Council of the
European Union

Brussels, 22 March 2024
(OR. en)

7567/24

Interinstitutional File:
2022/0140(COD)

SAN 140
PHARM 42
COMPET 296
MI 282
DATAPROTECT 135
CODEC 744

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. Cion doc.:	8751/22 + ADD 1-8
Subject:	Proposal for a Regulation on the European Health Data Space - Letter to the Chairs of the European Parliament Committees on Environment, Public Health and Food Safety (ENVI) and on Civil Liberties, Justice and Home Affairs (LIBE)

Following the meeting of the Permanent Representatives Committee on 22 March 2024, which endorsed the final compromise text with a view to agreement, delegations are informed that the Presidency sent the attached letter, together with its Annex, to the Chairs of the European Parliament Committees on Environment, Public Health and Food Safety (ENVI) and on Civil Liberties, Justice and Home Affairs (LIBE).

Council of the European Union

SGS 24 / 001657

Brussels, 22/03/2024

Mr Pascal CANFIN
Chair of the Committee on the Environment, Public Health and Food Safety

Mr Juan Fernando LÓPEZ AGUILAR
Chair of the Committee on Civil Liberties, Justice and Home Affairs

European Parliament
Rue Wiertz 60
B-1047 BRUSSELS

Subject: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space

Dear Mr CANFIN, Dear Mr. LÓPEZ AGUILAR,

Following the informal negotiations on this proposal between the representatives of the three institutions, today the Permanent Representatives Committee agreed with the final compromise text.

I am therefore now in a position to inform you that, should the European Parliament adopt its position at first reading, in accordance with Article 294(3) TFEU, in the exact form of the text set out in the Annex to this letter (subject to revision by the lawyer-linguists of the two institutions), the Council, in accordance with Article 294(4) TFEU, will approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the position of the European Parliament.

On behalf of the Council, I also wish to thank you for your close cooperation which should enable us to reach agreement on this file at first reading.

Yours sincerely

Pierre CARTUYVELS
Chair of the
Permanent Representatives Committee (Part 1)

Copy:
- Ms Stella KYRIAKIDES, Commissioner
- Mr Tomislav SOKOL, European Parliament co-rapporteur
- Ms Annalisa TARDINO, European Parliament co-rapporteur

Rue de la Loi/Wetstraat 175 – 1048 Bruxelles/Brussel – Belgique/België
Tél./Tel. +32 (0)2 281 61 11

REGULATION (EU) 2024/…

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,

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

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 ***to better achieve*** other purposes ***in the healthcare and care sector*** that would benefit ▌society***,*** such as research, innovation, policy-making, ***health threats preparedness and response including to prevent and address future pandemics,*** patient safety, personalised medicine, official statistics or regulatory activities (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 ***and technical*** framework in particular for the development, marketing and use of electronic health record systems ('EHR systems') in conformity with Union values***. The EHDS is a key component in the creation of a strong and resilient European Health Union***.

(2) The COVID-19 pandemic has highlighted the imperative of having timely access to ***quality*** electronic health data for health threats preparedness and response, as well as for ***prevention,*** diagnosis and treatment and secondary use of health data. Such timely access ***can potentially contribute***, through efficient public health surveillance and monitoring, to ▌more effective management of ***future pandemics, to a reduction of costs and to improving the response to health threats***, and ultimately ***can help*** to save ***more*** 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 ***and consistent*** approach at Member States and Union level***, both for improving the availability of electronic health data for healthcare as well as to facilitate access to electronic health data in order to steer effective policy responses and contribute to high standards of human health***.

(3) The COVID-19 crisis strongly anchored the work of the eHealth Network, a voluntary

---

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).

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***, while respecting the principle of data minimisation***. 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.

(3a) Given the sensitivity of personal health data, this Regulation seeks to provide sufficient safeguards at both Union and national level to ensure a high degree of data protection, security, confidentiality and ethical use. Such safeguards are necessary to promote trust in safe handling of the health data of natural persons for primary and secondary uses.

(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**,** bodies, ***offices and agencies*** 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, ***offices and agencies,*** 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

---

4 EOSC Portal (eosc-portal.eu).

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).

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, ***health threat assessment,*** 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.

(5b) 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, and other medical data, spread between different entities from the health system (general practitioners, hospitals, pharmacies, care services). In order to enable that electronic health data are 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 access to their own personal electronic health data and are empowered to share it. In this respect, appropriate actions at Union and national level

should be taken as a means of reducing fragmentation, heterogeneity, and division and to achieve a system that is user-friendly and intuitive in all 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, including people with disabilities.

(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 ***complements*** some of them ▌ 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 ***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 additional 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***.

▌

(8) ***The rights conferred by Regulation (EU) 2016/679 should continue to apply.*** The right of access to data by a natural person, established by Article 15 of Regulation (EU) 2016/679, should be further ***complemented*** in the health sector. Under Regulation (EU) 2016/679, controllers do not have to provide access immediately. ▌ 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 ***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*** 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 the defined priority categories of personal electronic health data, such***

as the patient summary, through an electronic health data access service. This right should be implemented 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 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 should be limited to the categories of data falling within its scope, be exercised via an electronic health data access service, and provide an immediate answer. Rights under Regulation (EU) 2016/679 should still apply, allowing individuals to benefit from the rights under both frameworks. In particular, the right to obtain a paper copy of the electronic health data should remain, as this is one of the rights provided under Regulation (EU) 2016/679.

(9) At the same time, it should be considered that immediate access ***of natural persons*** to certain types of ***their*** personal electronic health data may be harmful for the safety of natural persons ▌ or ***unethical***. 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, ***it*** should be ***possible to delay the provision of this access in*** such ***situations*** for a limited ***amount of time, for instance until the moment*** where ***the patient and the*** health ***professional get in contact.*** Member States ▌ 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***.

(9a) This Regulation does not affect Member States competences concerning the initial registration of personal electronic health data, such as making the registration of genetic data subject to the natural person's consent or other safeguards. Member States may require that data is made available in an electronic format prior to the application to this regulation. This should not affect the obligation to make personal electronic health data, registered after the application of this Regulation, available in an electronic format.

(10) ***Natural persons should be able*** 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***. Information inserted by natural persons may not be as reliable as electronic health data entered and verified by health professionals ***and does not have the same clinical or legal value as information provided by a health professional.*** Therefore***,*** it should be clearly ***distinguishable from*** data ***provided by professionals. This possibility for*** natural persons to ***add*** and ***complement personal*** electronic health data ▌ should ***not entitle them to change personal*** electronic health data ***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, through an electronic health data access service. Such rectification requests should then be treated by the relevant data controllers in line with Regulation (EU) 2016/679, if necessary involving health professionals with a relevant specialisation, responsible for the natural persons' treatment.

(11) ▌ Under ***Article 20 of*** Regulation (EU) 2016/679, ***the right to data*** portability is limited ▌ to data processed based on consent or contract ***and*** provided by the data subject to a controller ▌ . ***Additionally,*** 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. ***This right should be complemented under this Regulation, thereby empowering natural persons at least to exchange*** and ***to provide access to at least priority categories*** of ***their personal electronic health data to the health professionals of their choice,*** and ***to download such health data***. ***In addition,*** natural ***persons should have the right to request a healthcare provider to transmit a part of their electronic health data to a clearly identified recipient in the social security or reimbursement services sector. Such a transfer should be one-way only***.

(12) ▌ The framework laid down by this Regulation ***should build*** on 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*** 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***.

(12a) The access to personal health records by healthcare providers or other individuals should be transparent to natural persons. The health data access services should provide detailed information on accesses to data, such as when and which entity or individual accessed which data. Natural persons should also be able to enable or disable automatic notifications regarding access to their health data through the health professional access services. 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. ***This may especially be relevant in cases of sensitive health problems such as those related to mental or sexual health, sensitive procedures such as abortions, or data on specific medications which could reveal other sensitive issues.*** Such selective sharing of personal electronic health data should be ***therefore*** supported ***and implemented through*** restrictions ***set by the natural person in the same way within a Member State and for cross-border data sharing. These restrictions should allow for sufficient granularity to restricts parts of datasets, such as components of the patient summaries. Before setting the restrictions,*** natural ***persons should be informed*** of ▌ the ***patient safety risks associated with limiting access to health data.*** Because the unavailability of the restricted personal electronic health data may impact the provision or quality of health services provided to the natural person, ***they*** should assume responsibility for the fact that the healthcare provider cannot take the data into account when providing health services. ***However, such restrictions may have life threatening consequences and, therefore, access to personal electronic health data should be possible to protect vital interests in emergency situations. More specific legal provisions on the mechanisms of restrictions placed by the natural person on parts of their personal electronic health data could be provided by Member States in national law, in particular as regards medical liability in the event that restrictions have been placed by the natural person.***

(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 access by anyone except the original data controller, without an emergency override. 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. For natural persons who object, Member States may require the registration and storage of electronic health data in an EHR system used by the healthcare provider who provided the health services and accessible only to them. 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.***

(15) ***Timely and full access of health professionals to the medical records of patients is fundamental for ensuring continuity of care, avoiding duplications and errors, and reducing costs. 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 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 appropriate electronic devices and health professional portals or other health professional access services, to use personal electronic health data*** for the ***exercise of their duties. As it is difficult to exhaustively determine in advance which data from the existing data in the priority categories are medically relevant in a specific episode of care, health professionals should have a wide access. In accessing data relating to their patients, health professionals should comply with the applicable law, codes of conduct, deontological guidelines or other provisions***

governing ethical conduct with respect to sharing or accessing information, particularly in life-threatening or extreme situations. to limit the use of their access to what is relevant in that specific episode of care. In accordance with Regulation (EU) 2016/679, healthcare providers should follow the data minimisation principle when accessing personal health ***data, limiting the data accessed to data that are strictly necessary and justified for a given service. Providing health professionals access*** services ***is a task in the public interest assigned by this Regulation 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 ***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***. 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.

(15b) 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, at national or regional level, or by healthcare providers. 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), point (g) of Regulation (EU) 2016/679. This Regulation provides the required conditions and safeguards for the processing of electronic health data in the electronic health data access services, such as electronic identification of natural persons accessing such services.

(15c) 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 addition to these proxy services, Member States should also establish easily accessible support services for natural persons with adequately trained staff dedicated to assisting them with exercising their rights. 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 (EU) 910/2014[7] 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.

(15d) ***In some Member States, health care is provided by primary care management teams, defined as groups of health 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 health professional of such teams.***

(16b) ***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. The EHDS establishes additional rights for natural persons in primary use, going beyond the access and portability rights***

---

7 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).

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. Member States should ensure that those authorities are provided with the financial and human resources, premises and infrastructure necessary for the effective performance of this additional task. 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 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 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 should be effective, proportionate and dissuasive.

(16c) Member States should strive to adhere to ethical principles, such as the European ethical principles for digital health adopted by the eHealth Network on 26 January 2022 and the principle of health professional-patient confidentiality in the application of this Regulation, recognising their importance, the European ethical principles for digital health provide guidance to practitioners, researchers, innovators, policy-makers and regulators.

(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, ▌ 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. ***Where such priority data categories represent groups of electronic health data, this Regulation should not only apply to the whole groups but also to individual data entries falling under them. For example, because the vaccination status is part of a patient***

summary, the rights and requirements linked to the patient summary should also apply to such specific vaccination status even if it is processed separately from the whole patient summary. When further needs for the exchange of ***additional*** categories of electronic health data are identified for healthcare purposes, ***access to and exchange of these additional categories*** should be ***enabled under this Regulation. The additional categories should be first implemented at Member State level*** and ▌ their ***exchange enabled in the cross-border situations between*** the ***cooperating*** Member States ***on a voluntary basis***. 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.

▌

(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 ***as well as for them to have better control over accessing and sharing their personal electronic health data***. 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 ***format*** should be ***accepted, and the recipient should be able to*** read ***the data*** and ***use it*** 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. ***The format should be designed in a way that facilitates translation of electronic health data represented using it into the Union's official languages, to the extent possible.*** Commission Recommendation (EU) 2019/243[8] provides the foundations for such a common European electronic health record exchange

---

8 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).

format. The ***interoperability of the EHDS should contribute to a high quality of European health data sets. The*** use of European electronic health record exchange format should become more ***widespread*** at EU and national level. ***The Commission should be empowered to extend the European electronic health record exchange format through implementing acts to additional data categories, which are used by willing*** Member States***.*** The European electronic health record exchange format ***may have different profiles for its use at the level of EHR systems*** and ***at the level of the national contact points in MyHealth@EU for cross-border*** data ***exchange***.

(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 ▌ data quality requirements.

(21) ***Telemedicine is becoming an increasingly important tool that can provide patients with access to care and tackle inequities and has the potential to reduce health inequalities and reinforce the free movement of Union citizens across borders. Digital and other technological tools can facilitate the provision of care in remote regions. When digital services accompany the physical provision of a healthcare service, the digital service should be included in the overall care provision.*** Under Article 168 of the Treaty ***on the Functioning of the European Union (TFEU),*** Member States are responsible for their health policy, in particular for ***the organisation and delivery of health*** services ***and medical care,*** including ***regulation of activities such as online pharmacies,*** telemedicine ***and other services*** that they provide and reimburse***, in line with their national legislation***. Different ***healthcare*** policies should ***not***, however, ▌ constitute barriers to the free movement of ***electronic*** health ***data in the context of cross-border*** healthcare***, including telemedicine, such as online pharmacy services***.

(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, 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***. Electronic*** health ***data*** access ***services and telemedicine 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***.

(22a) Member States should establish relevant digital health authorities for the planning and implementation of standards for electronic health data access and transmission and the enforcement of the rights of natural persons and health professionals, as separate organisations or as part of currently existing authorities. The digital health authority staff should not have financial or other interests in industries or economic activities which could affect their impartiality. In addition, Member States should facilitate the participation of national actors in the cooperation at Union level, channelling expertise and advising on 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. In the exercise of their tasks, digital health authorities should cooperate notably with the supervisory authorities established pursuant to Regulation (EU) 2016/679 and supervisory bodies established pursuant to Regulation (EU) 910/2014. They may also cooperate with the European Artificial Intelligence Board under [AI act], the Medical Device Coordination Group under

---

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).

Regulation (EU) 2017/745, the European Data Innovation Board under Regulation (EU) 2022/868 and the competent authorities under the Data Act Regulation (EU) 2023/2854.

(22b) Without prejudice to any other administrative or non-judicial remedy, each natural or legal person should have the right to an effective judicial remedy against a legally binding decision of a digital health authority concerning them. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person should have the right to an effective judicial remedy where a digital health authority does not handle a complaint or does not inform the natural or legal person within three months about the progress or outcome of the complaint. Proceedings against a digital health authority should be brought before the courts of the Member States where the digital health authority is established.

