.~~

~~12. Data users shall inform the health data access body of any clinically significant findings that may influence the health status of the natural persons whose data are included in the dataset.~~

13. The Commission may, by means of implementing act, develop a logo for acknowledging the contribution of the EHDS. That implementing act shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

~~14. The liability of health data access bodies as joint controller is limited to the scope of the issued data permit until the completion of the processing activity.~~

Article 47

Data request

1. ~~Any~~***A*** natural or legal person may submit a ~~data~~ request for ~~the purposes referred to in Article 34. A~~ ***electronic*** health data ~~access body shall only provide an answer to a data request in an anonymised~~ ***in a*** statistical format ~~and the data user shall have no access~~***for the purposes referred to in Article 34*** to the ~~electronic~~ health data ~~used to provide this answer.~~***access body.***

2. A data request ~~shall include the elements mentioned in paragraphs 2 (a) and (b) of Article 45 and if needed may also include~~ ***referred to in paragraph 1 shall include the following information*** :

   (a) a description of the ~~result expected from the health data access body~~ ***applicant's identity, professional function and activities***;

   (b) a ~~description~~ ***detailed explanation of the intended use of the electronic health data, including for which*** of the ~~statistic's content.~~***purposes referred to in Article 34(1) access is sought;***

(c) a description of the requested electronic health data, their format and data sources, where possible;

(d) a description of the statistic's content;

(e) a description of the safeguards planned to prevent any misuse of the electronic health data.

(f) a description of how the processing would comply with Articles 6(1) of Regulation (EU) 2016/679 or Articles 5(1) and 10(2) of Regulation (EU) 2018/1725;

2a. The health data access body shall assess if the request is complete and take into account the following risks:

(a) risks for national defense, security, public security and public order;

(b) risks of undermining protected IP-rights and trade secrets;

(c) risks of undermining confidential data in governmental databases of market regulatory authorities;

(d) risks of misuse, including the prohibited use in Article 35.

3. Where an applicant has requested a result in an anonymised form, including statistical format, based on a data request, the health data access body shall assess ***the request***, within ~~2~~ ***3*** months and, where possible, provide the result to the ***health*** data user within ~~2~~ ***3*** months. ***The health data access body shall only provide an answer in an anonymised statistical format and the health data user shall have no access to the electronic health data used to provide the answer.***

Article 47A

Templates to support access to electronic health data for secondary use

1. The Commission may, by means of implementing acts, set out the templates for the data access application referred to in Article 45, the data permit referred to in Article 46 and the data request referred to in Article 47

2. The Commission may, by means of implementing acts, adopt the necessary rules for facilitating the handling of data access applications for HealthData@EU referred to in Article 45(5A), including the single application template, a common data permit template, standard templates for common electronic health data access contractual arrangements, and common procedures for handling cross-border requests, pursuant to Articles 45, 46 and 47.

3. The implementing acts referred to in paragraphs 1 and 2 shall be adopted in accordance with the examination procedure referred to in Article 68(2).

Article 47B

Data applications and data requests from third countries

1. ***Without prejudice to Articles 45, 46 and 47, for health data access bodies designated by the Member States and the Union data access service, data applications and data requests submitted by a data user established in a third country shall be considered eligible if the third country concerned***

(a) is covered by an implementing act referred to in Article 52 (5); or

(b) allows EU applicants access to electronic health data in that third country under conditions that are not more restrictive than provided for in this regulation and therefore are covered by the implementing acts referred to in paragraph (2).

2. The Commission shall adopt implementing acts establishing the list of third countries referred to in paragraph (1) point b). These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68 (2). The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available.

3. Health data access bodies may also decide on the eligibility of data applications submitted by a data user established in a third country not covered by paragraph 1 on a case-by-case basis.

~~*Article 48*~~

~~Making data available for public sector bodies and Union institutions, bodies, offices and agencies without a data permit~~

~~By derogation from Article 46 of this Regulation, a data permit shall not be required to access the electronic health data under this Article. When carrying out those tasks under Article 37 (1), points (b) and (c), the health data access body shall inform public sector bodies and the Union institutions, offices, agencies and bodies, about the availability of data within 2 months of the data access application, in accordance with Article 9 of Regulation […] [Data Governance Act COM/2020/767 final]. By way of derogation from that Regulation […] [Data Governance Act COM/2020/767 final], the health data access body may extend the period by 2 additional months where necessary, taking into account the complexity of the request. The health data access body shall make available the electronic health data to the data user within 2 months after receiving them from the data holders, unless it specifies that it will provide the data within a longer specified timeframe.~~

Article 49

*Access to electronic health data from a single **health** data holder in **Member States***

1. ***Member States may allow any or specific health data holder to fulfil the tasks referred to in Article 37(1)(a) in situations*** where an applicant requests access to electronic health data only from a single ***health*** data holder in a single Member State***. In such cases***, by way of derogation from Article 45(1) ***and Article 47(1)***, that applicant may file a data access application or a data request directly to ~~the~~***that health*** data holder. The data access application shall comply with the requirements set out in Article 45 and the data request shall comply with requirements in Article 47. ~~Multi-country requests and requests requiring a combination of datasets from several data holders shall be adressed to health data access bodies.~~

(1a) The Commission may allow that data applications or data requests are submitted directly to an Union institution, agency or body. In such case, this Article applies mutatis mutandis.

2. In ***situations referred to in paragraph 1 in this Article, the health*** ~~such case, the~~ data holder may issue a data permit in accordance with Article 46 or provide an answer to a data request in accordance with Article 47. ***When issuing a data permit, the health*** ~~The~~ data holder shall ~~then~~ provide access to the electronic health data in a secure processing environment in compliance with Article 50 and may charge fees in accordance with Article 42.

~~3. By way of derogation from Article 51, the single data provider and the data user shall be deemed joint controllers.~~

4. ~~Within 3 months the~~***The single health*** data holder***, referred to in paragraph 1 of this Article,*** shall ***within 3 months*** inform the relevant health data access body by electronic means of all data access applications filed and all the data permits issued and the data requests fulfilled under this Article in order to enable the health data access body to fulfil its obligations under ~~Article 37(1) and Article~~ ***Articles 37 and*** 39.

Article 50

Secure processing environment

1. The health data access bodies shall provide access to electronic health data ***pursuant to a data permit*** only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, ~~they~~***the secure processing environment*** shall ~~take~~ ***comply with*** the following security measures:

(a) restrict access to the secure processing environment to authorised ***natural*** persons listed in the respective data permit;

(b) minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;

(c) limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;

(d) ensure that ***health*** data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

(e) keep identifiable logs of access to ***and activities in*** the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;

(f) ensure compliance and monitor the security measures referred to in this Article to mitigate potential security threats.