(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 ***intermediation solutions and*** patient portals. 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. ***Member States should ensure that appropriate training initiatives are undertaken. In particular, health professionals should be informed and trained with respect to their rights and obligations under this Regulation.*** 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, ***health professionals,*** manufacturers of EHR systems and wellness applications, as well as ***other*** 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. ***The gradual expansion of the infrastructure and its funding should be considered.*** 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. ***Building on this experience***, the participation of Member States in the digital infrastructure MyHealth@EU ***as established by this Regulation*** should ***be*** mandatory. ***Technical specifications for the MyHealth@EU infrastructure should enable the exchange of priority categories of electronic health data as well as additional categories supported by the European electronic health record exchange format. These specifications should be defined by means of implementing acts and should be based on the cross-border specifications of the European electronic health record exchange format, complemented by further specifications on cybersecurity, technical and semantic interoperability, operations and service management. This Regulation should oblige*** Member States ***to*** join the infrastructure***, comply with the technical specifications for MyHealth@EU,*** and connect healthcare providers ***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. ▌

(25) ▌ MyHealth@EU ***provides*** a common infrastructure for the Member States to ensure connectivity and interoperability in an efficient and secure way ***to support cross-border healthcare, without affecting Member States' responsibilities before and after transmission of personal electronic health data through this infrastructure. Member States are responsible for the organisation of their national contact points and for [the processing of personal data for] the delivery of healthcare before and after transmission of data through this infrastructure. The Commission should monitor the compliance of national contact points with necessary requirements through compliance checks. In case of a serious non-compliance by a national contact point, the Commission should be***

enabled to suspend the impacted services provided by that national contact point. The Commission should act as a processor on behalf of the Member States within this infrastructure and should provide central services for it. To ***ensure*** compliance with data protection rules and to provide a risk management framework for the transmission of personal electronic health data, the ***specific responsibilities of the Member States, as joint controllers, and*** the ***Commission's obligations as processor on their behalf*** should ***be laid down in detail in*** implementing acts***. Each*** Member ***State is solely responsible for data and services in a Member State. 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), point (e), of Regulation (EU) 2016/679. This processing is necessary for the provision of healthcare, as mentioned in Article 9(2), point (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. ***MyHealth@EU should support exchanges of personal electronic health data with contact points of relevant third countries and international organisations to contribute to continuity of healthcare. This is particularly relevant for cross-border mobile populations with neighbouring third countries, for candidate countries, and for the association of overseas countries and territories. Connecting such*** 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 ▌ contact point with the technical specifications, data protection rules and other requirements of MyHealth@EU. ***In addition, given that connection*** to ***MyHealth@EU will entail transfers of personal electronic health data to third countries, such as sharing*** a ***patient summary when the patient seeks care in that*** third country***, relevant transfer instruments pursuant to Chapter V of Regulation (EU) 2016/679 will have to be in place. The Commission*** should be ***empowered to adopt implementing acts to connect such third***

countries and international organisations to MyHealth@EU. ***In preparing these implementing acts, Member States' national security interests should be taken into account.***

(27) In order to ***enable seamless exchange of electronic health data and*** ensure respect for the rights of natural persons and health professionals, EHR systems marketed in the ***Single*** Market of the Union should be able to store and transmit, in a secure way, high quality electronic health data. ***It*** is a key ***objective*** of the EHDS to ensure the secure and free movement of electronic health data across the Union. To that end, a mandatory ***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-assessment***, EHR systems ***will*** prove compliance with ***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'. These two components are focused on data transformation, although they may imply indirect requirements for data registry and data presentation in EHR systems. Technical specifications for the 'European interoperability component for EHR systems' and for the 'European logging component for EHR systems' should be defined by means of implementing acts and should be based on the use of the European electronic health record exchange format. Components should be designed to be reusable and to integrate seamlessly with other components within a larger software system.*** In relation to security ***of those components, these*** requirements should cover elements specific to EHR systems, as more general security properties should be supported by other mechanisms such as ▌Regulation ***[…]… [Cyber-Resilience Act COM/2022/454 final]. To support this process, European digital testing environments should be set up, providing automated means to test whether the harmonised components of an EHR system function in compliance with the requirements laid down in Chapter III of this Regulation. To that end, implementing powers should be conferred on the Commission to determine the common specifications for this environment. The Commission should develop the necessary software for the testing environment and make it available as open source. Member States should be the ones operating the testing environments, as they are closer to manufacturers and better placed to support them. Manufacturers should use these environments to test their products before placing them on the market while continuing***

to bear full responsibility for the compliance of their products. The results of the test should become part of the ***product's technical documentation. Where the EHR system or any part of it complies with*** European ***standards or common specifications, the list of the relevant European standards*** and ***common specifications should also be indicated in*** the ***technical documentation. To support comparability, the Commission should prepare a uniform template for the technical documentation***.

(27a) EHR systems should be accompanied by an information sheet that includes information for its professional users. If the EHR system is not accompanied by such information sheet and by clear and complete instructions for use in accessible formats for persons with disabilities, the manufacturer of the EHR system concerned, its authorised representative and all other relevant economic operators should be required to add to the EHR system that information sheet and those instructions for use.

(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. ***This covers cases such as text processing software used for writing reports that would then become part of narrative electronic health records, general-purpose middleware, or database management software that is used as part of data storage solutions.***

(28a) This Regulation imposes a mandatory conformity self-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.

(28aa) Member States should build upon existing mechanisms to ensure correct application of the regime governing the CE marking and should take appropriate action in the event of improper use of that marking. Where EHR systems are subject to other Union law in respect of aspects not covered by this Regulation, which also requires the affixing of the CE marking, the CE marking should indicate that the systems also fulfil the

requirements of that other law.

(28b) 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. In order to promote the smooth functioning of the single market for electronic health record systems, digital health products and associated 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. Member States should notify the Commission of those national requirements so it has the necessary information to ensure that they do not impede or adversely interact with the harmonised components of EHR systems.

(29) ***Certain components of EHR systems could qualify as medical devices under Regulation (EU) 2017/745[10] or in-vitro diagnostic devices under Regulation (EU) 2017/746 of the European Parliament and of the Council[11].*** 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 and Regulation […] of the European Parliament and of the Council [AI Act COM/2021/206 final], as applicable. ***While such products need to fulfil the requirements under each applicable regulation, Member States should take appropriate measures to ensure that the respective conformity assessment is carried out as a joint or coordinated procedure in order to limit the administrative burden on manufacturers and other economic operators.*** 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 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

---

10 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).

11 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

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. ***Where***

applicable, these common specifications should be based on existing harmonised standards for the harmonised components of EHR systems and be compatible with sectoral legislation. Where common specifications have a particular importance in relation to data protection requirements for EHR systems, they should be subject to consultation with the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) before their adoption, pursuant to Article 42(2) of Regulation (EU) 2018/1725.

(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.

(34aa) Staff of market surveillance authorities should have no direct or indirect economic, financial or personal conflicts of interest that might be considered prejudicial to their independence and, in particular, they should not be in a situation that may, directly or indirectly, affect the impartiality of their professional conduct. Member States should determine and publish the selection procedure for market surveillance authorities. They should ensure that the procedure is transparent and does not allow for conflicts of interest.

(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 ***mandatory***

labelling scheme ***for wellness applications claiming interoperability with EHR systems*** 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 ***should*** set out in implementing acts the details regarding the format and content of such label.

(35a) Member States should remain free to regulate other aspects of the use of wellness applications as referred to in Article 31, 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 mechanisms in place, this Regulation is aimed at establishing a common mechanism to access electronic health data*** for ▌ secondary use ***across the Union. Under this mechanism data holders should make*** the ▌ data ***they hold available on the basis of a data permit or a data request.*** For ▌ the ***purpose*** of ***processing electronic health data for secondary use, one of the legal bases set out in Article 6(1), points (a), (c), (e) or (f), of*** Regulation (EU) 2016/679 ***combined with Article 9(2) of that Regulation*** should be ***required.*** This Regulation provides ***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),

points (g), (h), (i) and (j), of Regulation (EU) 2016/679 ***and Articles 10(2), points (g), (h), (i) and (j), of Regulation (EU) 2018/1725***, in terms of lawful purposes, trusted governance for providing access to health data (through ***the involvement of*** health data access bodies) and processing in a secure environment, as well as 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, except as referred to in Article 33(5).*** At the same time ▌ 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. ***At the same time, the health data access body should assess the information provided by the data applicant, based on which they should be able to issue a data permit for the processing of personal electronic health data pursuant to this Regulation that should fulfil the requirements and conditions set out in Chapter IV of this Regulation.*** More specifically***,*** for processing of electronic health data held by the ***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), points (i) and (j), of the same Regulation*** for ***making available*** the ***personal electronic health*** 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 ***healthcare)*** is unaffected. ▌ This Regulation ***also*** assigns tasks in the public interest ▌ in the sense of Article 6(1), point (e), of Regulation (EU) 2016/679 to the health data access bodies, and meets the requirements of Article 9(2), points ***(g),*** (h), (i), ***and*** (j)***, as applicable,*** of the Regulation (EU) 2016/679. ▌ If the ***health data*** user relies upon a legal basis offered by Article 6(1), point (e), ***or on*** Article 6(1), point (f), of Regulation (EU) 2016/679 ***or Article 5(1), point (a) of Regulation (EU) 2018/1725***, in this case it is this Regulation that ***should provide*** the safeguards ***required under Article 9(2) of Regulation (EU) 2016/679 or Article 10(2) of Regulation (EU) 2018/1725***.

(37b) ***The secondary use of electronic health data can bring great societal benefits. The uptake of real-world data and real-world evidence, including patient-reported outcomes, for evidence-based regulatory and policy purposes as well as for research, health technology assessment and clinical objectives should be encouraged. Real-world data and real-***

world evidence have the potential to complement health data currently made available. 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.

(37c) To balance the need of data users to have exhaustive and representative datasets with the autonomy of natural persons over their personal electronic health data that are considered particularly sensitive, natural persons should have a say in the processing of their personal electronic health data for secondary use under this Regulation, in the form of a right to opt-out from having such their personal electronic health data being made available for secondary use. An easily understandable and accessible user-friendly opt-out mechanism should be provided for in this regard. Moreover, it is imperative to provide natural persons with sufficient and complete information regarding their right to opt-out, including on the benefits and drawbacks when exercising this right. Natural persons should not be required to give any reasons for opting out and should have the possibility of reconsidering their choice at any time. However, for certain purposes with a strong link to the public interest, such as activities for protection against serious cross-border threats to health or scientific research for important reasons of public interest, it is appropriate to provide for a possibility for Member States to establish, with regards to their national context, a mechanism to provide access to data of natural persons that have made use of the right to opt out, to ensure that complete datasets can be made available in those situations. Such mechanisms should comply with the requirements established for secondary use under this Regulation. Scientific research for important reasons of public interest could for example include research addressing unmet medical needs, including for rare diseases, or emerging health threats. Rules on such overrides should respect the essence of the fundamental rights and freedoms and be a necessary and proportionate measure in a democratic society to fulfil public interest in the area of legitimate scientific and societal objectives. Such an override should only be available to health data users that are public sector bodies, including relevant European institutions, bodies, offices, or agencies, entrusted with carrying out tasks in the area of public health or by another entity entrusted with carrying out public tasks in the area of public health, or acting on behalf of or commissioned by a public authority and only under the conditions that the data cannot be obtained by alternative means in a timely and effective

manner. Such health data users should justify that the use of the override is necessary for an individual access application or data request. When such an override is used, the safeguards under Chapter IV will continue to apply, notably the ban against re-identification, including attempts, by data users.

(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. ▌ 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 ***health*** data holders should contribute to this effort in making different categories of electronic health data they are holding available for secondary use ***provided that such effort is always made through effective and secured processes, with due respect for professional duties, such as confidentiality duties***. ***In justified cases, such as in the case of a complex and burdensome request, the health data access body may extend the time period for health data holders to make the requested electronic health data available to the health data access body.***

(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 ***health*** data users, while remaining limited to data related to health or known to influence health. ***They*** can also include relevant data from the health system (electronic health records, claims data, ***dispensation data, data from*** disease registries, genomic data etc.), as well as data with an impact on health (for example consumption of different substances, ***socio-economic*** status, behaviour, including environmental factors (for example, pollution, radiation, use of certain chemical substances). They ▌ include ***some categories of*** data ***that were initially collected for*** other ***purposes such as research, statistics, patient safety, regulatory activities or policy making (e.g. 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.). Data can also include automatically generated data from medical***

devices, and person-generated data, such ***as wellness applications. Data on clinical trials and clinical investigations*** should be ***included when the clinical trial or clinical investigation has ended, without affecting any voluntary data sharing by the sponsors of ongoing trials and investigations***. Data ***for*** secondary use ▌ should ▌ be ***made available preferably*** in ***a structured electronic format that facilitates their processing by computer systems. This should encompass formats such as records in a relational database, XML documents or CSV files, but also include free text, audios, videos and images provided as computer-readable files.***

(39aa) The health 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. Health data users should be encouraged to report critical errors in datasets to health data access bodies. 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.

(39b) 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, the availability in the EHDS of electronic health data described in Chapter IV should be enabled in a way that the data are as accessible, high-quality, ready and suitable for the purpose of creating scientific, innovative and societal value and quality as possible. Work on the EHDS implementation and further dataset improvements should be conducted prioritising datasets that are best fit for creating such value and quality.

(40) ▌ 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 ***areas*** where the collection of such data is fragmented of difficult, such as rare diseases, cancer etc. Such data, collected and processed by ***health*** data holders with the support of Union or national public funding, should be made available ▌ 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. ***The health*** data ***holders in the context of secondary use of electronic health data should therefore be entities that are health or care providers or carry out research with regards to the healthcare or care sectors, or develop products or services intended for the healthcare or care sectors. Such entities can be public, non for profit or private. In line with this definition, 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 should be considered*** health data ***holders. Legal persons developing wellness applications should also be*** health ***data holders. Union institutions, bodies, offices or agencies that process the categories of health and healthcare data mentioned above, as well as mortality registries should also be considered health data holders. In order to avoid a disproportionate burden, natural persons and micro-enterprises should be, as a general rule, exempted from the obligations as health data holders. Member States should, however, be able to extend the obligations of data holders to natural persons and micro-enterprises in their 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.*** Such ***health*** data ***intermediation entities*** should be ***legal persons able to process*** and ***make available for*** secondary use ***electronic*** health data ▌ provided ***by data holders. Such health*** data ***intermediation entities perform*** different ***tasks than data intermediation services referred to*** in ***Article 10 of*** Regulation ***(EU) 2022/868. 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***.

(40c) Electronic health data protected by intellectual property rights or trade secrets, including data on clinical trials, investigations and studies, can be very useful for secondary use and can foster innovation within the Union for the benefit of Union patients. In order to incentivise continuous Union leadership in this domain, the sharing of the clinical trials and clinical investigations data through the EHDS for secondary use. They should be made available to the extent possible, while taking all necessary measures to protect such rights. This Regulation should not be used to reduce or circumvent such protection and should be consistent with the relevant transparency provisions laid down in Union law, such as those laid down for clinical trial and clinical investigation data. 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.

(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. ***In particular, the secondary use of health data for research and development purposes should contribute to a benefit to society in the form of new medicines, medical devices, health care products and services at affordable and fair prices for Union citizens, as well as to enhancing access to and the availability of such products and services in all Member States.*** 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 the supervisor of these activities. The provision of the data should also support activities related to scientific research***. The notion of scientific research purposes should be interpreted in a broad manner*** including ***for example technological*** development and ***demonstration, fundamental research, applied research and privately funded research. Examples are*** innovation activities ***including*** training of ***artificial intelligence*** algorithms that could ***be used in healthcare*** or care of natural persons***, as well as the evaluation and further development of existing algorithms and product for such purposes. The EHDS should also contribute to fundamental research; while the benefits to end-users and patients may be less direct in fundamental research, such research is crucial for societal benefits in the longer term***. 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 ***(EU) 2023/2854***. 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. ▌

(41aa) Any attempt to use the data for any measures detrimental to the natural person, such as 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, to automate individual decision-making, to re-identify natural persons 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. It should be also prohibited to provide access to, or otherwise make available, the electronic health data to third parties not mentioned in the data permit. The identity of authorised persons, in particular the identity of the principal investigator, who will have the right to access the electronic health data in the secure processing environment should be indicated in the data permit. The principal investigators are the main persons responsible for requesting access to the electronic health data and for processing the

requested data within the secure processing environment on behalf of the health data user.

(41a) This Regulation should 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 should not be among the secondary use purposes covered under this Regulation. Therefore, courts and other entities of the justice system should not be considered data users in the secondary use of health data under this Regulation. In addition, courts and other entities of the justice system should not be covered under the definition of health data holders and should not therefore be addressees of obligations on health data holders under this Regulation. 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.

(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 ▌. Health data access bodies should not be influenced in their decisions on access to electronic data for secondary use ***and avoid any conflict of interest. Members of the governance and decision-making bodies and staff of each health data access body should therefore refrain from any action that is incompatible with their duties and should not engage in any incompatible occupation.*** 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***, technical*** 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(2)*** of Regulation ***(EU) 2022/868***, 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 ***(EU) 2022/868*** or in designating existing or new sectoral bodies responsible for such tasks in relation to access to health data. ***The members and staff of health data access bodies should have the necessary qualifications, experience and skills.***

(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***.*** The health data access bodies should also cooperate with stakeholders, including patient organisations. ***The health data access bodies should support health data holders that are small enterprises in accordance with Commission Recommendation 2003/361/EC, in particular medical practitioners and pharmacies***. 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 ***remain the only authorities competent for*** enforcing these rules. ▌ The health data access bodies should inform the data protection authorities of any ***penalties issued and any potential*** issues related to the data processing for secondary use ***and exchange any relevant information at their disposal to ensure enforcement of the relevant rules.*** 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, ▌ and promote the development of common standards. They should apply tested ***state-of-the-art*** 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. ***In that regard, health data access bodies should cooperate across borders to develop and exchange best practices and techniques.*** This includes rules for ***anonymisation*** of microdata sets. ***When relevant, the Commission should set out the procedures and requirements, and provide technical tools, for a unified procedure for anonymising and pseudonymising the electronic health data.***

(44) ▌Health data access bodies ***should ensure transparency of secondary use by providing public information about the permits granted and their justifications, the measures taken*** to ***protect*** the ***rights of*** natural persons***, how natural persons can exercise their rights in relation to secondary use, and the outcomes of secondary use, such as links to scientific publications. Where appropriate, this information on the outcomes of secondary use should also include a lay summary to be provided by the health data user. These transparency obligations complement the obligations laid down in Article 14 of Regulation (EU) 2016/679.*** The exceptions provided for in Article 14(5) of Regulation (EU) 2016/679 ***could*** apply***.*** ▌Where ***such exceptions are applied, these transparency obligations contribute to ensuring*** fair and transparent processing ***as referred to in*** Article 14(2) of Regulation (EU) 2016/679, e.g. information on the purpose and the data categories processed***, enabling natural persons to understand whether their data are being made available for secondary use pursuant to data permits.***

(44a) ***Natural persons*** should be ***informed through*** the ***health*** data ***holders about significant findings related to their health discovered by*** health data ***users. Natural persons*** should ***have the right to request not to be informed of such findings. Member States could lay down conditions for this. Member States*** should be ***enabled, in accordance with Article 23(1), point (i), of Regulation (EU) 2016/679,*** to ***restrict the scope of the obligation to inform the natural persons whenever necessary for their protection based on patient safety and ethics, by delaying the communication of their information until a health professional can communicate and explain to the natural persons information that potentially can have an impact on them***.

(44b) In order to promote transparency ***health data access bodies should also publish biennial activity reports providing an overview of*** their ***activities. Where a Member State has designated more than one*** health data access body***, the coordinating body*** should ***prepare and*** publish ***a common*** report***. Activity reports should follow a structure agreed in the EHDS Board and provide*** an overview of ▌activities***, including information on decisions***

on application, audits, and engagement with relevant stakeholders. Such stakeholders can include representatives of natural persons, patient organisations, health professionals, researchers, and ethical committees.

▌(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 a health data holder is a public sector body, the part of the fees linked to its costs should not cover the costs of the initial collection of the data.*** Where ethical approval is necessary for providing a data permit, its evaluation should be based on its own merits. ▌

(47) Health data access bodies ▌ should be allowed to charge fees***, considering*** the ***horizontal rules provided by*** Regulation ***(EU) 2022/868,*** 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. Health data access bodies should be able to cover the costs of their operation with fees established in a proportionate, justified and transparent manner. This may result in higher fees for some users, if servicing their data access applications and data requests requires more work. Health*** data holders should be allowed to also ***ask for*** fees for making data available ***reflecting their costs. The health data access bodies should decide on the amount of*** such fees ***which would also include*** the ***fees asked by health data holder. Such fees should be charged by the health data access body to the health data user in a single invoice. The health data access body should then transfer the relevant part to the health data holder***. In order to ensure a harmonised approach concerning fee policies and structure, the Commission ***should*** adopt implementing acts. Provisions in Article 10 of ▌Regulation ***(EU) 2023/2854 should*** apply for fees charged under this Regulation.

(48) In order to strengthen the enforcement of the rules on the secondary use of electronic health data, appropriate measures ***should be envisaged*** that can lead to ***administrative fines or enforcement measures by health data access bodies*** or temporary or definitive exclusions from the EHDS framework of the ***health*** data users or ***health*** data holders that do not comply with their obligations. The health data access body should be empowered to

verify compliance and give ***health*** data users and holders the opportunity to reply to any findings and to remedy any infringement. ***When deciding on the amount of the administrative fine or enforcement measure for each individual case, health data access bodies should take into account the margins for costs and criteria set out in this Regulation***, ***ensuring that measures or fines are proportionate***.

(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, ***non-personal*** electronic health data ▌ should be made available ***in all cases where this is sufficient***. 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 ***and*** the ***health*** data ***access body should assess the validity of that justification***. The personal electronic health data should only be made available in pseudonymised format***. 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. When providing access to an anonymised or pseudonymised dataset, a health data access body should use state-of-the-art anonymisation or pseudonymisation technology and standards, ensuring to the maximum extent possible that natural persons cannot be re-identified by health data users. Such technologies and standards for data anonymisation should be further developed. Health*** data users should not attempt to re-identify natural persons from the dataset provided under this Regulation, subject to administrative ***fines and the enforcement measures laid down in this Regulation*** or possible criminal penalties, where the national laws foresee this. ▌ Moreover, ***a health data*** applicant ***should be able to*** request ***an*** answer to a ***health*** data request ▌ in ***an anonymised*** statistical ***format***. In this case, the ***health*** data ***user*** would ***only*** process ***non-personal*** data***,*** and the health data access body would remain sole controller for ***any personal*** data necessary to provide the answer to the ***health*** 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 ***data***

access application and decide if the applicant may receive a data permit for secondary use of data, also ensuring coherence between different health data access bodies. ***The*** information ***provided as part of the data access application should follow the requirements established*** under ***this*** Regulation ***in order*** to ***enable its thorough assessment, as*** a ***data permit should only be issued if all the necessary conditions set out in this Regulation are met. In addition,*** where ***relevant, it should include a declaration by the health*** data ***applicant that the intended use of the data requested does not pose a risk of stigmatisation or causing harm to the dignity of individuals or the groups to which the dataset requested relates.*** An ethical assessment may be requested based on national law. ***Where this is the case, it should be possible for existing ethic bodies to carry out such assessments for the HDAB. Existing ethic bodies of Member States should make their expertise available to the health data access body for this purpose. Alternatively, Member States may decide to make ethic bodies or expertise to be an integral part of the health data access body***. The health data access ***body*** and, where relevant ***health*** data holders, should assist ***health*** data users in the selection of the suitable datasets or data sources for the intended purpose of secondary use. Where the applicant needs ***data in an*** anonymised statistical ***format***, it should submit a data request application, requiring the health data access body to provide directly the result. ***A refusal of a data permit by the health data body should not preclude the applicant from submitting a new data access application.*** In order to ensure a harmonised approach between health data access bodies ***and to limit an unnecessary administrative burden for the health data applicants***, the Commission should support the harmonisation of ***health*** data ***access applications***, as well as ***health*** data ***requests, including by establishing the relevant templates***.

(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 ***health*** 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 ***health*** data permit and may be subject to an ***additional*** fee. However, in all the cases, the data permit should reflect ***these additional*** uses of the dataset. Preferably, the ***health*** 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 ***with a legal mandate in the field of public health***, especially the Commission, need access to health data for a longer period and on a recurring basis. This ▌ may be the case not only ***for*** specific circumstances ***stipulated by Union or national law*** 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. ***Such health data users should be able to benefit from an accelerated procedure for having data be made available normally in less than 2 months, with a possibility to prolong the timeline by 1 month in more complex cases.***

(53) ***Member States should be enabled*** to ***designate trusted*** data ***holders for which the*** data ***permit procedure would be performed in a simplified manner,*** in order to ***alleviate*** the administrative burden for heath data access bodies of managing ***requests for*** the data ***processed by them. Trusted*** data ***holders*** should be ***enabled*** to ***assess the*** data ***access applications submitted under this simplified procedure, considering their expertise in dealing with the type of health*** data ***they are processing,*** and ▌ issue a ***recommendation regarding a*** data permit ▌ . ***The health data access body should remain responsible for issuing the final data permit and*** should ***not be bound by the recommendation provided by*** the ***trusted*** data holder**.** Health data ***intermediation entities should not be designated as trusted health data holders***.

(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, ***trusted*** 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. ▌ 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.

(54a) Regulation (EU) 2022/868 sets out the general rules for the management of data altruism. Given that the health sector manages sensitive data, additional criteria should be established through the rulebook foreseen in Regulation (EU) 2022/868. 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 (EU) 2022/868 to supervise the activity of data altruism organisations in the health or care sector.

(55) For the processing of electronic health data in the scope of a granted permit ***or a data request, the health data holders including trusted ones***, the health data access bodies and the ***health*** data users should ***each, in turn,*** be ***deemed a controller for a specific part of the process and according to their respective roles therein. The health data holder should be deemed controller for the disclosure of the requested personal electronic health data*** to ***the*** health data access ***body, while the health*** data ***access body*** should ***in turn be deemed controller for the processing of the personal electronic health data when preparing the data and making them available to the health data user. The health data user should be deemed controller for the processing of personal electronic health data in pseudonymised form in the secure processing environment pursuant to its data permit. The*** health data access ***body should be deemed a processor on behalf of the health*** data ***user for processing carried out by the health data user pursuant to a data permit in the secure processing environment as well as for the processing to generate an answer to a data request. Similarly, the trusted health data holder should be deemed controller for its processing of personal electronic health data related to the provision of electronic health data to the health data user pursuant to a data permit or a data request. The trusted health data holder should be deemed to act as a processor for the health data user when providing data through a secure processing environment.***

(55b) 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"***,*** ***"privacy by default",*** and "bring questions to data instead of moving data" should be respected whenever possible. ***Member States should designate national contact points for secondary use of electronic health data, as organisational and technical gateways for*** health data access bodies, ***and connect these contact points to HealthData@EU. The Union data access service should also connect to HealthData@EU. In addition, authorised participants in HealthData@EU could be*** research infrastructures established as an European Research Infrastructure Consortium ('ERIC') under Council Regulation (EC) No 723/2009[12]***, as a European digital infrastructure consortium ('EDIC') under Decision (EU) 2022/2481***[13] 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). ***National contact points of third countries and systems established at an international level could also become authorised participants in*** HealthData@EU***, provided that they are compliant with the requirements in this Regulation***. ***The Commission digital strategy promotes the linking of the various common European data spaces.*** HealthData@EU should ***therefore*** 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. ***Such interoperability between the health sector and the sectors such as the environmental, social, agricultural sectors may be relevant for additional insights on health determinants.*** 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,

---

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 ***Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (OJ L 323, 19.12.2022, p. 4).***

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. ▌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[14].

(55a) In addition, given that connection to HealthData@EU could entail transfers of personal data related to the applicant or health data user to third countries, relevant transfer instruments pursuant to Chapter V of Regulation (EU) 2016/679 will have to ***be in place for such sharing***.

(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 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 ***can*** obtain authorisation from multiple health data access bodies in different Member States ***or authorised participants***.

(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. ***The health data holder should, at least every year, check that its dataset description in the national datasets catalogue is accurate and up to date.*** Therefore, an EU datasets catalogue should be established to facilitate the discoverability of datasets

---

14 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).

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. ***The use of datasets could be prioritised by their users according to their usefulness and quality.***

(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 ***(EU) 2022/868. Interoperability should be ensured between the EU datasets catalogue, the*** national data catalogues ***and the*** 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, ***cardiovascular and metabolic diseases, risk factor assessment,*** and statistics and ***should*** be taken into account when defining new standards ***and disease-specific harmonised templates for structured data elements***. 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 ▌ coding and registration of electronic health data ***to enable its supply for secondary use in a consistent way. 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. ***Existing health data infrastructures and registries can provide models useful for defining and implementing data standards and interoperability and should be leveraged to enable continuity and to build on existing expertise.***

(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. ***They should take into account the specific conditions of different categories of stakeholders, such as that are civil society, researchers, researchers, medical societies and SMEs.***

(62a) Improving digital health literacy for both natural persons and health professionals is key in order to achieve trust, safety and appropriate use of health data and thus to achieve successful implementation of this Regulation. Health professionals are faced with a profound change in the context of digitalisation and will be offered further digital tools as part of the implementation of the EHDS. Health professionals need to develop their digital health literacy and digital skills. Member States should enable health professionals to take digital literacy courses to be able to prepare to work with EHR systems. Such courses should enable health professionals and IT operators to receive

sufficient training in working with new digital infrastructures to ensure cybersecurity and ethical management of health data. The trainings should be developed and reviewed, and kept up to date, on a regular basis in consultation and cooperation with relevant experts. Improving digital health literacy is fundamental in order to empower natural persons to have true control over their health data and actively manage their health and care, and understand the implications of the management of such data for both primary and secondary use. Different demographic groups have varying degrees of digital literacy, which can affect natural persons' ability to exercise their rights to control their electronic health data. Member States, including regional and local authorities, should therefore support digital health literacy and public awareness, while ensuring that the implementation of this Regulation contributes to reducing inequalities and does not discriminate against people lacking digital skills. Particular attention should be given to persons with disabilities and vulnerable groups including migrants and the elderly. Member States should create targeted national digital literacy programmes, including programmes to maximise social inclusion and to ensure all natural persons can effectively exercise their rights under this Regulation. Member States should also provide patient-centric guidance to natural persons in relation to the use of electronic health records and primary use of their personal electronic health data. Guidance should be tailored to the patient's level of digital health literacy, with specific attention to be given to the needs of vulnerable groups.

(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. ***Union funds should be distributed transparently among the Member States, taking into account different levels of health system digitalisation. Making data available for secondary use requires additional resources for healthcare systems, in particular public systems. That additional burden should be addressed and minimised during the implementation phase of the EHDS.***

(63a) The implementation of the EHDS requires appropriate investments in capacity building and training and a well-funded commitment to public consultation and engagement both

at Member State and Union level. The economic costs of implementing this Regulation should be borne at both Member State and Union level, and a fair sharing of that burden between national and Union funds should be found.

(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 clinical investigations***, 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 ***(EU) 2022/868***. These types of health data would thus fall within the empowerment set out in Article 5(13) of Regulation ***(EU) 2022/868*** 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 ***(EU)***

2022/868.

(64b) ***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 solely 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.***

(64d) ***Access to electronic health data for entities from third countries or international organisations should take place only on the basis of the reciprocity principle. Making available of health data to a third country can take place only where the Commission has established by means of an implementing act that the third country concerned allows for the use of health data by Union entities under the same conditions and with the same safeguards as within the Union. The Commission should monitor the situation in these third countries and international organisation, list and provide for a periodic review thereof. Where the Commission finds that a third country no longer ensures access on the same terms, it should revoke the corresponding implementing act.***

(65) In order to promote the consistent application of this Regulation, ***including cross-border interoperability of health data,*** a European Health Data Space Board (EHDS Board) should be set up. The Commission should participate in its activities and ***co-chair*** it. ***The EHDS Board*** should ***be able to issue written contributions related*** 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***, and the funding for these activities. This may also include sharing information on risks and incidents in the secure processing environments. This kind of information sharing does not affect obligations under other legal acts, such as data breach notifications under Regulation (EU) 2016/679. More generally, the activities of the EHDS Board are without prejudice to the powers of the supervisory authorities pursuant to Regulation (EU) 2016/679.*** Given that, at national level, digital health authorities dealing with the primary use of electronic health data may be different ***from*** 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]. ***The EHDS Board should operate independently, in the public interest and in line with its Code of Conduct.***

(65a) Where the issues of relevance according to the EHDS board are discussed, the board should be able to invite observers, for instance the European Data Protection Supervisor, representatives of EU institutions, including the European Parliament and other stakeholders.

(65b) A stakeholders forum should be set up to advise the EHDS Board in the fulfilment of its tasks by providing stakeholder input on matters pertaining to this Regulation. The stakeholders forum should be composed of representatives of patients, consumers, health professionals, industry, scientific researchers and academia. It should have a balanced composition and represent the views of different relevant stakeholders. Both commercial and non-commercial interests should be represented.

(66) In order to ***ensure proper day-to-day management of*** the cross-border infrastructures for primary and secondary use of electronic health data, it is necessary to create ***steering groups consisting of Member State representatives. These groups should take operational decisions on the technical day-to-day management of the infrastructures and their technical development, including on technical changes to the infrastructures,***

improving functionalities or services, or ensuring interoperability with other infrastructures, digital systems or data spaces. Their activities do not extend to contributing to the development of implementing acts affecting these infrastructures***. These groups may also invite representatives of other authorised participants as observers to their meetings. These groups should consult relevant experts when carrying out their tasks***.