2. The health data access bodies shall ensure that electronic health data can be uploaded by ***health*** data holders and can be accessed by the ***health*** data user in a secure processing environment. The ***health data access bodies*** ~~data users~~ shall ~~only be~~ ***ensure by reviewing that the health data users are only*** able to download ~~non-personal~~ electronic health data ***in an anonymised statistical format*** from the secure processing environment.

3. The health data access bodies shall ensure regular ***third party*** audits of the secure processing environments.

3a. Where recognised data altruism organisations under Chapter IV of Regulation (EU) 2022/868 process personal electronic health data using a secure processing environment, such environments shall also comply with the security measures set out in point (a) to (f) in paragraph 1 in this Article.

4. The Commission shall, by means of implementing acts, provide for the technical, information security and interoperability requirements for the secure processing environments***, including the technical characteristics and tools available to the health data user within the secure processing environment***. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

Article 51

~~*Joint controllers*~~ ***Controllership***

1. ***The health data holder shall be deemed controller for the disclosure of the requested personal electronic health data to*** the health data access ~~bodies and the data users, including Union institutions, bodies, offices and agencies, body~~ ***pursuant to Article 35B(1) and (1a) of this Regulation. The health data access body shall be deemed controller for the processing of the personal electronic health data when fulfilling its tasks pursuant to Article 37(1)(a)(i) of this Regulation. The health data user*** shall be deemed ~~joint controllers of~~ ***controller for the processing of personal*** electronic health data ~~processed in accordance with~~***in pseudonymised form in the secure processing environment pursuant to its data permit and for the processing to generate an answer in an anonymised statistical form following a data request pursuant to Article 46. The health data access body shall be deemed to act as a processor for the health data user's processing pursuant to a*** data permit ***in the secure processing environment when providing such environment and for the processing to generate an answer to a data request pursuant to Article 46.***

1a. In situations referred to in Article 49, the single health data holder shall be deemed controller for its processing of personal electronic health data related to the providing of electronic health data to the health data user pursuant to a data permit or a data request. The single health data holder shall be deemed to act as a processor for the health data user's processing pursuant to a data permit when providing a secure processing environment to the health data user.

~~2. The Commission shall, by means of implementing acts, establish a template for the joint controllers' arrangement. Those implementing acts shall be adopted in accordance with the advisory procedure set out in Article 68(2).~~

SECTION 4

CROSS-BORDER ~~ACCESS TO~~ *INFRASTRUCTURE FOR SECONDARY USE OF* ELECTRONIC HEALTH DATA ~~FOR SECONDARY USE~~

Article 52

~~*Cross-border infrastructure for secondary use of electronic health data*~~ ***HealthData@EU***

1. Each Member State shall designate ~~a~~***one*** national contact point for secondary use of electronic health data***. The national contact point shall be an organisational and technical gateway, enabling and*** , responsible for making electronic health data available for secondary use in a cross-border context***. Each Member State*** ~~and~~ shall ~~communicate their names~~***inform the Commission the name*** and contact details ~~to the Commission~~***of the national contact point by the date of application of this Regulation***. The national contact point may be the coordinator health data access body pursuant to Article 36. The Commission and the Member States shall make this information publicly available.

1a. The Union data access service shall act as the Union Institutions', bodies, offices and agencies' contact point for secondary use of electronic health data and shall be responsible for making electronic health data available for secondary use.

2. The national contact points referred to in paragraph 1 ***and the Union Institutions' contact point referred to in paragraph 1A*** shall be authorised participants in the cross-border infrastructure for secondary use of electronic health data (HealthData@EU). The national contact points ***and the Union Institutions' contact point*** shall facilitate the cross-border access to electronic health data for secondary use for different authorised participants in the infrastructure***. The national contact points and the Union Institutions' contact point*** ~~and~~ shall cooperate closely with each other and with the Commission.

~~3. Union institutions, bodies, offices and agencies involved in research, health policy or analysis, shall be authorised participants of HealthData@EU.~~

3~~4~~. Health-related research infrastructures or similar structures whose functioning is based on Union law and which support the use of electronic health data for research, policy making, statistical, patient safety or regulatory purposes ~~shall~~ ***may*** be authorised participants of HealthData@EU.

4~~5~~. Third countries or international organisations may become authorised participants where they comply with the rules of Chapter IV of this Regulation***, the transfer stemming from such connection would comply with the rules in Chapter V of Regulation (EU) 2016/679 and they*** ~~and~~ provide access to ***health*** data users located in the Union, on equivalent terms and conditions, to the electronic health data available to their health data access bodies. The Commission ~~may~~ ***shall*** adopt implementing acts establishing that a national contact point of a third country or a system established at an international level is compliant with requirements of HealthData@EU for the purposes of secondary use of health data, is compliant with the Chapter IV of this Regulation and ***Chapter V of Regulation (EU) 2016/679 and*** provides access to ***health*** data users located in the Union to the electronic health data it has access to on equivalent terms and conditions. The compliance with these legal, organisational, technical and security requirements, including with the standards for secure processing environments pursuant to Article 50 shall be checked under the control of the Commission. These implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68 (2). The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available. ***When adopting the implementing act, the national security interests of Member States shall be taken into account.***

5~~6~~. Each authorised participant shall acquire the required technical capability to connect to and participate in HealthData@EU. Each participant shall comply with the requirements and technical specifications needed to operate the cross-border infrastructure and to allow the authorised participants to connect to each other within it.

~~7.~~ ~~The Commission is empowered to adopt delegated acts in accordance with Article 67 in order to amend this Article to add or remove categories of authorised participants in HealthData@EU, taking into account the opinion of the joint controllership group pursuant to Article 66 of this Regulation.~~

6~~8~~. The Member States and the Commission shall set up HealthData@EU to support and facilitate the cross-border access to electronic health data for secondary use, connecting the national contact points for secondary use of electronic health data of all Member States and authorised participants in that infrastructure ***and the central platform***.

~~9~~***7***. The Commission shall develop, deploy and operate a ***central and interoperability*** ~~core~~ platform for HealthData@EU by providing information technology services needed to ***support and*** facilitate the ~~connection~~ ***exchange of information*** between health data access bodies as part of the cross-border infrastructure for the secondary use of electronic health data. The Commission shall only process electronic health data on behalf of the ~~joint~~ controllers as a processor.

~~10~~***8***. Where requested by two or more health data access bodies ***or authorised participants in this infrastructure***, the Commission ~~may~~ ***shall*** provide a secure processing environment for data from more than one Member State compliant with the requirements of Article 50. Where two or more health data access bodies put electronic health data in the secure processing environment managed by the Commission, they shall be ~~joint controllers~~ ***controller*** and the Commission shall be processor.