(66a) Without prejudice to any other administrative, judicial or non-judicial remedy, any natural or legal person should have the right to lodge a complaint with a digital health authority or with a health data access body, if the natural or legal person considers that his or her rights or interests under this Regulation have been affected. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The digital health authority or health data access body should inform the natural or legal person of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another digital health authority or health data access body, intermediate information should be given to the natural or legal person. In order to facilitate the submission of complaints, each digital health authority and health data access body should take measures such as providing a complaint submission form which can also be completed electronically, without excluding the possibility of using other means of communication. Where the complaint concerns the rights of natural persons related to the protection of their personal data, the digital health authority or health data access body should transmit the complaint to the supervisory authorities under Regulation (EU) 2016/679. Digital health authorities or health data access bodies shall cooperate to handle and resolve complaints, including by exchanging all relevant information by electronic means, without undue delay.

(66b) Where a natural person considers that his or her rights under this Regulation have been infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data, to lodge a complaint on his or her behalf.

(66f) The digital health authority, health data access body, health data holder or health data user should compensate any damage which a person could suffer as a result of actions

that infringe this Regulation. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or national law. Natural persons should receive full and effective compensation for the damage they have suffered.

(66h) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of, appropriate measures imposed by the health data access body pursuant to this Regulation. The imposition of penalties, including administrative fines, should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process.

(66j) It is appropriate to lay down provisions enabling health data access bodies to apply administrative fines for certain infringements of this Regulation whereby certain infringements are to be regarded as serious infringements, such as the re-identification of natural persons, downloading personal health data outside of the secure processing environment and processing of data for prohibited uses or outside a data permit. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent health data access body in each individual case, taking into account all the relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the health data access bodies or of other penalties under this Regulation.

(66k) The legal system of Denmark does not provide for administrative fines as set out in this Regulation. It should be possible to apply the rules on administrative fines in a manner

such that in Denmark the fine is imposed by competent national courts as a criminal penalty, provided that such an application of the rules in Denmark has an equivalent effect to administrative fines imposed by health data access bodies. Therefore the competent national court should take into account the recommendation by the health data access body initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(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[15]. 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.

15 OJ L 123, 12.5.2016, p. 1.

(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[16].

(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. ***When deciding on the amount of the penalty for each individual case*** Member States should take into account the margins and criteria set out in this Regulation. ***Re-identification of natural persons should be considered a serious breach of this Regulation.***

(70a) Implementing the EHDS will require significant development work across Member States and central services. To track the progress, the Commission should, until the full application of this Regulation, report annually on the progress made, taking into account information provided by the Member States. These reports may include recommendations for remedial measures, as well as an assessment of the progress made.

(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 ***8*** years after its entry into force, ▌ and an overall evaluation ***10*** 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[17] 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

---

16 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).

17 European Commission, European Interoperability Framework.

of eHealth Network, but also strong potential for EU work in this area, as shown by the 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.

(73a) This Regulation complements the essential requirements laid down in Regulation 2024/XXX [CRA] for electronic health record systems falling under the scope of this Regulation which are products with digital elements within the meaning of the [CRA] and which should therefore also comply with the essential requirements set out in the [CRA]. Their manufacturers should demonstrate conformity as required by this Regulation. To facilitate compliance, manufacturers may draw up a single technical documentation containing the elements required by both legal acts. It should be possible to demonstrate compliance of EHR systems with essential requirements laid down in CRA Regulation through the assessment framework under this Regulation, except for the use of the testing environment under this Regulation.

(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 ***Joint*** opinion ***n. 03/2022 on 12 July 2022***.

(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 ***24*** months after entry into force***. In order to support the successful implementation of the EHDS and the creation of effective conditions for European health data cooperation, a staged approach to its implementation should be taken,***

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, ▌ standards ▌ , infrastructures and a governance framework ***with a view to facilitating access to electronic health data*** for the ***purposes of*** primary and secondary use of ***these*** data.

2. This Regulation:

(a) ***specifies and complements*** the rights ***laid down in the Regulation (EU) 2016/679*** of natural persons in relation to the ***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*** systems***' and the*** '***European logging component for*** EHR systems' ***as defined in Article 2(2), points (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 ***for primary and*** secondary use of electronic health data;

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

(e) establishes a ▌ 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.

4. This Regulation shall be without prejudice to 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, ***(EU) 536/2014, No 223/2009, (EU) 2022/868*** and […] [Data Act COM/2022/68 final] ***and Directives 2002/58/EC and (EU) 2016/943***.

4a. References to the provisions of Regulation (EU) 2016/679 shall be understood also as references to the corresponding provisions of Regulation (EU) 2018/1725, where relevant.

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 ***be without prejudice to*** Union or national law ***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.

6b. 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 does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Article 2

Definitions

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

(a) the definitions ***of 'personal data', 'processing', 'pseudonymisation', 'controller', 'processor', 'third party', 'consent', 'genetic data', 'data concerning health', 'international organisation' pursuant to Article 4, points (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, ***points*** (a), (c), (d), (f), (g), (i) and (k), ▌ 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***, points*** (1), ***(13), (16***), (***17***) and (***20***), of ***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', ▌ 'recall' and 'withdrawal', pursuant to Article 2***, points*** (1), (2), (3), (4), (7), (8), (9), (10), (13), (16), ▌ (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***, points*** (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***, points*** (1), (2) and (3), of the Regulation (EU) No 910/2014***;***

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

(h) the definition of 'public health' pursuant to Article 3, point (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 data concerning health and genetic data as defined in ***Article 4, points (13) and (15), of*** Regulation (EU) 2016/679, ▌ processed in an electronic form;

(b) ‘non-personal electronic health data’ means ***electronic health*** data ***other than personal electronic*** health ▌ data***, encompassing both*** data ***that has been anonymised so that it no longer relates to an identified or identifiable natural person and data that has never related to a data subject;***

(c) ‘electronic health data’ means personal or non-personal electronic health data;

(d) ‘primary use of electronic health data’ means the processing of ▌ electronic health data for the provision of ***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 ▌ , 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 of this Regulation***, other than*** the ***initial purposes for which they were*** collected ***or produced;***

(f) ‘interoperability’ means the ability of organisations as well as software applications or devices from the same manufacturer or different manufacturers to interact ▌ , 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;

▌

(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;

▌

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

(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 ***by healthcare providers in providing patient care*** or ***by patient to access to their*** health ***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 functions or procedures and which can operate independently or in conjunction with other components;

(nc) ‘European interoperability component for EHR systems’ (or ‘the interoperability component’) means a software component of the EHR system which provides and receives 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;

(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 a hazard causing the harm to health, safety or 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 ***or serious prejudice to a natural persons rights***;

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

(xa) 'care' means a professional service for 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, including preventive and supportive measures, to carry out essential activities of daily living in order to support their personal autonomy;

(y) '***health*** data holder' means any natural or legal person, ***public authority, agency*** or ***other*** body in the ***healthcare*** or ***the*** care ***sectors; including reimbursement services when needed*** as well as ***any natural or 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 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 ***non-personal electronic health*** data***, through control of the technical design of a product and related services.***

(z) ***'health*** data user' means a natural or legal person***, including Union institutions, bodies or agencies, which*** has ***been granted*** lawful access to ▌electronic health data for secondary use ***pursuant to a data permit, data request or an access approval by an authorized participant in Health Data @ EU***;

(aa) 'data permit' means an administrative decision issued to a ***health*** data user by a health data access body ▌to process ***certain*** electronic health data specified in the data permit for ***specific*** secondary use purposes ▌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 ***the elements*** of electronic health data are 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***;***

(aea) 'wellness application' means any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data specifically for providing information on the health of individual persons, or the

delivery of care for other purposes than the provision of healthcare.

CHAPTER II

Primary use of electronic health data

Section 1

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

Article 3

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

▌

12. The Commission shall, by means of implementing acts, determine the requirements ***for*** the technical implementation of the rights set out in this ***Section***.

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

▌

Article 5

Priority categories of personal electronic health data for primary use

1. ***For the purposes of this Chapter,*** where data is processed in electronic format, ***the priority categories*** of personal electronic health data ***shall be*** the following ▌:

(a) patient summaries;

(b) electronic prescriptions;

(c) electronic dispensations;

(d) medical ***imaging studies and related imaging*** reports;

(e) ***medical test results, including*** laboratory ***and other diagnostic*** results ***and related reports***;

(f) discharge reports.

The main characteristics of the ***priority*** categories of ***personal*** electronic health data ▌shall

be as set out in Annex I.

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 ▌ Annex I by adding, modifying or removing the main characteristics of the priority categories of ***personal*** electronic health data ***as referred to in paragraph 1. The amendments*** shall satisfy the following ***cumulative*** criteria:

(a) the ***characteristic*** is relevant for ***healthcare*** provided to natural persons;

(b) ***the characteristic as modified*** is used in ***the majority of*** Member States ***according to the most recent information***;

(c) 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) ***harmonised*** 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;

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

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

1a. The Commission shall provide regular updates of the European electronic health record exchange format through implementing acts to integrate relevant revisions of the healthcare coding systems and nomenclatures.

-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(1), subparagraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

3. Member States shall ensure that the priority categories of personal electronic health data referred to in Article 5 are issued in the ***European electronic health record exchange*** format referred to in paragraph 1***. Where*** such data ***are transmitted by automatic means for primary use the receiving provider*** shall ***accept the format of*** the data ***and be able to read it***.

Article 7

Registration of personal electronic health data

1. Member States shall ensure that, where ***electronic health*** data is processed ***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).

When health data are registered or updated, electronic health records shall ***identify the health professional, time and health care provider that carried out the registration or the update. Member States may provide for other aspects of data registration to be recorded***.

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 or their representatives as referred to in Article 8g(2) shall have the right to download 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 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 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 8h. Such access services shall be free of charge for the natural persons and their representatives.***

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

(a) ***natural persons to authorise other natural persons of their choice to access their personal electronic health data, or part thereof, on their behalf for a specified or indeterminate period and if needed, for a specific purpose only, and to manage those authorisations; and***

(b) ***legal representatives of patients to access electronic health data of the natural persons whose affairs they administer, in accordance with national law.***

Member States shall establish rules regarding such authorisations, actions of guardians and representatives.

2aa. ***The proxy services shall provide authorisations in a transparent and easily understandable way, free of charge, electronically or on paper. Natural persons and those acting on their behalf shall be informed about their authorisation rights, how to exercise them, and what they can expect from the authorisation process.***

The proxy services shall provide an easy complaint mechanism for natural persons.

2a. ***The proxy services shall be interoperable among Member States. 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).***

2b. The electronic health data access services as well as the proxy services shall be easily accessible for persons with disabilities, vulnerable groups or persons with low digital literacy.

Article 8b

Right of natural persons to insert information in their own EHR

1. Natural persons or their representatives as referred to in Article 8g(2) shall 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

3. Electronic health data services referred to in Article 8g shall provide a possibility for natural persons to easily request rectification of their personal data online as a way to exercise their right to rectification under Article 16 of Regulation (EU) 2016/679. Where appropriate, the data controller shall validate the accuracy of the information provided in the request with a relevant health professional.

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 to another healthcare provider of their choice immediately, free of charge and without hindrance from the health care provider or from the manufacturers of the systems used by that healthcare provider.

2. Natural persons shall have the right that, where the healthcare providers are located in

different Member States the electronic health data shall be transmitted 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. Natural persons shall have the right to request a healthcare provider to transmit a part of their electronic health data to a clearly identified recipient in the social security or reimbursement services sector, immediately, free of charge and without hindrance from the healthcare provider or from the manufacturers of the systems used by that healthcare provider. Such a transmission shall be one-way only.

4. Where natural persons have received an electronic copy of their priority categories of personal electronic health data as referred to in Article 3(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.

Article 8e

Right to restrict access

Natural persons shall have the right to restrict access of health professionals and healthcare providers to all or parts of their personal electronic health data referred to in Article 8a.

When exercising this right, natural persons shall be made aware that restricting access may impact the provision of healthcare provided to them.

The fact that a restriction has been made by the natural person shall not be visible to healthcare providers.

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

Article 8f

Right to obtain information on accessing data

Natural persons shall have the right to obtain information, including through automatic notifications, on any access to their personal electronic health data through the health

professional access service made in the context of healthcare, including access provided in accordance with Article 4(4).

The information shall be provided without delay and free of charge through electronic health data access services. The information shall be available for at least three years after each data access. 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.

Member States may provide for restrictions to this right in exceptional circumstances, where there are factual indications that disclosure would endanger the vital interests or rights of the health professional or the care of the natural person.

Article 8h

Right of natural person to opt out in primary use

1. Member States laws may provide that natural persons have the right to opt out from 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 opt out in primary use.

Article 7a

Access by health professionals to personal electronic health data

1. Where they process data in an electronic format, health professionals shall have access to the relevant and necessary 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 shall also establish rules providing for the categories of personal electronic health data accessible by different categories of health professionals or different healthcare tasks.

Such rules shall take into account the possibility of restrictions imposed in according to Article 8e.

2a. ***In the case of treatment in a Member State other than the Member State of affiliation, the rules referred to in paragraphs 1a and 2 of the Member States of treatment shall apply.***

3. ***Where access to electronic health data has been restricted by the natural person pursuant to Article 8e(1), the healthcare provider or health professionals shall not be informed of the restricted content of the electronic health data.***

Where access is necessary in order to protect the vital interests of the data subject 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 data subject.

Member States' law may add 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, including for cross-border care, 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.

The electronic health data in the electronic health records shall be presented in a user-friendly manner to allow for easy use by health professionals.

Article 9

Identification management

1. Where a natural person uses ▌ personal health data access services referred to in Article ***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. 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 ***examination*** procedure referred to in Article 68(2).

3. The Commission***, in cooperation with Member States,*** 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 ***Member States' competent*** authorities and the Commission shall implement the cross-border identification and authentication mechanism at ▌ Member States' ***and Union*** level,

respectively.

Article 9a

Compensation for making personal electronic health data available

1. The receiving provider shall not be required to compensate the healthcare provider for making electronic health data available. A health care provider or a third party shall not directly or indirectly charge data subjects a fee, compensation or costs for sharing data or accessing it.

[Section 3]

Article 10

Digital health authority

1. Each Member State shall designate ***one or more*** digital health ***authorities*** responsible for the implementation and enforcement of this Chapter at national level. The Member State shall ***inform the Commission of*** the identity of the digital health ***authorities*** by the date of application of this Regulation. Where a ***Member State*** designated ***more than one*** digital health authority ***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 ***these various entities***. The Commission shall make this information publicly available. ***Where a Member State designates several digital health authorities, it shall designate one to act as coordinator.***

2. Each digital health authority shall be entrusted with the following tasks ***and powers***:

(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[18]***;***

(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, ▌ the development of the European electronic health record exchange format and to the elaboration of common specifications addressing ***quality,*** interoperability, security, safety***, ease of use, accessibility, non-discrimination*** 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;

▌

(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;

---

18 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 ***local, regional,*** national or Union level, to ensure interoperability, data portability and security of electronic health data ▌;

(n) cooperate with supervisory authorities in accordance with Regulation (EU) 910/2014, Regulation (EU) 2016/679***,*** Directive ***2022/2555 and*** with other relevant authorities, including those competent for cybersecurity ***and*** electronic identification***.***

▌

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 ***avoid any conflicts of interest***. The digital health authority ***staff*** shall ***act in the public*** interest ***and in an independent manner***.

5a. In the performance of their tasks, the digital health authorities shall actively cooperate and consult with relevant stakeholders' representatives, including patients' representatives, health care providers and health professionals' representatives, including health professional associations, consumer organisations and industry associations.

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:

(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;

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

▌

(viii) number of non-compliance cases with the mandatory requirements***.***

▌

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 ***Articles 8a to 8h*** of this Regulation, the digital health authority shall ***transmit the complaint to the competent*** supervisory authorities under Regulation (EU) 2016/679. ***The digital health authority shall provide the necessary information at its disposal to the competent supervisory authority under Regulation (EU) 2016/679 in order to facilitate its assessment and investigation.***

2. The ***competent*** digital health authority with which the complaint has been lodged shall inform***, in accordance with national law,*** the complainant of the progress of the proceedings and of the decision taken***, including, where applicable, that the complaint was referred to the relevant supervisory authority under Regulation (EU) 2016/679, and that the supervisory authority will, from that moment on, be the sole point of contact for the complainant in that matter***.

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.

3a. Each digital health authority shall facilitate submitting complaints.

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 8h. The relevant provisions of Regulation (EU) 2016/679 shall apply mutatis mutandis. 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 ***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***, as an organisational and technical gateway for the provision of services linked to the cross-border exchange of personal electronic health data in the context of primary use. The national contact point shall connect*** to all other national contact points for digital health and to the central ***interoperability*** 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. ▌ Each Member State shall ***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 ***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(1)*** with ▌ national contact points ***in other Member States through MyHealth@EU***. The exchange shall be based on the European electronic health record exchange format. ***Where Member States allow for additional categories, the national contact point for digital health shall enable the exchange of additional categories of electronic health data referred to in Article 5(1), point (a) insofar as Member State law has provided for these additional categories of personal electronic health to be accessed and exchanged, according to Article 5(1), point (a).***

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 ***for*** compliance checks necessary to join and remain connected to MyHealth@EU ▌. Those implementing acts shall be adopted in accordance with the ***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*** shall ensure that ▌ connected ***healthcare providers*** 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***, provided that the requirements in Article 11 of Directive 2011/24/EU are fulfilled***. 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 ***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. Those implementing acts shall be adopted in accordance with the ***examination*** procedure referred to in Article 68(2).

9. The ***national contact points referred to in paragraph 2 shall fulfil the conditions*** to join ***and*** to ***remain connected to*** MyHealth@EU ***as laid down pursuant to paragraph 4. Their compliance*** shall be ***verified through compliance checks performed*** by the ***Commission***.

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 ***services***. Those implementing acts shall be adopted in accordance with the ***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 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 ***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 ***68(2)***.

3. ***A national contact point of a third country or a system*** established at ***an*** international level ***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 legal, organizational, operational, semantic, technical and cybersecurity measures are equivalent to those applicable to Member States in the operation of MyHealth@EU services. The requirements in subparagraph 1*** shall be ***verified through compliance check performed by*** the Commission.

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 ***MyHealth@EU. These implementing acts*** shall be ***adopted in accordance with the examination procedure*** referred to in Article ***68(2)***.

The Commission shall ***maintain*** the list of ***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.***

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

[19] ***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).***

systems

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.

▌

3. 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. Providers of high-risk AI systems as defined in Article 6 of Regulation […] [AI act COM/2021/206 final], which ***do*** 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*** 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 ***provided that such requirements are compliant with Union law and do not affect the functioning or compliance of the harmonised components***.

▌

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 ***professional*** user ***as defined under Regulation (EU)***

2018/1807 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 ***professional*** 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.

Article 16a

Procurement, reimbursement and financing of EHR systems

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 provided that such requirements are compliant with Union law and do not affect the functioning or compliance of 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:

(a) ensure that ***the harmonised components of*** their EHR systems ***and the EHR systems as such, to the extent that this Chapter establishes requirements for them,*** are in conformity with the essential requirements laid down in Annex II and with the common specifications in accordance with Article 23;

(aa) ensure that the 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 in accordance with Article 24 ***before placing their systems on the market, and subsequently keep them up to date***;

(c) ensure that 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 ***the*** EU declaration of conformity ***in accordance with*** Article 26;

(e) affix the CE marking in accordance with Article 27;

(ea) indicate the name, registered trade name or registered trade mark, and the postal address and website, e-mail address or other digital contact at which they can be contacted, in the EHR system; the address shall indicate a single point at which the manufacturer can be contacted and the contact details shall be in a language that is easily understood by users and market surveillance authorities;

(f) comply with the registration obligations in Article 32;

(g) take without undue delay any necessary corrective action in respect of their EHR systems***, where they consider or have reasons to believe that such systems*** are not ***or no longer*** in conformity with the essential requirements laid down in Annex II, or recall or withdraw such systems; ***they shall then inform the national 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;***

(h) inform the distributors of their EHR systems and, where applicable, the authorised representative***,*** importers ***and the users of the non-conformity and*** of any corrective action, recall or withdrawal ***of that system***;

(i) inform the ***distributors of*** their EHR systems ***and, where applicable, the authorised representative, importers and the users,*** of any ***mandatory preventive maintenance and its frequency***;

(j) upon request ***provide*** market surveillance ***authorities in the Member States*** with all the information and documentation necessary to demonstrate the conformity of ***the*** EHR system ***which they have placed on the market or put into service*** with the essential requirements laid down in Annex II ***in the official language of the Member State;***

(k) cooperate with market surveillance authorities, at their request, on any action taken to bring their EHR systems ***which they have placed on the market or put into service*** in conformity with the essential requirements laid down in Annex II ***and Article 27a in the official language of the Member State;***

(ka) establish channels of complaint and keep a register of complaints, of non-conforming EHR systems, and keep distributors informed of any such monitoring.

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), points (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 ▌EHR system covered by the EU declaration of conformity has been placed on the market.

The source code or the programming logic included in the technical documentation shall, upon a reasoned request, be made available to the relevant authorities, if that source code or programming logic is necessary in order for them to be able to check compliance with the essential requirements set out in Annex II.

3a. A manufacturer of EHR systems established outside the Union shall ensure that its authorised representative has the necessary documentation readily available in order to fulfil the tasks referred to in Article 18(2).

3b. Manufacturers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the EHR system with the essential requirements set out in Annex II and the common specifications referred to in Article 23, in a language which can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the risks posed by the EHR system, which they have placed on the market or put into service.

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 ***agreed with*** 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 ▌ provide ***authorities of the Member States concerned a copy of the mandate and*** 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***;

(ba) without undue delay inform the manufacturer if the authorised representative has a reason to believe that an EHR system is no longer in conformity with the essential requirements laid down in Annex II;

(bb) without undue delay inform the manufacturer about complaints received by consumers and professional users;

(c) cooperate with the market surveillance authorities, at their request, on any corrective action taken in relation to the EHR systems 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 relevant authorities, upon request.

1c. In the event of a change of the authorised representative, the detailed arrangements for the change shall address at least the following aspects:

(a) the date of termination of the mandate of the outgoing authorised representative

and the date of the beginning of the mandate of the incoming authorised representative;

(b) the transfer of documents, including confidentiality aspects and property rights.

1d. Where the manufacturer is established outside the Union and has not complied with the obligations laid down in Article 17, the authorised representative shall be legally liable for non-compliance with this Regulation on the same basis as, and jointly and severally with, the manufacturer.

Article 19

Obligations of importers

1. Importers shall place on the Union market only EHR systems which are in conformity with the essential requirements 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;

(aa) the manufacturer is identified and an authorised representative in accordance with Article 18 has been appointed;

(b) the EHR system bears the CE marking of conformity ***referred to in Article 27 after the conformity assessment procedure has been completed***;

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

3. Importers shall indicate their name, registered trade name or registered trade mark and the ***postal*** address ***and website, e-mail address or other digital contact*** at which they can be contacted in a document accompanying the EHR system. ***The address shall indicate a single point at which the manufacturer can be contacted. The contact details shall be in a language easily understood by users and the market surveillance authorities. They shall ensure that any additional label does not obscure any information on the label***

provided by the manufacturer.

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 ***and Article 27a*** is jeopardised.

5. Where an importer considers or has reason to believe that an EHR system is not ***or no longer*** in conformity with the essential requirements in Annex II ***and Article 27a***, it shall not make that system available on the market***, or shall recall it or withdraw it if was already 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***, giving details, in particular, of the non-conformity and of any corrective measures, recall or withdrawal of that system taken. Where an importer considers or has reason to believe that an EHR system presents a risk to the health or safety of natural persons, it shall without undue delay inform the market surveillance authority of the Member State in which the importer is established, as well as the manufacturer and where applicable, the authorised representative***.

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 ***authorities of Member States concerned*** provide it with all the information and documentation necessary to demonstrate the conformity of an EHR system***. They shall cooperate with that authority, at its request, and with the manufacturer and, where applicable, with the manufacturer's authorised representative*** 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 ***or to ensure that their EHR systems are withdrawn or recalled***.

7a. Importers shall establish reporting channels and ensure their accessibility to allow users to submit complaints, keep a register of complaints, of non-conforming EHR systems

and EHR systems recalls. Importers shall verify whether the established channels of complaint referred to in Article 17(2) are publicly available allowing them to submit complaints and communicate any risk related to their health and safety or to other aspects of public interest protection and of any serious incident involving an EHR system. If such channels are not available, the importer shall provide for them, taking into account the accessibility needs of vulnerable groups and persons with disabilities.

7b. Importers shall investigate complaints and information on incidents involving an EHR system they made available on the market and file those complaints, as well as of system recalls and any corrective measures taken to bring the EHR system into conformity, in the register referred to in Article 17(1), point (ka), or in their own internal register. Importers shall keep the manufacturer, distributors and, where relevant, authorised representatives informed in a timely manner of the investigation performed and of the results of the investigation.

Article 20

Obligations of distributors

1. Before making an EHR system available on the market, distributors shall verify that:

   (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 ***with clear*** and ***complete*** instructions for use ***in accessible formats***;

   (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 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. Furthermore, the distributor shall inform without undue delay the manufacturer or the

importer, 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. ***Where a distributor considers or has reason to believe that an EHR system presents a risk to the health or safety of natural persons, it shall [] inform the market surveillance authority of the Member State in which the distributor is established, as well as the manufacturer and the importer.***

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. They shall cooperate with that authority, at its request, ***and with the manufacturer, the importer and, where applicable, with the manufacturer's authorised representative*** on any action taken to bring ***the*** EHR systems in conformity with the essential requirements laid down in Annex II ***or to withdraw or recall it***.

Article 21

Cases in which obligations of manufacturers of an EHR system apply to ***other economic operators***

An importer***, distributor or user*** 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 ***do any of the following:***

(a) ***make*** an EHR system available on the market under their own name or trademark***;***

(b) modify an EHR system already placed on the market in such a way that conformity with the applicable requirements may be affected***;***

(c) ***make modifications to the EHR system which lead to changes in the intended purpose as declared by the manufacturer***.

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 ***common template document and a*** time limit for implementing those common specifications. Where relevant, the common specifications shall take into account the specificities of medical devices and high risk AI systems referred to in paragraphs ***3*** and ***4*** 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 ***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 adoption of those common specifications 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] ***and the EDPB***, 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 ***have been*** preceded by a consultation with the EHDS Board ***and the EDPB, as applicable***.

Article 24

Technical documentation

1. ***Manufacturers*** shall ***draw up technical documentation*** 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 ***and a reference to the results obtained from an European digital testing environment referred to in Article 26a***.

3. The technical documentation shall be drawn up in one of the official languages of the ***Member State concerned or an easily understandable language***. 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. EHR systems shall be accompanied by an information sheet that includes concise, complete, correct and clear information that is relevant, accessible and comprehensible to ***professional*** 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. ***As an alternative to supplying the information sheet referred to in paragraph 1 with the EHR system,*** manufacturers ***may*** enter the information referred to in paragraph 2 into the EU database ▌ referred to in Article 32 ▌ .

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 ▌ 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.

3a. Digital EU declarations of conformity shall be made accessible online for the expected lifetime of the EHR system and in any event for at least 10 years after the placing on the market or the putting into service of the EHR system.

4. By drawing up the EU declaration of conformity, the manufacturer shall assume

responsibility for the ***compliance*** of the EHR system ***with the requirements laid down in this Regulation when it is placed on the market or put into service***.

4b. The Commission shall publish a standard uniformed template for the EU declaration of conformity and make it available in a digital format in all the official Union languages.

Article 26a

European digital testing environment

1. The Commission shall develop a European digital testing environment for the assessment of harmonised components of EHR systems. The Commission shall make the software supporting the European digital testing environment available as open source.

2. Member States shall set up digital testing environment for the assessment of harmonised components of EHR systems. Such environments shall comply with the common specifications for the European digital testing environments laid down pursuant paragraph 4. Member States shall inform the Commission about their digital testing environments.

3. Before placing EHR systems on the market, Manufacturers shall use the testing environments mentioned in paragraphs 1 and 2 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 the European digital testing environment. 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.

1a. The CE marking shall be affixed before placing the EHR system on the market.

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[20].

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 there about the Commission.

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 requirements applicable to and risks 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 ***necessary*** powers, ***human, financial and technical*** resources, equipment***,*** and knowledge necessary for the proper performance of their tasks pursuant to this Regulation. ***Market surveillance authorities shall be empowered to 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. ***The Commission and the Member States*** shall ***make this information publicly available.***

---

20 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).

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 ***is*** avoided.

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

4b. When a manufacturer or another economic operator fails to cooperate with market surveillance authorities or if the information and documentation provided is incomplete or incorrect, market surveillance authorities may take all appropriate measures to prohibit or restrict the relevant EHR system from being available on the market until the manufacturer cooperates or provides complete and correct information, or to withdraw it from the market or to recall it.

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 ***of one Member State has a reason to believe*** that an EHR system presents a risk to the health***,*** safety ***or rights*** of natural persons***,*** to ***the protection*** of ***personal data*** it shall ***carry out an evaluation in relation to*** the EHR system concerned ***covering all relevant requirements laid down in this regulation.*** Its authorised ***representatives*** and all other relevant economic operators ***shall cooperate as necessary with the market surveillance authorities for that purpose and*** take all appropriate measures to ensure that the EHR system concerned no longer presents that risk when placed on the market to withdraw the EHR system from the market or to recall it within a reasonable period.

1a. ***Where the market surveillance authorities consider that non-compliance is not restricted to their national territory, they shall inform the Commission and the other Member States of the results of the evaluation and of the actions which they have required the economic operator to take.***

1b. ***Where a market surveillance authority concludes that an EHR system has caused damage to the health or safety of natural persons or to other aspects of public interest protection, the manufacturer shall immediately provide information and documentation, as applicable, to the affected person or user and, as appropriate, other third parties affected by the damage caused to the person or user, without prejudice to data protection rules.***

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

3. The market surveillance authority shall ***without undue delay*** inform the Commission and the market surveillance authorities***, or, if applicable, the supervisory authorities under Regulation (EU) 2016/679,*** 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.

3a. ***Where a finding of a market surveillance authority, or a serious incident it is informed of, concerns personal data protection, the market surveillance authority shall without undue delay inform and cooperate with the relevant supervisory authorities under Regulation (EU) 2016/679.***

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) ***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 ***3*** days after the manufacturer becomes aware of the serious incident involving the EHR system.

5. The ▌ authorities referred to in paragraph 4 shall inform the other ▌ 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 presenting a risk, including risks related to interoperability, security and patient safety, and of any corrective action, recall or withdrawal of such EHR systems.

6b. 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***, inter alia,*** 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 ***bring*** the ***EHR system into conformity***:

(a) the EHR system is not in conformity with essential requirements laid down in Annex II ***and with the common specifications in accordance with Article 23***;

(b) the technical documentation is ▌ not available***,*** not complete ***or not in accordance with Article 24***;

(c) the EU declaration of conformity has not been drawn up or has not been drawn up correctly ***as referred to in Article 26***;

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

(da) the registration obligations of Article 32 have not been fulfilled.

1a. Where the relevant economic operator does not take adequate corrective action within a reasonable period, the market surveillance authorities shall take all appropriate provisional measures to prohibit or restrict the EHR system being made available on their national market, to withdraw the EHR system from that market or to recall it.

The market surveillance authorities shall inform the Commission and the other Member States, without delay, of those measures. This information shall include all available details, in particular the data necessary for the identification of the noncompliant EHR system, the origin of that EHR system, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant economic operator. In particular, the market surveillance authorities shall indicate whether the noncompliance is due to any of the following:

(a) failure of the EHR system to meet the requirements relating to the essential requirements set out in Annex II;

(b) shortcomings in the common specifications referred to in Article 23;

(d) Member States other than the Member State initiating the procedure under this Article shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the EHR system concerned, and, in the event of disagreement with the adopted national measure, of their objections;

(e) Where, within three months of receipt of the information referred to in the second subparagraph, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified.

2. Where the non-compliance referred to in paragraph 1 persists, the ***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.

Article 30a

Union safeguard procedure

1. ***Where, on completion of the procedure set out in Article 29(2) and Article 30(1a), objections are raised against a measure taken by a Member State, or where the Commission considers a national measure to be contrary to Union law, the Commission shall without delay enter into consultation with the Member States and the relevant economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall adopt an implementing act in the form of a decision determining whether the national measure is justified or not. The Commission shall address its decision to all Member States and shall immediately communicate it to them and to the relevant economic operator or operators.***

2. ***If the national measure is considered justified, all Member States shall take the necessary measures to ensure that the non-compliant EHR system is withdrawn from their market, and shall inform the Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw that measure.***

Section 5

Other provisions on interoperability

Article 31

▌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 ***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 ***shall***, by means of implementing acts, determine the format and content of the label. Those implementing acts shall be adopted in accordance with the ***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 ***easily understandable*** languages determined by the Member State(s) ▌ in which the wellness application is placed on the market ***or put into service***.