~~11~~***9***. The authorised participants shall act as joint controllers of the processing operations in which they are involved carried out in HealthData@EU ***for which they determine the purpose and the means*** and the Commission shall act as a processor ***for the processing of electronic health data for the purposes of secondary use pursued by the health data user***.

10~~12.~~ Member States and the Commission shall seek to ensure interoperability of HealthData@EU with other relevant common European data spaces as referred to in Regulations ~~[…] [Data Governance Act COM/2020/767 final]~~***(EU) 2022/868*** and […] [Data Act COM/2022/68 final].

~~13~~***11***. The Commission ~~may~~ ***shall***, by means of implementing acts, set out:

(a) requirements, technical specifications, the IT architecture of HealthData@EU, conditions and compliance checks for authorised participants to join and remain connected to HealthData@EU and conditions for temporary or definitive exclusion from HealthData@EU;

(b) the minimum criteria that need to be met by the authorised participants in the infrastructure;

(c) the responsibilities of the ~~joint~~ controllers and processor(s) participating in the cross-border infrastructures;

(d) the responsibilities of the ~~joint~~ controllers and processor(s) for the secure environment managed by the Commission;

(e) common specifications for the interoperability and architecture concerning HealthData@EU with other common European data spaces.

Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

~~14~~***12.*** ***Subject to the outcome of the compliance check performed by the Commission concerning the fulfilment of the requirements in this Article, the Commission shall, by means of implementing act, take decisions to connect*** ~~The approval for~~ individual authorised ~~participant~~ ***participants*** to join ~~HealthData@EU~~***the infrastructure*** or to disconnect ~~a participant from the infrastructure~~ ***them. These implementing acts*** shall be ~~issued by the Joint Controllership group, based on the results of the compliance checks~~***adopted in accordance with the examination procedure referred to in Article 68(2)***.

Article 53

Access to cross-border registries or databases of electronic health data for secondary use~~Access to cross-border sources of electronic health data for secondary use~~

1. In the case of cross-border registries and databases, the health data access body in which the ***health*** data holder ***for the specific registry or database*** is registered shall be competent to decide on data access applications to provide access to electronic health data ***pursuant to a data permit***. Where ~~the registry has~~***such registries or databases have*** joint controllers, the health data access body that shall ***decide on the data access applications to*** provide access to electronic health data shall be the body in the Member State where one of the joint controllers is established.

2. Where registries or databases from a number of Member States organise themselves into a single network of registries or databases at Union level, the associated registries may designate ~~one of their members as~~ a coordinator to ensure the provision of data from the registries' network for secondary use. The health data access body of the Member State in which the coordinator of the network is located shall be competent to decide on the data access applications to provide access to electronic health data for the network of registries or databases.

~~3. The Commission may, by means of implementing acts, adopt the necessary rules for facilitating the handling of data access applications for HealthData@EU, including a common application form, a common data permit template, standard forms for common electronic health data access contractual arrangements, and common procedures for handling cross-border requests, pursuant to Articles 45, 46, 47 and 48. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).~~

~~*Article 54*~~

~~*Mutual recognition*~~

~~1. When handling an access application for cross-border access to electronic health data for secondary use, health data access bodies and relevant authorised participants shall remain responsible for taking decisions to grant or refuse access to electronic health data within their remit in accordance with the requirements for access laid down in this Chapter.~~

~~2. A data permit issued by one concerned health data access body may benefit from mutual recognition by the other concerned health data access bodies.~~

SECTION 5

HEALTH DATA QUALITY AND UTILITY FOR SECONDARY USE

Article 55

Dataset description ***and datasets catalogue***

1. The health data access ~~bodies~~***body*** shall***, through a publicly available and standardised machine-readable datasets catalogue, provide information, in the form of metadata,*** ~~inform the data users~~ about the available datasets and their characteristics ~~through a metadata catalogue.~~***. A description of*** each dataset shall include information concerning the source, the scope, the main characteristics, ***the*** nature of electronic health data and ***the*** conditions for making electronic health data available.

1a. The dataset descriptions in the national datasets catalogue of the Member States shall be available, at least, in an official language of the Union. The dataset catalogue for Union institutions provided by the Union data access service shall be available in all official languages of the Union.

1b. The datasets catalogue shall also be made available to single information points under Article 8 of Regulation (EU) 2022/868

2. The Commission shall, by means of implementing acts, set out the minimum ~~information~~ elements ***health*** data holders are to provide for datasets and their characteristics. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

Article 56

Data quality and utility label

1. Datasets made available through health data access bodies may have a Union data quality and utility label ~~provided~~ ***applied*** by the ***health*** data holders.

2. Datasets with electronic health data collected and processed with the support of Union or national public funding shall have a data quality and utility label, in accordance with the ~~principles~~ ***elements*** set out in paragraph 3.

3. The data quality and utility label shall ~~comply with~~ ***cover*** the following elements***, where applicable***:

   (a) for data documentation: meta-data, support documentation, data ~~model, data dictionary,~~***dictionary, format and*** standards used, provenance***, and when applicable, data model***;

   (b) ~~technical quality, showing the~~ ***for assessment of technical quality:*** completeness, uniqueness, accuracy, validity, timeliness and consistency of the data;

   (c) for data quality management processes: level of maturity of the data quality management processes, including review and audit processes, biases examination;

   (d) ***for assessment of*** coverage: ***time period, population coverage and, when applicable*** ~~representation of multi-disciplinary electronic health data~~, representativity of population sampled, ***and*** average timeframe in which a natural person appears in a dataset;

   (e) ***for*** information on access and provision: time between the collection of the electronic health data and their addition to the dataset, time to provide electronic health data following ***an*** ~~electronic health data access application approval~~;

(f) ***for*** information on data ~~enrichments~~ ***modifications*** : merging and adding data to an existing dataset, including links with other datasets~~;~~**.**

4. The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the list of ~~principles~~ ***elements*** for data quality and utility label. Such delegated acts may also amend the list set out under paragraph 3 by adding, modifying or removing requirements for data quality and utility label.

5. The Commission shall, by means of implementing acts, set out the visual characteristics and technical specifications of the data quality and utility label, based on the elements referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2). Those implementing acts shall take into account the requirements in Article 10 of Regulation […] [AI Act COM/2021/206 final] and any adopted common specifications or harmonised standards supporting those requirements***, where applicable***.