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

6. If the wellness application is ***an integral part of a device or*** embedded in a device ***after its putting into service***, the accompanying label shall be ***shown in the application itself or*** placed on the device ***and in the case of software a digital label. Two-dimensional,*** 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 ▌ .

Article 31a

Interoperability of wellness applications with EHR systems

1. Manufacturers of wellness applications may claim interoperability with an EHR system, after relevant conditions are met. When this is the case, the users of such wellness applications shall be duly informed about such interoperability and its effects.

2. The interoperability of wellness applications with EHR systems shall not mean automatic sharing or transmission of all or part of the health data from the wellness application with the EHR system. The sharing or transmission of such data shall only be possible following the consent of the natural person and in accordance with Article 8B of this Regulation and interoperability shall be limited exclusively to this end. The manufacturers of wellness applications claiming interoperability with an EHR system

shall ensure that the user is able to choose which categories of health data from the wellness application they want to insert in the EHR system and the circumstance for that sharing or transmission.

Section 5a

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 ***and include the results of the test environment as mentioned in Article 26a***.

3. Medical devices***, in vitro diagnostic medical devices*** or high-risk AI systems referred to in paragraphs ***1*** and ***2*** of Article 14 of this Regulation shall ***also*** 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.

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.

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. In that case, the data shall still be considered as being made available from several data holders.

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) ***electronic health data from*** EHRs;

(b) data ***on factors*** impacting on health, including ***socio-economic***, 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) ▌ pathogen ▌ data, impacting on human health;

(d) ***healthcare-related*** administrative data, including ***dispensation,*** claims and reimbursement data;

(e) human genetic, ***epigenomic*** and ***genomic*** data;

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

(f) ***automatically*** generated ***personal*** electronic health data, ***through*** medical devices ▌ ;

(fa) data from wellness applications;

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

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

(i) ▌ data from medical registries ***and mortality registries***;

(j) ▌ data from clinical trials***, clinical studies and clinical investigations subject to Regulation (EU) 536/2014, Regulation [SOHO], Regulation (EU) 2017/745 and Regulation (EU) 2017/746, respectively***;

(k) ***other*** health data from 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) ▌ health data from biobanks and ***associated*** databases***.***

▌

6. Where 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*** it may be supported by a health data access body to ***providing*** technical support to process the data or ***combining*** it with other data for joint analysis.

▌

8. ***Member States*** may provide ***by virtue*** of ▌ national law ***that additional categories of*** electronic health data ***shall be made available for secondary use pursuant to this Regulation***.

8a. 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 and additional safeguards at national level aimed at safeguarding the sensitivity and value of the data that falls under Article 33 (1) points (e), (fa), (m) 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 33a

Intellectual property rights and trade secrets

1. Electronic health data protected by intellectual property rights, trade secrets and/or covered by the regulatory data protection right provided by Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004 shall be made available for secondary use in accordance with the principles set forth in this Regulation. In this respect, the following shall apply:

(a) health data holders shall inform the health data access body of and identify any electronic health data containing content or information protected by intellectual property rights, or trade secrets and/or covered by the regulatory data protection right provided by Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004. They shall indicate which parts of the datasets are concerned and justify why the data needs the specific protection which the data benefits from. This information shall be provided when communicating to the health data access body the dataset descriptions pursuant to Article 41(2) for the

datasets it holds, or at the latest following a request received from the health data access body;

(b) health data access bodies shall take all specific appropriate and proportionate measures, including legal, organisational, and technical ones, they deem necessary to preserve the protection of intellectual property rights, trade secrets and/or the regulatory data protection right provided by Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004. the determination of the necessity and appropriateness of such measures shall rest with the health data access body;

(c) when issuing data permits, health data access bodies may condition the access to certain electronic health data to legal, organisational, and technical measures. Such measures may include contractual arrangements between health data holders and health data users in order to share data containing information or content protected by intellectual property rights or trade secrets. The Commission shall develop and recommend non-binding model contractual terms for such arrangements;

(d) should the granting of access of electronic health data for secondary purpose incur a serious risk that cannot be addressed in a satisfactory manner of infringing the intellectual property rights, trade secrets and/or the regulatory data protection right provided by Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004, the health data access body 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. Health data holders and health data users shall have the right to lodge a complaint in accordance with Article 38b.

Article 34

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

1. Health data access bodies shall only ***grant*** access ***for secondary use*** to electronic health data referred to in Article 33 ***to a health data user*** where the ▌processing ***of the data*** by the ***data user is necessary for one of the following purposes***:

(a) ▌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) ***statistics, such as*** national, multi-national and Union level official statistics ***defined in Regulation (EU) No 223/2009***[21] 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***,*** ▌ contributing to public health or ***health technology assessment,*** or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices***, with the aim of benefitting the end-users, such as patients, health professionals and health administrators, including:***

(i) development and innovation activities for products or services;

(ii) training, testing and evaluating of algorithms, including in medical devices***, in-vitro diagnostic medical devices***, AI systems and digital health applications ▌;

▌

(h) ***improving delivery of care, treatment optimization and providing healthcare***, based on the ***electronic*** health data of other natural persons.

2. Access to electronic health data ***for*** the purposes referred to in points (a) to (c) of paragraph 1 ***is 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

---

21 ***Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).***

that public sector body or of Union institutions, agencies and bodies.

▌

Article 35

Prohibited secondary use of electronic health data

Health data users shall only process electronic health data for secondary use on the basis of and in accordance with the purposes laid down in a data permit pursuant to Article 46 or data requests pursuant to Article 47.

In particular, seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 46 ***or a data request granted pursuant to Article 47*** for the following ***uses*** 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 economic,*** effects or similarly significantly affect those natural persons;

(b) taking decisions in relation to a natural person or groups of natural persons ***in relation to job offers or offering less favourable terms in the provision of goods or services, including*** to exclude them from the benefit of an insurance ***or credit*** contract or to modify their contributions and insurance premiums ***or conditions of loans, or taking any other decisions in relation to a natural person or groups of natural persons having the effect of discriminating on the basis of the health data obtained***;

(c) advertising or marketing activities ▌;

▌

(e) developing products or services that may harm individuals***, public health or*** societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco ***and nicotine*** products, ***weaponry*** or ***products*** or services which are designed or modified in such a way that they ***create addiction or that they*** contravene public order or ***cause a risk for human health;***

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

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 ***carrying out the tasks set out in Articles 37, 38 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 ***tasks*** with the other health data access bodies ***both within the Member State and towards health data access bodies in other Member States***.

Each health data access body shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the health data access bodies shall cooperate with each other and with the Commission, and, for concerns regarding data protection, with the relevant supervisory authorities.

2. Member States shall ensure that each health data access body is provided with the human ▌ and financial resources ***and necessary expertise, to support their tasks and the exercise of its powers.***

Where an assessment by ethic bodies is required under national law, those bodies shall make expertise available to the health data access body. As an alternative, Member States may provide for ethics bodies integrated into the health data access body.

Member States shall also ensure technical resources, premises and infrastructure necessary for the effective performance of its tasks and the exercise of its powers.

2a. Member States shall ensure that any conflict of interest between the different tasks of health data access bodies is avoided. This may include organisational safeguards such as functional segregation between health data access bodies' different functions, including between assessing applications, the reception and preparation of datasets, including anonymisation, pseudonymisation, as well as provisioning data in secure processing environments.

3. In the performance of their tasks, health data access bodies shall actively cooperate with ***relevant*** stakeholders' representatives, especially with representatives of patients, data holders and data users ***and*** shall avoid any conflicts of interest. ▌

3a. In the performance of their tasks and exercise of their powers in accordance with this Regulation, health data access bodies shall avoid any conflicts of interest. Health data access bodies' staff shall act in the public interest and in an independent manner.

4. Member States shall ***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 ***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 ▌ remit for secondary use and decide on data requests ***pursuant to Article 47*** in accordance with ***this Chapter and*** Chapter II of Regulation ***(EU) 2022/868 including:***

(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;

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

(vi) request electronic health data referred to in Article 33 from relevant health data holders pursuant to a data permit or a data request granted;

(d) process electronic health data ***referred to*** in Article ***33 such as the receiving***, combination, preparation and ***compiling*** of ***necessary requested*** data ***from health data holders,*** the ***pseudonymisation or anonymisation*** of ***the*** data***;***

▌

(f) take all measures necessary to preserve the confidentiality of IP rights and ***regulatory data protection, and the confidentiality*** of trade secrets ***as provided for in Article 35a and taking into account the relevant rights of both the health data holder and health data user***;

▌

(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 those applications*** 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 ***common standards, technical requirements and*** appropriate measures ▌ 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 ***the secondary*** use and management ***of electronic health data***;

(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**;**

▌

(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 ***55,*** 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 Article 8 of Regulation […] [Data Governance Act COM/2020/767 final];

(ii) all ***health*** data ***applications and*** requests ***without undue delay*** after ***initial reception***;

(iia) all health data permits or requests granted as well as rejection decisions, including their justification, within 30 working days of their issuance;

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

(iv) results communicated by ***health*** data users pursuant to Article ***XX***;

(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 35e;

▌

(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 ▌ in relation to personal electronic health data and the EHDS Board;

▌

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

(d) cooperate with other national competent bodies, including the national competent bodies supervising data altruism organisations under Regulation ***(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.

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 and accessible for natural persons*** 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 ***to the health data user***;

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

(da) the identity and the contact details of the health data access body;

(db) the record on who has been granted access to which sets of electronic health data and the permit regarding the purposes for processing them as referred to in Article 34(1);

(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 opt out 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 opt out and facilitate the exercise of this right***.

3. Where a health data access body is informed by a ***health*** data user of a ***significant*** finding ***related to*** the health of a natural person, ***as referred to in Article 41a(5) of this Regulation,*** the health data access body ***shall*** inform the ***data holder about that finding. The data holder shall, under the conditions laid down by national law, inform the*** natural person ▌or ▌treating health professional***. Natural persons shall have the right to request not to be informed of such findings***.

4. Member States shall ▌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 ***a biennial*** activity report ***and make it publicly available on its website. If a Member State 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 in the EHDS Board. The activity report shall contain at least the following ***categories of information***:

(a) information relating to the data access applications ***and data requests*** 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;

▌

(c) information on the fulfilment of regulatory and contractual commitments by ***health*** data users and ***health*** data holders, as well as ***the number and amount of administrative fines*** imposed ***by health data access bodies***;

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

(e) information on ***internal and third party*** audits on compliance of secure processing environments with the defined standards, specifications and requirements***, as referred to in 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 ▌;

▌

(i) revenues from data permits and data requests;

▌

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

(l) number of data quality labels issued ***by data holders***, 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 ***sent*** to the Commission ***and the EHDS Board within 6 months after the end date of the 2 year reporting period. The report shall be accessible via the Commission's website***.

▌

Article 41

Duties of ***health*** data holders

1. ***Health*** data ***holders shall*** make ***relevant*** electronic health data available under Article 33 ***upon request to*** the health data access ***body according to a data permit pursuant to Article 46 or data request pursuant to Article 47***.

1b. 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 no later than 3 months of receiving the request from the health data access body. In justified cases the health data access body may extend this period by up to three 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.

6. ***Health*** 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.

Article 41a

Duties of health data users

1. Health data users may access and process the electronic health data for secondary use referred to in Article 33 only in accordance with a data permit pursuant to Article 46, a data request pursuant to Article 47 or, in situations referred to in Article 45(3), a data access approval of the relevant authorised participant.

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.

2a. Health data users shall not re-identify or seek to re-identify the natural persons to which the electronic health data which they obtained based on the data permit, data request or access approval decision by an authorized participant in Health Data EU relate.

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. Without prejudice to paragraph 2, health data users shall inform the health data access body of any significant findings related to the health of the natural person whose data are included in the dataset.

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 42

Fees

1. Health data access bodies***, including EU access services or trusted health*** data holders ***referred to in Article 49*** may charge fees for making electronic health data available for secondary use.

Such fees shall ▌ 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 ***access*** application or a data request, granting, refusing or amending a data permit pursuant to ***Article*** 45 and 46 or providing an answer to a data request pursuant to Article 47, ***including costs related to the consolidation, preparation, anonymisation, pseudonymisation, and provisioning of the electronic health data.***

Reduced fees may be established by the Member States for certain types of data users located in the Union, such as public sector bodies or Union institutions, offices, agencies and bodies with a legal mandate in the field of public health, university researchers or micro-enterprises.

2. ***The fees may include compensation for the costs incurred by the health data holder for compiling and preparing the electronic health data to be made available for secondary***

use. The health data holder shall provide an estimate of such costs to the health data access body. 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.

▌

4. Any fees charged to ***health*** data users pursuant to this Article by the health data access bodies or ***health*** data holders shall be transparent and ***non-discriminatory.***

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 ***shall***, by means of implementing acts, lay down principles ▌ for the fee policies and fee structures***, including deductions for the entities listed in paragraph 1, second sub-paragraph, in order to support consistency and transparency between Member States***. Those implementing acts shall be adopted in accordance with the ***examination*** procedure referred to in Article 68(2).

Article 43

Enforcement by health data access bodies

▌

2. When ***carrying out their monitoring and supervisory tasks, as referred to in Article 37(1), point (ra)***, the health data access bodies shall ***have the right*** to ***request and receive all*** the ***necessary information from health data holders and health data users to verify***

compliance ***with this Chapter***.

3. Where health data access bodies find that a ***health*** data user or ***health*** data holder does not comply with the requirements of this Chapter, they 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 ***the concerned health data user or the health data holder*** the opportunity to state its views within ***a reasonable time that shall not exceed 4 weeks.***

Where the finding of non-compliance concerns a possible breach of Regulation (EU) 2016/679, the health data access body shall immediately inform the supervisory authorities under Regulation (EU) 2016/679 and provide them with all relevant information concerning this finding.

4. ***With regard to non-compliance by a health data user,*** 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 ***without undue delay***, and shall take appropriate and proportionate measures aimed at ensuring compliant processing by the ***health*** data users.

As part of such measures, the health data access bodies shall ***also*** be able, where appropriate, to ***exclude or initiate proceedings*** to exclude ***in accordance with national law the health*** 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.

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(1b)***, the health data access body shall have the power to fine the ***health*** data holder ▌ for each day of delay ***with periodic penalty payment***, which shall be transparent and proportionate. The amount of the fines shall be established by the health data access body ***in accordance with national law***. In case of repeated breaches by the ***health*** data holder of the obligation of ▌ cooperation with the health data access body, that body ***may*** exclude ***or initiate proceedings in accordance with national law the health to exclude*** data holder from ***submitting data access applications*** pursuant to ***Chapter IV for a period of up to 5 years, while still being obliged to make data accessible pursuant to***

Chapter IV, where applicable.

6. The health data access body shall communicate the measures imposed pursuant to ***paragraphs*** 4 and ***5 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*** pursuant to paragraph 4 shall be ***notified to other health data access bodies, through the tool referred to in paragraph 8.*** Health data access bodies ***may make this information available on their websites***.

8. The Commission ***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 ***measures related to non-compliance*** referred to in this Article, especially ***periodic penalty payments, revoking of data permits*** and exclusions***, as part of the HealthData@EU infrastructure***. Those implementing acts shall be adopted in accordance with the ***examination*** procedure referred to in Article 68(2).

▌

10. The Commission ***shall issue*** guidelines***, after 3 years of entry of application of Chapter 4, in close cooperation with EHDS Board, on enforcement measures including periodic penalty payments and other measures*** to be applied by the health data access bodies.