Article 57

EU Datasets Catalogue

1. The Commission shall establish ***and publicly provide*** an EU Datasets Catalogue connecting the national ~~catalogues of~~ datasets ***catalogues*** established by the health data access bodies ~~and other~~***in each Member State as well as datasets catalogues of*** authorised participants in HealthData@EU.

2. The EU Datasets Catalogue and the national datasets catalogues ***as well as datasets catalogues of authorised participants in HealthData@EU*** shall be made publicly available.

Article 58

Minimum dataset specifications

The Commission may, by means of implementing acts, determine the minimum specifications for ***datasets of high impact for the*** ~~cross-border datasets~~ for secondary use of electronic health data, taking into account existing Union infrastructures, standards, guidelines and recommendations. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

Chapter V
Additional actions

Article 59

Capacity building

The Commission shall support sharing of best practices and expertise, aimed to build the capacity of Member States to strengthen digital health systems for primary and secondary use of electronic health data. To support capacity building, the Commission shall ~~draw up benchmarking guidelines~~ ***in close cooperation and consultation with Member States establish indicators for self assessment*** for the primary and secondary use of electronic health data.

Article 60

Additional requirements for public procurement and Union funding

1. ~~Public procurers, national competent~~***Contracting*** authorities , including digital health authorities and health data access bodies~~,~~ and ***Union institutions, bodies, offices or agencies, including*** the Commission**,** shall make reference to the applicable technical specifications, standards and profiles as referred to in Articles 6***, 12***, 23, 50, ***52, 56, as well as to the requirements laid down in Regulations (EU) 2016/679 and (EU) 2018/1725, as*** ~~56, as~~ relevant, ~~as points of orientation~~ for public procurements and when formulating their

tender documents or calls for proposals, as well as when defining the conditions for Union funding regarding this Regulation, including enabling conditions for the structural and cohesion funds.

2. The ~~ex-ante conditionality for Union~~***criteria for obtaining*** funding ***from the Union*** shall take into account ~~the requirements developed in the framework of Chapters II, III and IV.~~**:**

a) the requirements developed in Chapters II, III and IV;

b) the requirements laid down in Regulations (EU) 2016/679 or (EU) 2018/1725, where applicable.

Article 60A

Storage of personal electronic health data by health data access bodies and secure processing environments

1. Health data access bodies, single data holders and the Union data access service shall store and process personal health electronic data in the European Union when performing pseudonymisation, anonymisation and any other personal data processing operations referred to in Articles 45 to 49, through secure processing environments within the meaning of article 50 and article 52(8) or through HealthData@EU. This requirement shall apply to any entity performing these tasks on their behalf. 2. By way of exception, the data referred to in paragraph 1 may be stored and processed in a third country, a territory or one or more specified sectors within that third country covered by an adequacy decision, pursuant to Article 45 of Regulation (EU) 2016/679.

Article 61

~~*Third country transfer of non-personal electronic data*~~ ***Transfer of anonymous electronic health data presenting a risk of re-identification to a third country or international organisation***

1. ~~Non-personal~~***Anonymous*** electronic ***health*** data made available by health data access bodies ***to a health data user or its contractor in a third country according to a data permit pursuant to Article 46 or a data request pursuant to Article 47 or to an authorised participants or its contractor in a third country or an international organisation***, that are based on a natural person's electronic ***health*** data falling within one of the categories of

Article 33 ~~[(a), (e), (f), (i), (j), (k), (m)]~~ shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation ~~[…] [Data Governance Act COM/2020/767 final]~~***(EU) 2022/868***, provided that their transfer to third countries presents a risk of ***becoming personal electronic health data allowing*** re-identification through means going beyond those ~~likely~~ reasonably ***likely*** to be used, ***in particular*** in view of the limited number of natural persons involved in that data, the fact that they are geographically scattered or the technological developments expected in the near future.

2. The protective measures for the categories of data mentioned in paragraph 1 shall ~~–~~ depend on the nature of the data and anonymization techniques and shall be detailed in the Delegated Act under the empowerment set out in Article 5(13) of Regulation ~~[…] [Data Governance Act COM/2020/767 final]~~***(EU) 2022/868*** .

Article 62

~~*International access and*~~ *Transfer of* ***anonymous*** ~~*non-personal*~~ *electronic health data* ***to a third country or an international organisation***

1. The digital health authorities, health data access bodies, the authorised participants in the cross-border infrastructures provided for in Articles 12 and 52 and ***health*** data users shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent ***transfer to a third country or an international organisation, including*** ~~international transfer or~~ governmental access ~~to non-personal~~ ***in a third country of anonymous*** electronic health data held in the Union where such transfer ~~or access~~ would create a conflict with Union law or the national law of the relevant Member State~~, without prejudice to paragraph 2 or 3 of this Article~~.

~~2. Any judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a digital health authority, health data access body or data users to transfer or give access to non-personal electronic health data within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State.~~

~~3.~~ ~~In the absence of an international agreement as referred to in paragraph 2 of this Article, where a digital health authority, a health data access body, data users is the addressee of a decision or judgment of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where:~~

~~(a) the third-country system requires the reasons and proportionality of such a decision or judgment to be set out and requires such a decision or judgment to be specific in character, for instance by establishing a sufficient link to certain suspected persons or infringements;~~

~~(b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and~~

~~(c) the competent third-country court or tribunal issuing the decision or judgment or reviewing the decision of an administrative authority is empowered under the law of that third country to take duly into account the relevant legal interests of the provider of the data protected under Union law or the national law of the relevant Member State~~

~~4.~~ ~~If the conditions laid down in paragraph 2 or 3 are met, digital health authority, a health data access body or a data altruism body shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation of the request.~~

~~5.~~ ~~The digital health authorities, health data access bodies, data users shall inform the data holder about the existence of a request of a third-country administrative authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.~~

Article 63

*~~International access and~~ **Additional conditions for** transfer of personal electronic health data **to a third country or an international organisation***

In the context of ~~international access and~~ transfer of personal electronic health data ***to a third country or an international organisation***, Member States may maintain or introduce further conditions, including limitations, in accordance with and under the conditions of Article 9(4) of ***Regulation (EU) 2016/679, in addition to the requirements set out in Articles 13(3) and 52(5) of this Regulation and the requirements laid down in Chapter V of*** ~~the~~ Regulation (EU) 2016/679.

Chapter VI
European governance and coordination

Article 64

European Health Data Space Board (EHDS Board)

1. A European Health Data Space Board (EHDS Board) is hereby established to facilitate cooperation and the exchange of information among Member States ***and the Commission***. The EHDS Board shall be composed of ~~the high level~~ representatives of ~~digital health authorities and health data access bodies of all the Member States. Other~~ national authorities~~, including market surveillance authorities referred to in Article 28, European Data Protection Board and European Data Protection Supervisor may be invited to the meetings, where the issues discussed are of relevance for them. The Board may also invite experts and observers to attend its meetings, and may cooperate with other external experts as appropriate. Other Union institutions, bodies, offices and agencies, research infrastructures and other similar structures~~ ***nominated by each Member State. Each Member State*** shall have ~~an observer role~~***one vote***.

1a. A representative of the Commission and a representative of the Member States shall co-chair the meetings of the EHDS Board.

1b. ***Market surveillance authorities referred to in Article 28, European Data Protection Board and European Data Protection Supervisor, maybe invited to the meetings, where the issues discussed are of relevance for them.***

1c. ***The Board may also invite other national authorities, experts and observers, as well as other Union institutions, bodies, offices and agencies, research infrastructures and other similar structures to attend its meetings. When these participants are invited, they shall have an observer role***

1d. ***The Board may cooperate with other external experts as appropriate.***

1e. ***Stakeholders and relevant third parties, including patients' representatives, maybe invited to attend meetings of the EHDS Board and to participate in its work, depending on the topics discussed and their degree of sensitivity.***

2. Depending on the functions related to the use of electronic health data, the EHDS Board may work in subgroups ***for certain topics***, where digital health authorities or health data access bodies ***shall be represented. The subgroups*** ~~for a certain area~~ shall ~~be represented~~***support the EHDS Board with specific expertise***. The subgroups may have joint meetings, as required.

3. ***The EHDS Board shall adopt its rules of procedures on the basis of a proposal of the Commission. A two-thirds majority is required for the rules of procedures to be adopted. The rules of procedures shall include rules pertaining to*** the composition, ~~organisation, functionings~~***structure, operation*** and cooperation of the sub-groups ***and*** shall ~~be set out in the~~ ***regulate the role of invitees referred to in paragraphs 1b to 1e, taking into account the topics under discussion and the level of confidentiality involved. Regarding voting*** rules***, the EHDS Board shall deliberate by consensus as far as possible. If consensus cannot be reached the EHDS Board shall deliberate by a majority of two thirds of the Member States representatives. Each member shall have one vote*** ~~of procedure put forward by the Commission~~.

~~4. Stakeholders and relevant third parties, including patients' representatives, shall be invited to attend meetings of the EHDS Board and to participate in its work, depending on the topics discussed and their degree of sensitivity.~~

5. The EHDS Board shall cooperate with other relevant bodies, entities and experts, such as the European Data Innovation Board referred to in Article ~~26 of Regulation […] [Data Governance Act COM/2020/767 final~~***29 of Regulation 2022/868***], competent bodies set up under Article 7 of Regulation […] [Data Act COM/2022/68 final], supervisory bodies set up under Article 17 of Regulation […] [eID Regulation], European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679***, cybersecurity bodies, and the European Open Science Cloud, in the effort of reaching advanced solutions for the FAIR data usage in research and innovation*** ~~and cybersecurity bodies~~.

~~6. The Commission shall chair the meetings of the EHDS Board.~~

7. The EHDS Board shall be assisted by a secretariat provided by the Commission.

8. The Commission shall, by means of implementing acts, adopt the necessary measures for the establishment~~, management and functioning~~ ***and management*** of the EHDS Board. Those implementing acts shall be adopted in accordance with the ~~advisory~~ ***examination*** procedure referred to in Article 68(2).

Article 65

Tasks of the EHDS Board

1. The EHDS Board shall have the following tasks relating to the primary use of electronic health data in accordance with Chapters II and III:

   (a) to assist Member States in coordinating practices of digital health authorities;

   (b) to issue written contributions and to exchange best practices on matters related to the coordination of the implementation at Member State level of this Regulation and of the delegated and implementing acts adopted pursuant to it, in particular as regards:

      (i) the provisions set out in Chapters II and III;

      (ii) development of online services facilitating secure access, including secure electronic identification, to electronic health data for health professionals and natural persons;

      ~~(iii) other aspects of the primary use of electronic health data.~~

(c) to facilitate cooperation between digital health authorities through capacity-building, establishing the structure for ~~annual~~ ***biennial*** activity reporting, ~~peer-review of annual activity~~***and exchange of information in those*** reports ~~and exchange of information~~;

(d) to share information concerning risks posed by EHR systems and serious incidents as well as their handling;

(e) to facilitate the exchange of views on the primary use of electronic health data with the relevant stakeholders, including representatives of patients, health professionals, researchers, regulators and policy makers in the health sector.

2. The EHDS Board shall have the following tasks related to the secondary use of electronic health data in accordance with Chapter IV:

(a) to assist Member States in coordinating practices of health data access bodies in the implementation of provisions set out in Chapters IV, to ensure a consistent application of this Regulation;

(b) to issue written contributions and to exchange best practices on matters related to the coordination of the implementation at Member State level of this Regulation and of the delegated and implementing acts adopted pursuant to it, in particular as regards:

(i) implementation of rules for access to electronic health data;

(ii) technical specifications or existing standards regarding the requirements set out in Chapter IV;

(iii) incentives policy for promoting data quality and interoperability improvement;

(iv) policies concerning fees to be charged by the health data access bodies and ***health*** data holders;

(v) the establishment and application of penalties;

~~(vi) other aspects of the secondary use of electronic health data.~~

(c) to facilitate cooperation between health data access bodies through capacity-building, establishing the structure for ~~annual~~***biennial*** activity reporting, ~~peer-review of annual activity reports and~~ ***and*** exchange of information ***in those reports***;

(d) to share information concerning risks and ~~data protection~~ incidents related to secondary use of electronic health data, ***such as risks and incidents in the secure processing environment as referred to in Article 50,*** as well as their handling;

~~(e) to contribute to the work of the European Data Innovation Board to be established in accordance with Article 29 of the Regulation […] [Data Governance Act COM/2020/767 final];~~

(f) to facilitate the exchange of views on the secondary use of electronic health data with the relevant stakeholders, including ***health data holders, health data users,*** representatives of patients, health professionals, researchers, regulators and policy makers in the health sector.

3. The EHDS Board shall be consulted by the European Commission in the preparation of draft delegated acts before their adoption pursuant to the procedure laid down in Article 67, and in the preparation of draft implementing acts before presenting them to the committee referred to in Article 68.

Article 66

*~~Joint controllership~~**The Steering** Groups for ~~Union~~**the** infrastructures **MyHealth@EU and HealthData@EU***

1. ~~The Commission shall establish two groups dealing with joint controllership~~ ***Two Steering groups are hereby established*** for the cross-border infrastructures provided for in Articles 12 and 52~~. The groups~~***; the MyHealth@EU Steering group and the HealthData@EU Steering group. Each group*** shall be composed of ~~the representatives~~***one representative per Member State*** of the ***respective*** national contact points ~~and other authorised participants in those infrastructures~~.