Article 43a

General conditions for the imposition of administrative fines by health data access bodies

1. Each health data access body shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements referred to in paragraphs 4 and 5 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 43(4) and (5). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement;

(b) whether any penalties or administrative fines have already been applied by other competent authorities for the same infringement;

(c) the intentional or negligent character of the infringement;

(d) any action taken by the health data holder or health data user to mitigate the damage caused;

(e) the degree of responsibility of the health data user, taking into account technical and organisational measures implemented by them pursuant to Article 45(2), points (e) and (f), and Article 45(4) of this Regulation;

(f) any relevant previous infringements by the health data holder or health data user;

(g) the degree of cooperation with the health data access body, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(h) the manner in which the infringement became known to the health data access body, in particular whether, and if so to what extent, the health data user notified the infringement;

(i) where measures referred to in Article 43(4) and (5) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a health data holder or health data user intentionally or negligently, for the same or linked health data permits or health data requests, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. In accordance with paragraph 2, infringements of the obligations of the health data holder or health data user pursuant to Article 41 and Article 41a(1), (4), (5) and (7) shall be subject to administrative fines of up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial

year, whichever is higher.

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines of up to EUR 20 000 000, or in the case of an undertaking, of up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) health data users processing electronic health data obtained via a data permit issued in line with Article 46 for the purposes referred to in Article 35;

(b) health data users extracting personal electronic health data from secure processing environments;

(c) re-identifying or seeking to re-identify the natural persons to whom the electronic health data which they obtained based on the data permit or data request pursuant to Article 41a(3) relate;

(d) non-compliance with enforcement measures by the health data access body pursuant to Article 43.

6. Without prejudice to the corrective powers of health data access bodies pursuant to Article 43, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

7. The exercise by the health data access body of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedies and due process.

8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that, in accordance with their national legal framework, ensures that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by health data access bodies. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify the Commission of the provisions of their laws which they adopt pursuant to this paragraph by ... [date of application of this Chapter of this Regulation] and, without delay, any subsequent amendment law or amendment affecting them.

Article [43b]

Relationship with data protection supervisory authorities

The supervisory authority or authorities responsible for monitoring and enforcement the application of Regulation (EU) 2016/679 shall also be responsible for monitoring and enforcement of the right to object to the processing of personal electronic health data for secondary use pursuant to Article 35f. The relevant provisions of Regulation (EU) 2016/679 shall apply mutatis mutandis. They shall be competent to impose administrative fines up to the amount referred to in Article 83 respectively of that Regulation. 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

Access to electronic health data ***for secondary use***

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 ***that are adequate,*** relevant ***and limited to what is necessary in relation to*** the purpose of processing indicated in the data access application by the ***health*** data user and in line with the data permit granted.

2. The health data access bodies shall provide ▌ electronic health data in an anonymised 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 ***health data user has sufficiently demonstrated that the*** purpose of ▌ processing cannot be achieved with anonymised data ***in line with Article 46(1), point (c)***, 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 ***or a body that acts as trusted third party in accordance with national law.***

Article 45

Data access applications

1. ***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) the health data applicant's identity, description of professional functions and operations, including the identity of the natural persons who will have access to electronic health data, if a data permit is granted; the list of natural persons can be updated and in that case it shall be notified to the health data access body;

(a) ***which of the purposes referred to in Article 34(1) access is sought for;***

(ab) detailed explanation of the intended use ***and expected benefit related to the use*** of the electronic health data ***and how this benefit contributes to*** the purposes referred to in ***point (a);***

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

(c) ***a description*** whether electronic health data ***need to*** be made available in ***a pseudonymised or*** anonymised format***, in case of pseudonymised format, a justification why the processing cannot be pursued using anonymised data***;

(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***, proportionate to the risks,*** planned to ***prevent any misuse of the electronic health data, as well as to*** protect the rights and interests of the ***health*** data holder and of the natural persons concerned***, including to prevent any re-identification of natural persons in the dataset***;

(g) ***a justified 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***;***

(ha) where applicable, information on the assessment of ethical aspects of the

processing, obtained in line with national law, which may serve to replace their own ethics assessment;

(hb) where the applicant wants to make use of an exception under Article 35f(3), the explanations required by national law pursuant to that Article.

3. ***Where a*** data ***applicant*** seeking access to electronic health data from ***health data holders established in*** more than one Member State ***or from the relevant authorised participants referred to in Article 52, the applicant*** shall submit a single ***data access*** application ***through*** the ▌ health data access ***body*** of ***the main establishment of the applicant or of one of these data holder 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 and to the*** health data access bodies of the ***Member States where the health data holders identified in*** the data access application ***are established***.

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

(a) a description of how the processing would comply with ***applicable Union and national law on data protection and privacy, notably Regulation (EU) 2016/679 and, notably,*** Article 6(1) of Regulation (EU) 2016/679;

▌

5. ▌ 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.

▌

Article 46

Data permit

1. ***The*** health data access bodies shall ***decide to grant access to electronic health data only***

when the following cumulative criteria are fulfilled***:***

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

(b) the requested data is necessary, adequate and proportionate for the purpose or purposes described in the health 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) Regulation (EU) 2016/679, in particular that in the case of pseudonymized data, there is sufficient justification that the purpose cannot be achieved with anonymized data;

(e) the applicant is qualified vis-à-vis the intended purposes of data use and has appropriate expertise, including professional qualifications in the areas of healthcare, care, public health, research, consistent with ethical practice and applicable laws and regulations;

(f) the applicant demonstrates sufficient technical and organisational measures to prevent misuse of the electronic health data and to protect the rights and interests of the data holder and of the natural persons concerned;

(g) the information on the assessment of ethical aspects of the processing, where applicable, is in line with national law;

(h) where the applicant wants to make use of an exception under Article 35f(3), the explanations required by national law adopted pursuant to that Article;

(ha) all other requirements in this Chapter are fulfilled by the health data applicant.

1a. The health data access body shall also take into account the following risks:

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

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

2. ***If the*** health data access ***body in its assessment comes to the conclusion that the***

requirements in paragraph 1 are met and the risks referred to in paragraph 1A 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.

Where the requirements for granting a data permit are not met, but the requirements to provide an answer in an anonymous statistical format under article 47 are met, the 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, provided that the health data applicant agrees to this change of procedure.

3. ***By way of derogation from Regulation (EU) 2022/868, the*** health data access body shall issue or refuse a data permit within ***3*** months of receiving ***a complete*** data access application. ***If the health data access body finds that the data access application is incomplete, it shall notify the health data applicant, who shall be given the possibility of completing their application. If the health data applicant does not fulfill this request within four weeks, a permit shall not be granted.*** The health data access body may extend the period for responding to a data access application by ***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. ▌

3a. When handling a data access application for cross-border access to electronic health data referred to in Article 45(3), 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.

A data permit issued by one concerned health data access body may benefit from mutual recognition by the other concerned health data access bodies.

3b. ***Member States shall provide for an accelerated application procedure for public sector bodies and Union institutions, bodies, offices and agencies with a legal mandate in the field of public health if the processing of the data is to be carried out for the purposes in Article 34(1), points (a), (b) and (c). Under this accelerated procedure, the HDAB shall issue or refuse a data permit within 2 months of receiving a complete data access application.***

The HDAB may extend the period for responding to a data access application by 1 additional month where necessary.

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 ***health data*** applicant.

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

(a) ***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) where an exception under Article 35f(3) has been applied for, information on whether it has been granted or not and the reason for that decision;

(ba) the identity of authorised persons, in particular the identity of the principal

investigator, 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 ***a secure processing environment in*** accordance with the data permit delivered to them on the basis of this Regulation.

▌

9. A data permit shall be issued for the duration necessary to fulfil the requested purposes which shall not exceed ***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 ***10*** years. ▌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 ***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*** 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 ***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.

▌

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 ***examination*** procedure referred to in Article 68(2).

Article 47

Health data request

1. ***The applicant*** may submit a ***health*** data request for the purposes referred to in Article 34 ***with the aim of obtaining an answer only in anonymised statistical format***. A health data access body shall ***not*** provide an answer to a ***health*** data request in ***any other*** format and the ***health*** data user shall have no access to the electronic health data used to provide this answer.

2. A ***health*** data request ***referred to in paragraph 1*** shall include the ***following information***:

   (a) a description of the ***applicant's identity, professional function and activities;***

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

   (ba) a description of the requested electronic health data, their format and data sources, where possible;

   (bb) a description of the statistic's content;

   (bd) a description of the safeguards planned to prevent any misuse of the electronic health data;

   (be) 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;

   (bf) where the applicant wants to make use of an exception under Article 35f(3), the explanations requited by national law pursuant to that Article.

2a. The health data access body shall assess if the request is complete and take into account the risks mentioned above in Article 46(1a).

3. The health data access body shall assess ***the health data request***, within ***3*** months and, where possible, provide the result to the ***health*** data user within ***3*** months.

Article 47a

Templates to support access to electronic health data for secondary use

The Commission shall, 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.

I

Article 35f

Right to opt-out from the processing of personal electronic health data for secondary use

1. ***Natural persons shall have the right to opt-out at any time and without stating reasons from the processing of personal electronic health data relating to them for secondary use under this Regulation. The exercise of this right shall be reversible.***

2. ***Member States shall provide for an accessible and easily understandable opt-out mechanism to exercise this right, whereby natural persons shall be offered the possibility to explicitly express their will not to have their personal electronic health data processed for secondary use.***

2a. ***After natural person has opted out, and where personal electronic health data relating to them can be identified in a dataset, personal electronic health data relating to them shall not be made available or otherwise processed pursuant to data permits pursuant to Article 46 or data requests pursuant to Article 47 granted after the natural person has opted out. This shall not affect the processing of personal electronic health data relating to that natural person for secondary use pursuant to data permits or data requests that were granted before the natural person has opted out.***

3. ***Member States may establish by national law a mechanism to make data in regard of which an opt-out mentioned in paragraph 1 has been exercised, available under the following conditions:***

(i) ***The data access or request application is submitted by a public sector body or a Union institution, body, office or agency with a mandate in carrying out tasks in the area of public health, or by another entity entrusted with carrying out public tasks in the area of public health, or acting on behalf of or commissioned by a***

public authority, when necessary for any of the following purposes:

a. the purposes referred to in Article 34(1), points (a) to (c);

b. scientific research for important reasons of public interest;

(ii) the data cannot be obtained by alternative means in a timely and effective manner under equivalent conditions;

(iii) the applicant has provided the justification referred to in Articles 46(1), point (h), or Article 47(2), point (be).

Conditions listed under points i), ii) and iii) shall be cumulatively fulfilled.

The national law providing for such a mechanism shall contain, specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons.

Where a Member State has decided to provide for the possibility to request access to data in regard of which an opt-out has been exercised referred to in this paragraph in its national law and these criteria are met, the data for which an opt-out pursuant to paragraph 1 has been exercised may be included when carrying out the tasks under Article 37(1), points (a) (iii), (vi) and (d).

4. The exceptions in paragraph 3 shall respect the essence of the fundamental rights and freedoms and be a necessary and proportionate measure in a democratic society to fulfil public interest in the area of legitimate scientific and societal objectives.

5. Any processing according to the exception in paragraph three shall comply with the requirements of this Chapter, notably the ban on re-identification, including attempts, in accordance with Article 41(2a). Any legislative measure referred to in paragraph 3 shall contain specific provisions for safety and protection of the rights of natural persons.

6. Members States shall notify the Commission of the provisions of their law which they adopt pursuant to paragraph 3 of this Article, without delay, any subsequent amendment affecting them.

7. If the purposes for which a health data holder processes personal electronic health data do not or do not longer require the identification of a data subject by the controller, the

health data holder shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the right to opt out under this Article.

Article 49

Simplified procedure for access to electronic health data from a ***trusted health*** data holder

1. Where ***a health data*** access ***body receives a data*** access application ***pursuant to Article 45*** or a data request ***pursuant to*** Article ***47,*** that ***only covers electronic health data held by a trusted health*** data ***holder designated pursuant to paragraph 2, the procedure in paragraphs 3 to 6*** shall ***apply.***

1a. Member States may establish a procedure by which health data holders may apply to be designated as trusted health data holders, where the health data holder meets the following conditions:

(i) can provide access to health data through a secure processing environment that complies with Article 50;

(ii) has the necessary expertise to assess data access applications and data requests;

(iii) provides the necessary guarantees to ensure compliance with this regulation.

Member States shall designate trusted single data holders following an assessment of these conditions by the relevant health data access body.

Member States shall establish a procedure to regularly review whether the trusted health data holder continues to fulfil these conditions.

Health data access bodies shall indicate the trusted single data holders in the dataset catalogue referred to in Article 55.

2. ▌Data ***access applications and data requests referred to*** in ***paragraph 1*** shall ***be submitted*** to the ▌health data ***access body, which may forward them to the relevant trusted health data holder***.

3. ***The trusted health data holder shall assess the data access application or data request against the criteria listed in Article 46(1) and (1a) or Article 47(2) and (2a), as applicable***.

4. ***The trusted health*** data holder shall ***submit its assessment, accompanied by a proposal for decision, to*** the ▌ health data access body ***within 2 months after receipt of the application from*** the health data access body***. Within 2 months from receipt of the assessment, the health data access body shall issue a decision on the data access application or data request pursuant to this*** Article***.*** The health data access body ***shall not be bound by the proposal submitted by the trusted data holder.***

5. Following the health data access body's decision to issue the data permit or grant the data request, the trusted health data holder shall carry out the tasks referred to in Article 37(1)(d) and Article 37(1)(iii).

4a. The Union Health Data Access Service may designate health data holders that are Union institutions, bodies or agencies which comply with the criteria in paragraph 1 as trusted health data holders. Where it does so, paragraphs 2 to 5 apply mutatis mutandis.

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, ***the secure processing environment*** shall ***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 ***technical and organisational measures***;

(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. ***Logs of access should be kept for not shorter than one year;***

(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 ***from health data holders in the format determined by the data permit*** 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 shall ensure by reviewing that the health*** data users ***are*** only able to download non-personal electronic health data ***including, electronic health data in an anonymised statistical format*** from the secure processing environment.

3. The health data access bodies shall ensure regular audits***, including by third parties,*** of the secure processing environments ***and take corrective actions for any shortcomings, risks or vulnerabilities identified in 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***, organisational***, information security***, confidentiality, data protection*** 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 ***examination*** procedure referred to in Article 68(2).

Article 51

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 body pursuant to Article 41(1)***

and (1a). The health data access body shall be deemed ***controller for the processing of the personal*** electronic health data ***when fulfilling its tasks pursuant to this Regulation. Notwithstanding the previous sentence, the health data access body shall be deemed to act as a processor on behalf of the health data user as controller for the processing pursuant to a*** data permit ***in the secure processing environment when providing data through such environment as well as for the processing to generate an answer to a data request pursuant to Article 46***.

1a. ***In situations referred to in Article 49, the trusted 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 trusted health data holder shall be deemed to act as a processor for the health data user when providing data through a secure processing environment.***

2. The Commission ***may***, by means of implementing acts, establish a template for ***controller-processor agreements in the situation of Article 51, paragraphs (1) and (1a)***. Those implementing acts shall be adopted in accordance with the ***examination*** procedure set out in Article 68(2).

Section 4

Cross-Border ***infrastructure for secondary use of*** electronic health data ▌

Article 52

▌ HealthData@EU ▌

1. Each Member State shall designate ***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*** shall ***inform the Commission of the name*** and contact details ***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 contact point referred to in paragraph 1a*** shall ***connect to*** the cross-border infrastructure for secondary use of electronic health data (HealthData@EU). The national contact points ***and contact point referred to in paragraph 1a*** shall facilitate the cross-border access to electronic health data for secondary use for different authorised participants in the infrastructure***. The national contact points*** shall cooperate closely with each other and with the Commission.

▌

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 ***may become*** authorised participants of ***and connect to*** HealthData@EU.

5. Third countries or international organisations may become authorised participants where they comply with the rules of Chapter IV of this Regulation***,*** provide access to data users located in the Union, on equivalent terms and conditions, to the electronic health data available to their health data access bodies***, subject to compliance with Chapter V of Regulation (EU) 2016/679***. The Commission may 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 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 ***examination*** procedure referred to in Article 68 (2). The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available.

6. Each ***national contact point and*** authorised participant shall acquire the required technical capability to connect to and participate in HealthData@EU. ***They*** shall comply with the requirements and technical specifications needed to operate the cross-border infrastructure and to allow ***them*** to connect to ▌ it.

▌

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 ▌ and authorised participants in that infrastructure ***and the central platform referred to in paragraph 9***.

9. The Commission shall develop, deploy and operate a ***central*** platform for HealthData@EU by providing information technology services needed to ***support and*** facilitate the ***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 ▌ controllers as a processor.