1a. The Steering groups shall take operational decisions concerning the development and operation of the cross-border infrastructures referred to in Chapters II and IV, on

changes of infrastructure, adding additional infrastructures or services, or ensuring interoperability with other infrastructures, digital systems or data spaces. The groups shall also state their view on accepting individual authorised participants to join the infrastructures or to disconnect them.

1b. ***The Steering Groups shall take decisions by consensus. Where consensus cannot be reached, the adoption of a decision shall require the support of members representing two-thirds majority, where each Member State has one vote.***

2. The composition, organisation, functioning and cooperation of the ~~sub-groups~~***Steering groups*** shall be set out in the rules of procedure adopted by those groups.

3. ~~Stakeholders and relevant third parties, including patients' representatives,~~ ***Other authorised participants*** may be invited to ~~attend meetings of the groups and to participate in their work~~***exchange information and views on relevant matters related to the cross-border infrastructures respectively provided for in Articles 12, 13 and 52. When these participants are invited, they shall have an observer role***.

3a. ***Stakeholders and relevant third parties, including patients' representatives, may be invited to attend meetings of the groups and to participate in their work.***

4. The groups shall elect chairs for their meetings.

5. The groups shall be assisted by a secretariat provided by the Commission.

~~6.~~ ~~The groups shall take decisions concerning the development and operation of the cross-border infrastructures pursuant to Chapters II and IV, on changes of infrastructure, adding additional infrastructures or services, or ensuring interoperability with other infrastructures, digital systems or data spaces. The group shall also take decisions to accept individual authorised participants to join the infrastructures or to disconnect them.~~

Article 66A

Roles and responsibilities of the Commission regarding the functioning of the European Health Data Space

1. ***In addition to its role in making available electronic health data held by Union institutions, bodies, or agencies, in accordance with 36, 36A, 52(1A) and its tasks under Chapter III, including Article 26A, the Commission shall provide the development, maintenance, hosting and operation of the infrastructures and all central services required to support the functioning of the European Health Data Space, to all relevant connected entities:***

i. an interoperable, cross-border identification and authentication mechanism for natural persons and health professionals, in accordance with Article 9(3) and (4);

ii. the central services and infrastructures for digital health of MyHealth@EU, in accordance with Article 12(1);

iii. compliance checks for connecting authorised participants to MyHealth@EU, in accordance with Article 12(9);

iv. the additional cross-border digital health services and infrastructures within the meaning of Article 13(1) of this Regulation

v. as part of HealthData@EU, a service to submit applications for making available electronic health data from health data holder in multiple Member States or from other authorised participants and to automatically forward them to the relevant contact points, in accordance with Article 45(5A);

vi. the central services and infrastructures of HealthData@EU in accordance with Article 52, paragraphs (6) and (7);

vii. a secure processing environment in accordance with Article 52(8), in which health data access bodies may decide to make data available in accordance with Article 46(5A);

viii. compliance checks for connecting authorised participants to HealthData@EU, in accordance with Article 52(12);

ix. a federated EU dataset catalogue connecting the national dataset catalogues, in accordance with Article 57;

x. a secretariat for the EHDS Board, in accordance with Article 64(7);

xi. a secretariat for the steering groups, in accordance with Article 66(5).

2 The services referred to in paragraph 1 shall meet sufficient quality standards in terms of availability, security, capacity, interoperability, maintenance, monitoring and evolution to ensure an effective functioning of the European Health Data Space. The Commission shall provide them in accordance with the operational decisions of the relevant Steering Groups. These standards, once defined, shall apply to subcontractors of the Commission.

3. ***The Commission shall adopt, by means of implementing acts, the rules and measures for the operation of the infrastructures and all required central services of the European Health Data Space with the required quality of service, simultaneously with the adoption of the implementing acts referred to in Articles 12, 13 and 52. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).***

4. The Commission shall issue a biennial public report on the infrastructures and services supporting the European Health Data Space that it provides in accordance with paragraph 1.

CHAPTER VII

Delegation and Committee

Article 67

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 5(2), ~~10(3), 25(3), 32(4), 33(7), 37(4), 39(3), 41(7), 45(7), 46(8), 52(7),~~***~~32(4), and~~*** 56(4) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The power to adopt delegated acts referred to in Articles 5(2), ~~10(3), 25(3), 32(4), 33(7), 37(4), 39(3), 41(7), 45(7), 46(8), 52(7),~~***~~32(4) and~~*** 56(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the ***~~Official Journal of the European Union~~***~~Official Journal of the European Union~~ or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 5(2), ~~10(3), 25(3), 32(4), 33(7), 37(4), 39(3), 41(7), 45(7), 46(8), 52(7),~~***~~32(4), and~~*** 56(4) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of 3 months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both

informed the Commission that they will not object. That period shall be extended by 3 months at the initiative of the European Parliament or of the Council.

Article 68

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article ~~4~~***5*** of Regulation (EU) No 182/2011 shall apply.

Chapter VIII
Miscellaneous

Article 69

Penalties

In addition to the measures laid down in Articles 30 and 43 of this Regulation and Chapter VIII of Regulation (EU) 2016/679, Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties shall be effective, proportionate and dissuasive. ~~Member States shall notify the Commission of those rules and measures by date of application of this Regulation and shall notify the Commission without delay of any subsequent amendment affecting them.~~

Member States shall take into account the following non-exhaustive and indicative criteria for the imposition of penalties for infringements of this Regulation, where appropriate:

(a) the nature, gravity, scale and duration of the infringement;

(b) any action taken by the infringer to mitigate or remedy the damage caused by the infringement;

(c) any previous infringements by the infringer;

(d) the financial benefits gained or losses avoided by the infringer due to the infringement, insofar as such benefits or losses can be reliably established;

(e) any other aggravating or mitigating factors applicable to the circumstances of the case;

(f) infringer's annual turnover of the preceding financial year in the Union.

3. Member States shall notify the Commission of those rules and measures by date of application of this Regulation and shall notify the Commission without delay of any subsequent amendment affecting them.

Article 70

~~Evaluation, and review~~ ***and progress report***

1. After ~~5~~ ***7*** years from the entry into force of this Regulation, the Commission shall carry out a targeted evaluation of this Regulation ~~especially with regards to Chapter III~~, and submit a report on its main findings to the European Parliament and to the Council, the European Economic and Social Committee and the Committee of the Regions, accompanied, where appropriate, by a proposal for its amendment. The evaluation shall include ~~an assessment of the self-certification of EHR systems and reflect on the need to introduce a conformity assessment procedure performed by notified bodies.~~***the following:***

(a) an assessment of the certification framework of EHR systems in Chapter III and of the need to introduce further tools regarding conformity assessment ;

(aa) an assessment of the functioning of the Internal Market for the EHR systems;

(b) an assessment of the costs and benefits of implementation of the provisions for secondary use laid out in Chapter IV.

2. After ~~7~~ ***9*** years from the entry into force of this Regulation, the Commission shall carry out an overall evaluation of this Regulation, and submit a report on its main findings to the European Parliament and to the Council, the European Economic and Social Committee

and the Committee of the Regions, accompanied, where appropriate, by a proposal for its amendment.

3. Member States shall provide the Commission with the information necessary for the preparation of that report ***and the Commission shall take this information duly into account in that report***.

4. ***Every year following the entry into force of this Regulation and until its full application, the Commission shall submit a progress report to the Council on the state of play of the preparations for the full implementation of this Regulation. The report shall contain information about the degree of progress and the readiness of the Member States including an assessment of the feasibility of reaching the time frames laid down in Article 72 of this Regulation. The report may also contain recommendations to Member States to improve preparedness for the application of this Regulation.***

Article 71

Amendment to Directive 2011/24/EU

Article 14 of Directive 2011/24/EU is deleted.

Chapter IX

Deferred application, *transitional* and final provisions

Article 72

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

~~It~~ ***This Regulation*** shall apply ~~from 12 months~~ ***2 years*** after ~~its~~ entry into force***, unless provided otherwise in paragraph 2***.

2. ~~However, Articles 3, 4, 5, 6, 7, 12, 14, 23 and 31~~***Articles 2A, 5, 6, 7A, 7B, 8A, 8B, 8C, 8D, 8E, 8F, 8G, 12, 13A, 13B, 14, 23, 31 and 32 in Chapters II and III*** shall apply as follows:

(a) from ~~1 year~~***5 years*** after date of entry into ~~application~~ ***force*** to categories of personal electronic health data referred to in Article 5(1), points (a), (b) and (c), and to EHR systems intended by the manufacturer to process such categories of data~~.~~;

(b) from ~~3~~***7*** years after date of entry into ~~application~~ ***force*** to categories of personal electronic health data referred to in Article 5(1), points (d), (e) and (f), and to EHR systems intended by the manufacturer to process such categories of data;

(c) from ***1 year after*** the date established in ***a*** delegated ~~acts~~***act*** pursuant to Article 5(2) for ~~other~~***amendments of the main characteristics of personal electronic health data in Annex 1, provided that this date of entry into application is subsequent to the date of entry into application referred to in point (a) and (b) for the*** categories of personal electronic health data ***concerned***.

The implementing acts referred to in Articles 2A(3), 6(1), 12(4) and 23(1) shall be adopted within 1 year after date of entry into force and apply as referred to in subparagraph 1 in this paragraph.

Chapter III shall apply to EHR systems put into service in the Union ~~pursuant to~~ ***referred to in*** Article ~~15(2) from 3~~ ***13B(2) from 7*** years after date of entry into ~~application~~***force***.

~~This Regulation~~ ***Chapter IV*** shall ~~be binding in its entirety and directly applicable in all Member States~~ ***apply from 5 years after date of entry into force, except Article 33(1), points (b) (e), (ea) (j), (l) and (n) which shall apply from 7 years after date of entry into force and article 52(4) which shall apply from 10 years after the data of entry into force.***

The implementing acts referred to in Articles 35F(5), 50(4), 52(13), 53(3), 55 and 56(5) shall be adopted within 2 year after date of entry into force and apply from 4 years after this Regulation enter into force.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg,

For the European Parliament
The President

For the Council
The President

Annex I

Main characteristics of ***priority categories of personal*** electronic health data ~~categories~~***for primary use***

Electronic health data category	Main characteristics of electronic health data included under the category
1. Patient summary	Electronic health data that includes important clinical facts related to an identified person and that is essential for the provision of safe and efficient healthcare to that person. The following information is part of a patient summary: 1. Personal details 2.- Contact information 3.- Information on insurance 4.- Allergies 5. Medical alerts 6. Vaccination/prophylaxis information, possibly in the form of a vaccination card 7.- Current, resolved, closed or inactive problems 8.- Textual information related to medical history 9. Medical devices and implants 10. Procedures 11. Functional status 12. Current and relevant past medicines 13. Social history observations related to health 14. Pregnancy history 15. Patient provided data 16. Observation results pertaining to the health condition 17. Plan of care 18. Information on a rare disease such as details about the impact or characteristics of the disease
2. Electronic prescription	Electronic health data constituting a prescription for a medicinal product as defined in Article 3(k) of Directive 2011/24/EU.
3. Electronic dispensation	Information on the supply of a medicinal product to a natural person by a pharmacy based on an

	electronic prescription.
4. Medical image and image report	Electronic health data related to the use of or produced by technologies that are used to view the human body in order to prevent, diagnose, monitor, or treat medical conditions.
5. Laboratory result	Electronic health data representing results of studies performed notably through in vitro diagnostics such as clinical biochemistry, haematology, transfusion medicine, microbiology, immunology, and others, and including, where relevant, reports supporting the interpretation of the results.
6. Discharge report	Electronic health data related to a healthcare encounter or episode of care and including essential information about admission, treatment and discharge of a natural person.

Annex II

Essential requirements for ***the harmonised components of*** EHR systems and products claiming interoperability with EHR SYSTEMS

The essential requirements laid down in this Annex shall apply mutatis mutandis to ***medical devices, in vitro diagnostic medical devices, AI systems, and wellness apps*** ~~products~~ claiming interoperability with EHR systems.

1. General requirements

1.1. ***The harmonised components of*** an electronic health record system (EHR system) shall achieve the performance intended by its manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, ~~it is~~***they are*** suitable for ~~its~~***their*** intended purpose and ~~its~~***their*** use does not put at risk patient safety.

1.2. ~~An~~***The harmonised components of the*** EHR system shall be designed and developed in such a way that ~~it~~***the system*** can be supplied and installed, taking into account the instructions and information provided by the manufacturer, without adversely affecting its characteristics and performance during its intended use.

1.3. ~~An EHR system shall be designed and developed in such a way that its interoperability, safety and security features uphold the rights of natural persons, in line with the intended purpose of the EHR system, as set out in Chapter II of this Regulation.~~

1.4. ***The harmonised components of*** an EHR system that is intended to be operated together with other products, including medical devices, shall be designed and manufactured in such a way that interoperability and compatibility are reliable and secure, and personal electronic health data can be shared between the device and the EHR system ***in relation to those two components***.