10. Where requested by two or more ***national contact points in this infrastructure***, the Commission may provide a secure processing environment for data from more than one Member State compliant with the requirements of Article 50. Where two or more ***national contact points or authorised participants*** put electronic health data in the secure processing environment managed by the Commission, they shall be joint controllers and the Commission shall be processor ***for the purpose of processing data in that environment***.

11. The ***national contact points*** shall act as joint controllers of the processing operations in which they are involved carried out in HealthData@EU and the Commission shall act as ***their*** processor***, without affecting the health data access bodies tasks prior and following these processing operations***.

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 ***Regulation (EU) 2022/868 and Regulation (EU) 2023/2854***.

13. The Commission ***shall***, by means of implementing acts, set out:

(a) requirements, technical specifications, the IT architecture of HealthData@EU, ***which shall ensure state-of-the-art data security, confidentiality, and protection of electronic health data in the cross border infrastructure***;

(aa) conditions and compliance checks ▌ to join and remain connected to HealthData@EU and conditions for temporary ***disconnection*** or definitive exclusion from HealthData@EU***, including specific provisions for cases of serious***

misconduct or repeated violation;

(b) the minimum criteria that need to be met by the ***national contact points and the*** authorised participants in the infrastructure;

(c) the responsibilities of the ▌ controllers and processor(s) participating in the cross-border infrastructures;

(d) the responsibilities of the ▌ 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 ***examination*** procedure referred to in Article 68(2).

14. ***Following a positive outcome of the compliance check, the Commission may, by means of implementing act, take decisions to connect individual authorised participants to*** the infrastructure***. These implementing acts shall be 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

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 ***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 ▌ 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.

▌

Section 5

Health data quality and utility for secondary use

Article 55

Dataset description ***and datasets catalogue***

1. The health data access ***body*** shall***, through a publicly available and standardised machine-readable datasets catalogue, provide information, in the form of metadata,*** about the available datasets and their characteristics ▌. ***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 ▌elements ***health*** data holders are to provide for datasets and their characteristics. Those implementing acts shall be adopted in accordance with the ***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 ***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 ***elements*** set out in paragraph 3.

3. The data quality and utility label shall ***cover*** the following elements***, where applicable***:

(a) for data documentation: meta-data, support documentation, data ***dictionary, format and*** standards used, provenance***, and when applicable, data model***;

(b) ***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***, 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 ***modifications***: merging and adding data to an existing dataset, including links with other datasets;

(fa) 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.

3a. Where a health data access body has reason to believe that a data quality and utility label may be inaccurate, it shall assess whether the data meets the requirements in paragraph 3 and shall revoke the label in the event the data does not meet the required quality.

4. The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the list of ***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 ***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 ▌ datasets ***catalogues*** established by the health data access bodies ***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*** 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 ***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 ***taking into account the specific conditions of different categories of stakeholders involved***. To support capacity building, the Commission shall ***in close cooperation and consultation with Member States establish indicators for self-assessment*** for the primary and secondary use of electronic health data.

Article 59a

Training and information for health professionals

1. Member States shall develop and implement or provide access to training programs for health professionals in order to understand and effectively exercise their role in the primary use of and access to electronic health data, including in relation to Articles 4, 7 and 9. The Commission shall support Member States in this regard.

2. The trainings and information shall be accessible and affordable to all health professionals, without prejudice to the organisation of healthcare at national level.

Article 59b

Digital health literacy and digital health access

1. Member States shall promote and support digital health literacy and relevant competences and skills for patients. The Commission shall support Member States in this regard.

2. Awareness raising campaigns or programmes shall aim in particular, to inform patients and the public at large about the primary and the secondary use of the electronic health data in the framework of the European Health Data Space, including of the rights arising from it, as well as advantages, risks and potential gains to science and society of the primary and secondary use of electronic health data.

3. The campaigns and programmes referred to in paragraph 2 shall be tailored to the needs

of specific groups and shall be developed and reviewed, and where necessary updated.

4. ***Member States shall promote the access to the infrastructure necessary for the effective management of natural persons' electronic health data, both within primary and secondary use.***

Article 60

Additional requirements for public procurement and Union funding

1. ***Within the meaning of Article 2(1)(1) of the Directive 2014/24/EU, contracting*** authorities, including digital health authorities and health data access bodies ▌ and ***Union institutions, bodies, offices or agencies,*** shall make reference to the applicable technical specifications, standards and profiles as referred to in Articles 6, ***12, 23, 50, 52, 56,*** 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 ***criteria*** for ***obtaining*** funding ***from the Union*** shall take into account the requirements developed in the framework of Chapters II, III and IV.

Article 60a

1. ***In accordance with the general principles of Union law, which include the fundamental rights guaranteed by Articles 7 and 8 of the Charter, Member States shall ensure a particular high level of protection and security when processing personal electronic health data for primary use, by means of appropriate technical and organisational measures. In this respect, this Regulation shall not preclude 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 Union, in compliance with Union law and international commitments.***

Article 60aa

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

1. Non-personal electronic ***health*** data made available by health data access bodies ***to a health data user in a third country according to a data permit pursuant to Article 46 or a data request pursuant to Article 47 or to authorised participants 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 ▌ shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation ***(EU) 2022/868***, provided that their transfer to third countries presents a risk of re-identification through means going beyond those ▌ 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 ▌ be detailed in the Delegated Act under the empowerment set out in Article 5(13) of Regulation ***EU) 2022/868.***

Article 62

International ***governmental*** access ***to*** non-personal electronic health data

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*** governmental access ***in a third country of non personal***

electronic health data held in the Union where such transfer ▌ would create a conflict with Union law or the national law of the relevant Member State ▌ .

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

Additional conditions for transfer of personal electronic health data ***to a third country or an international organisation***

Transfer of personal electronic health data ***to a third country or an international organisation, shall be granted in accordance with Chapter V of Regulation (EU) 2016/679*** Member States may maintain or introduce further conditions ***on international access to, and transfer of, personal electronic health data***, 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 Regulation (EU) 2016/679***.

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).

The Commission may adopt implementing acts establishing that a third country meets the criteria 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.

The Commission shall monitor developments in third countries and international organisations that could affect the functioning of implementing acts adopted pursuant to paragraph 2, and shall provide for a periodic review of the functioning of this Article.

Where the Commission considers that a third country no longer meets the requirement in point (b) of paragraph 1, it shall adopt an implementing act to remove such third country that benefits from access.

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 ***two*** representatives ***per*** Member ***State, one representative for primary use purposes and one for secondary use purposes, nominated by each Member State. Each Member State shall have one vote***. ***Members of the EHDS Board shall undertake to act in the public interest and in an independent manner***.

1a. A representative of the Commission and one of the representatives of the Member States referred to in paragraph 1 shall co-chair the meetings of the EHDS Board.

1b. Market surveillance authorities referred to in Article 28, the European Data Protection Board and the European Data Protection Supervisor EMA, ECDC, ENISA, shall be invited to attend the meetings, where the issues are of relevance according to the Board.

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.

1d. The Board may cooperate with other external experts as appropriate.

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 shall support the EHDS Board with specific expertise***. The subgroups may have joint meetings, as required.

3. ***The EHDS Board shall adopt rules of procedure and a code of conduct, following a proposal from the Commission. Those rules of procedure shall provide for*** the composition, organisation, functioning and cooperation of the ***subgroups, and the cooperation of the EHDS Board with the advisory forum. 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***.

▌

5. The EHDS Board shall cooperate with other relevant bodies, entities and experts, such as the European Data Innovation Board referred to in Article ***29*** of Regulation ***(EU) 2022/868***, competent bodies set up under Article ***37*** of Regulation ***(EU) 2023/2854***, supervisory bodies set up under Article 17 of Regulation ***(EU) 910/2014***, European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679***,*** cybersecurity bodies***, including ENISA, and the European Open Science Cloud, in the effort of reaching advanced solutions for the FAIR data usage in research and innovation***.

▌

7. The EHDS Board shall be assisted by a secretariat provided by the Commission.

7a. The EHDS Board shall publish meeting dates and minutes of the discussions and publish a biennial report on its activities.

8. The Commission shall, by means of implementing acts, adopt the necessary measures for the establishment ***and operations*** of the EHDS Board. Those implementing acts shall be adopted in accordance with the ***examination*** procedure referred to in Article 68(2).

Article 64a

Stakeholder forum

1. A Stakeholder Forum is hereby established for the purpose of facilitating the exchange of information and promoting cooperation with stakeholders in relation to the implementation of this Regulation.

2. The stakeholder forum shall be composed of relevant stakeholders, including representatives of patients' organisations, health professionals, industry, consumer

organisations, scientific researchers and academia. The advisory forum shall have a balanced composition and represent the views of different relevant stakeholders. Where commercial interests are represented in the advisory forum, they shall be balanced between large companies, SMEs and start-ups. Focus on primary and secondary use of electronic health data shall also be balanced.

3. Members of the stakeholder forum shall be appointed by the Commission following a public call for interest and a transparent selection procedure. Members of the advisory forum shall make an annual declaration of their interests, to be updated whenever relevant, which shall be made publicly available.

4. The stakeholder forum may establish standing or temporary subgroups as appropriate for the purpose of examining specific questions related to the objectives of this Regulation. The stakeholder forum shall draw up its rules of procedure.

5. The stakeholder forum shall hold regular meetings and a Commission representative shall chair the meetings.

6. The advisory forum shall prepare an annual report of its activities. That report shall be made publicly available.

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, ***taking into account the regional and local level,*** 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 ***biennial*** activity reporting ▌ and exchange of information;

(d) to share ***among the Members of the Board*** 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 ***advisory forum referred to in Article 64(a), as well as with*** 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;

(va) measures to protect the personal data of health professionals involved in the treatment of natural persons;

(vi) other aspects of the secondary use of electronic health data.

(ba) The EHDS Board shall, in consultation and cooperation with relevant stakeholders, including representatives of patients, health professionals and researchers, create guidelines in order to help health data users to fulfil their obligation under Article 41 paragraph 5, especially to determine whether their findings are clinically significant.

(c) to facilitate cooperation between health data access bodies through capacity-building, establishing the structure for ***biennial*** activity reporting, ▌ and exchange of information;

(d) to share information concerning risks and ▌ incidents related to secondary use of electronic health data, as well as their handling;

▌

(f) to facilitate the exchange of views on the secondary use of electronic health data with the ***advisory forum referred to in Article 64(a), as well as with*** health ***data holders, health data users***, regulators and policy makers in the health sector.

Article 66

The Steering Groups for ***the*** infrastructures ***MyHealth@EU and HealthData@EU***

1. ▌ Two ***Steering*** groups ***are hereby established*** for the cross-border infrastructures provided for in Articles 12 and 52***; the MyHealth@EU Steering group and the HealthData@EU Steering group. Each group*** shall be composed of ***one representative per Member State*** of the ***respective*** national contact points ▌ .

1a. The Steering groups shall take operational decisions concerning the development and operation of the cross-border infrastructures referred to in Articles 12 and 52.

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 ***Steering groups*** shall be set out in the rules of procedure adopted by those groups.

3. ***Other authorised participants may be invited to exchange information and views on***

relevant matters related to the cross-border infrastructures respectively provided for in Articles 12 and 52. When these participants are invited, they shall have an observer role.

3a. Stakeholders and relevant third parties, including patients', health professionals', consumers' and industry representatives, may be invited to attend meetings of the groups as observers.

4. The groups shall elect chairs for their meetings.

5. The groups shall be assisted by a secretariat provided by the Commission.

Article 66a

Roles and responsibilities of the Commission regarding the functioning of the European Health Data Space

1. 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.

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.

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 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(3);

(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).

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), ***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), ***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 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), ***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 ***5*** of Regulation (EU) No 182/2011 shall apply.

Article 68a

Horizontal complaints

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 a digital health authority where the complaint is related to the provisions in Chapter II, or with a health data access body where the complaint is related to the provisions of Chapter IV, provided that their rights or interests are negatively affected.

2. The digital health authority authorities or health data access body with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken on the complaint.

3. Digital health authority authorities and health data access bodies shall provide easily accessible tools to submit complaints.

4. Where the complaint concerns the rights of natural persons pursuant to Articles 8a to 8h or Article 35f of this Regulation, the complaint shall be transmitted to the competent supervisory authority under Regulation (EU) 2016/679. The digital health authority or health data access body shall provide the necessary information at its disposal to that supervisory authority under Regulation (EU) 2016/679 in order to facilitate the assessment and investigation of the complaint.

CHAPTER VIII

Miscellaneous

Article 69

Penalties

Member States shall lay down the rules on ***other*** penalties applicable to infringements of this Regulation ***in particular for infringements which are not subject to administrative fines pursuant to Article 43 and 43a,*** and shall take all measures necessary to ensure that they are implemented. The penalties shall be effective, proportionate and dissuasive. ▌

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.

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 69a

Right to receive compensation

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation, in accordance with national and Union law.

Article 69b

Representation of a natural person

Where a natural person considers that their rights under this Regulation have been infringed, they shall have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data, to lodge a complaint on their behalf or to exercise the rights referred to in Article 68a.

Article 70

Evaluation***,*** review ***and progress report***

1. After ***8*** years from the entry into force of this Regulation, the Commission shall carry out a targeted 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. The evaluation shall include ***the following:***

   (a) the possibilities to further extend interoperability between EHR systems and electronic health data access services other than those established by the Member States;

   (b) the need to update the data categories in Article 33 and the purposes of use in Article 34;

   (c) implementation and use by natural persons of the mechanisms to opt-out for secondary use referred to in Article 35f, notably on the impact on public health, scientific research and fundamental rights;

   (d) implementation and use of stricter measures referred to in Article 33(5);

   (e) the use and implementation of the right referred to in Article 3(9);

   (f) an assessment of the ***certification framework*** of EHR systems ***in Chapter III and*** the need to introduce ***further tools regarding*** conformity assessment ***and submit a report on its main findings;***

   (g) an assessment of the functioning of the Internal Market for the EHR systems;

(h) an assessment of the costs and benefits of implementation of the provisions for secondary use laid out in Chapter IV;

(i) as well as the application of fees as referred to in Article 42;

2. After ***10*** 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 ***or other appropriate measures***. ***This evaluation shall include an assessment of the efficiency and functioning of the systems providing for access to electronic health data for further processing, carried out on the basis of Union or national law referred to in Article 1(6a), with regard to their impact on the implementation of this Regulation.***

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 and 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 ***with effect from 6 years of entry into force of this Regulation***.

CHAPTER IX

Deferred application***, transitional*** and final provisions

Article 72

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall apply ***2 years*** after ▌ entry into force***, unless provided otherwise in paragraph 2***.

Articles ***2a, 5,*** 6, ***7a, 7b, 8a, 8b, 8c, 8d, 8e, 8f, 8g, 8h, 12(2), 12(3), 12(5), 12(6), 13a, 13b,*** 14, ▌ *31,* ***31a and 32 in Chapters II and III*** shall apply as follows:

(a) from ***4 years*** after date of entry into ***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 ***6*** years after date of entry into ***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 ***act*** pursuant to Article 5(2) for ***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 2 years 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 ***referred to in*** Article ***13b(2)*** from ***6*** years after date of entry into ***force***.

Chapter IV shall apply from 4 years after date of entry into force, except Article 33(1), points (b) (e), (ea) (j) and (l), which shall apply from 6 years after date of entry into force and article 52(5)

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	*For the Council*
The President	*The President*

Annex I

Main characteristics of ***priority categories of personal*** electronic health data ***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 ***including in an international classification coding*** 8. Textual information related to medical history 9. Medical devices and implants 10. ***Medical or care*** 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*** 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, ***they are*** suitable for ***their*** intended purpose and ***their*** use does not put at risk patient safety.

1.2. ***The harmonised components of the*** EHR system shall be designed and developed in such a way that ***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. ***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. ***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. ***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.***

2.3. An EHR system that includes a functionality for entering structured personal electronic health data shall enable the entry of data ***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 security ***and for logging***.

3.2. An EHR system designed to be used by health professionals shall provide reliable mechanisms for the identification and authentication of health professionals .

3.4. ***The harmonised logging component of*** an EHR system designed to enable access by health ***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 ***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.

3.6. ***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.

3.8. ***The harmonised components of*** an EHR system ***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.

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***.

5. References to any relevant ***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.