2. Requirements for interoperability

2.1. ~~An EHR system shall allow personal electronic health data to be shared between health professionals or other entities from the health system, and between health professionals and patient or health professional portals in a commonly used electronic interoperable format, which includes, inter-alia, dataset content, data structures, formats, vocabularies,~~

~~taxonomies, exchange formats, standards, specifications, profiles for exchange and code lists, thus enabling system to system communication.~~

2.1.a. ***Where an EHR system is designed to store or intermediate personal electronic health data, it shall provide an interface enabling access to the personal electronic health data processed by it in the European health record exchange format, by means of the European interoperability component for EHR systems.***

2.1.b. ***Where an EHR system is designed to store or intermediate personal electronic health data, it shall be able to receive personal electronic health data in the European health record exchange format, by means of the European interoperability component for EHR systems.***

2.1.c. ***Where an EHR system is designed to provide access to personal electronic health data, it shall be able to receive personal electronic health data in the European health record exchange format, by means of the European interoperability component for EHR systems.***

2.2. ~~An EHR system shall be interoperable and compatible with the European infrastructures set out in this Regulation for the cross-border sharing of electronic health data.~~

2.3. An EHR system that includes a functionality for entering structured personal electronic health data shall enable the entry of data ~~structured in a structured way that supports the data sharing in a structured, commonly used and machine-readable format, enabling system to system communication~~ ***with granularity sufficient to enable the provision of the entered personal electronic health data in the European health record exchange format***.

2.4. ***The harmonised components of*** an EHR system shall not include features that prohibit, restrict or place undue burden on authorised access, personal electronic health data sharing, or use of personal electronic health data for permitted purposes.

2.5. ***The harmonised components of*** an EHR system shall not include features that prohibit, restrict or place undue burden on authorised exporting of personal electronic health data for the reasons of replacing the EHR system by another product.

3. Requirements ***for logging***

3.1. ~~An EHR system shall be designed and developed in such a way that it ensures safe and secure processing of electronic health data, and that it prevents unauthorised access to such data.~~

3.2. ~~An EHR system designed to be used by health professionals shall provide reliable mechanisms for the identification and authentication of health professionals, including checks on professional rights and qualifications.~~

3.3. ~~An EHR system designed to be used by health professionals shall support the use of information on professional rights and qualifications as part of the access control mechanisms, such as role-based access control.~~

3.4. ***The harmonised logging component of*** an EHR system designed to enable access by health ~~professionals~~ ***providers*** or other individuals to personal electronic health data shall provide sufficient logging mechanisms that record, at least the following information on every access event or group of events:

(a) identification of the health ~~professional~~ ***provider*** or other ***individuals*** having accessed ***personal*** electronic health data;

(b) identification of the ***specific*** individual ***or individuals having accessed personal electronic health data***;

(c) categories of data accessed;

(d) time and date of access;

(e) origin(s) of data.

3.5. ~~An EHR system shall include tools and mechanism to allow natural persons to restrict health professionals' access to their personal electronic health data. It shall also include mechanisms that allow access to personal electronic health data in emergency situations, and ensure that access is strictly logged.~~

3.6. ***The harmonised components of*** an EHR system shall include tools or mechanisms to review and analyse the log data, or it shall support the connection and use of external software for the same purposes.

3.7. ~~An EHR system designed to be used by health professionals shall support digital signatures or similar non-repudiation mechanisms.~~

3.8. ***The harmonised components of*** an EHR system ~~designed for the storage of~~***that store personal*** electronic health data shall support different retention periods and access rights that take into account the origins and categories of electronic health data.

3.9. ~~An EHR system designed to be used by natural persons shall enable their identification using any recognised electronic identification means as defined in Regulation (EU) No 910/2014, regardless of the Member State that has issued it. If the service supports other electronic identification means, they shall be of assurance levels 'substantial' or 'high'.~~

Annex III

Technical documentation

The technical documentation referred to in Article 24 shall contain at least the following information, as applicable to the ***harmonised components of EHR systems in the*** relevant EHR system:

1. A detailed description of the EHR system including:

   (a) its intended purpose, the date and the version of the EHR system;

   (b) the categories of ***personal*** electronic health data that the EHR system has been designed to process;

   (c) how the EHR system interacts or can be used to interact with hardware or software that is not part of the EHR system itself;

   (d) the versions of relevant software or firmware and any requirement related to version update;

   (e) the description of all forms in which the EHR system is placed on the market or put into service;

   (f) the description of hardware on which the EHR system is intended to run;

   (g) a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing, including where appropriate, labelled pictorial representations (e.g. diagrams and drawings), clearly indicating key parts/components and including sufficient explanation to understand the drawings and diagrams;

   (h) the technical specifications, such as features, dimensions and performance attributes, of the EHR system and any variants/configurations and accessories that would typically appear in the product specification made available to the user, for example in brochures, catalogues and similar publications, including a detailed description of the data structures, storage and input/output of data;

(i) a description of any change made to the system throughout its lifecycle;

(j) the instructions of use for the user and, where applicable, installation instructions.

2. A detailed description of the system in place to evaluate the EHR system performance, where applicable.

3. The references to any common specification used in accordance with Article 23 and in relation to which conformity is declared.

4. The results and critical analyses of all verifications and validation tests undertaken to demonstrate conformity of the EHR system with the requirements laid down in Chapter III of this Regulation, in particular the applicable essential requirements;.

5. A copy of the information sheet referred to in Article 25.

6. A copy of the EU declaration of conformity.

Annex IV

EU declaration of conformity

The EU declaration of conformity ***for the harmonised components of EHR systems*** shall contain all of the following information:

1. The name of the EHR system, version and any additional unambiguous reference allowing identification of the EHR system.

2. Name and address of the manufacturer or, where applicable, their authorised representative.

3. A statement that the EU declaration of conformity is issued under the sole responsibility of the manufacturer.

4. A statement that the EHR system in question is in conformity with the provisions laid down in Chapter III of this Regulation and, if applicable, with any other relevant EU legislation that provides for the issuing of an EU declaration of conformity***, complemented by the result from the testing environment mentioned in article 26A obtained for the EHR system.***

5. References to any relevant ~~harmonized~~ ***harmonised*** standards used and in relation to which conformity is declared.

6. References to any common specifications used and in relation to which conformity is declared.

7. Place and date of issue of the declaration, signature plus name and function of the person who signed, and, if applicable, an indication of the person on whose behalf it was signed.

8. Where applicable, additional information.