**EUROPEAN UNION**

**THE EUROPEAN PARLIAMENT** **THE COUNCIL**

**Brussels, 8 January 2025**
**(OR. en)**

**2022/0140(COD)** **PE-CONS 76/24**

**SAN 195**
**PHARM 48**
**COMPET 369**
**MI 360**
**DATAPROTECT 159**
**CODEC 905**

**LEGISLATIVE ACTS AND OTHER INSTRUMENTS**

| | |
|---|---|
| Subject: | REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 |

**REGULATION (EU) 2024/…**
**OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**of …**

**on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847**

**(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[3],

---

1 OJ C 486, 21.12.2022, p. 123.
2 OJ C 157, 3.5.2023, p. 64.
3 Position of the European Parliament of 24 April 2024 (not yet published in the Official Journal) and decision of the Council of …

Whereas:

(1) The aim of this Regulation is to establish the European Health Data Space (EHDS) in order to improve natural persons' access to and control over their personal electronic health data in the context of healthcare, as well as to better achieve other purposes involving the use of electronic health data in the healthcare and care sectors that would benefit society, such as research, innovation, policy-making, health threats preparedness and response, including preventing and addressing future pandemics, patient safety, personalised medicine, official statistics or regulatory activities. In addition, this Regulation's 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 will be a key element in the creation of a strong and resilient European Health Union.

(2) The COVID-19 pandemic 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 for secondary use of such electronic health data. Such timely access could 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 could help to save more lives. In 2020, the Commission urgently adapted its Clinical Patient Management System, established by Commission Implementing Decision (EU) 2019/1269[4], to allow Member States to share electronic health data of COVID-19 patients moving between healthcare providers and Member States during the peak of that pandemic. However, that adaptation was only an emergency solution, showing the need for a structural and consistent approach at Member State and Union level, both in order to improve the availability of electronic health data for healthcare and to facilitate access to electronic health data in order to steer effective policy responses and contribute to high standards of human health.

[4] 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).

(3) The COVID-19 crisis strongly cemented the work of the eHealth Network, a voluntary network of authorities responsible for digital health, as the main pillar for the development of contact-tracing and contact-warning applications for mobile devices 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 (the 'FAIR principles'), and ensuring that electronic health data are as open as possible, while respecting the data minimisation principle as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council[5]. Synergies between the EHDS, the European Open Science Cloud and the European Research Infrastructures should be ensured, and lessons should be learned from data-sharing solutions developed under the European COVID-19 Data Platform.

[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).

(4) Given the sensitivity of personal electronic 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 electronic health data of natural persons for primary use and secondary use as defined in this Regulation.

(5) The processing of personal electronic health data is subject to the provisions of Regulation (EU) 2016/679 and, for Union institutions, bodies, offices and agencies, of 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, bodies, offices and agencies, where relevant.

---

[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).

(6) More and more individuals living in the Union cross national borders to work, study, visit relatives, or for other reasons. To facilitate the exchange of health data, and in line with the need to empower 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 related to the provision of healthcare services, and which reveal information about their health status, personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, as well as data determinants of health, such as behaviour, environmental and physical influences, medical care, and social or educational factors. Electronic health data also include data that have been initially collected for research, statistical, health threat assessment, policy making or regulatory purposes and it should be possible to make them available in accordance with the rules laid down in this Regulation. Electronic health data consist of all categories of those data, irrespective of whether such data are provided by the data subject or other natural or legal persons, such as health professionals, or are 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 automated means.

(7) In health systems, personal electronic health data are usually gathered in electronic health records, which typically contain a natural person's medical history, diagnoses and treatment, medications, allergies and vaccinations, as well as radiology images, laboratory results and other medical data, spread between different actors in the health system, such as general practitioners, hospitals, pharmacies or care services. In order to allow electronic health data to be accessed, shared and modified by 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. In addition, some Member States provide support to public and private healthcare providers to set up personal electronic health data spaces to enable interoperability between different healthcare providers. Several Member States also support or provide electronic health data access services for patients and health professionals, for instance through patient or health professional portals. Those Member States have also taken measures to ensure that EHR systems or wellness applications are able to transmit electronic health data to the central EHR system, for instance by providing a system of certification. However, not all Member States have put in place such systems, and those Member States that have implemented them have done so in a fragmented manner. In order to facilitate the free movement of personal electronic health data across the Union and avoid negative consequences for patients when receiving healthcare in a cross-border context, Union action is needed to improve natural persons' access to their own personal electronic health data and to empower them to share those data. In this respect, appropriate action at Union and national level should be taken as a means of reducing fragmentation, heterogeneity and division, and to create 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 also benefit natural persons with limited ability to access and use digital services, including people with disabilities.

(8) 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 those rights and complements some of them as applied to personal electronic health data. Those rights apply regardless of the Member State in which the personal electronic health data are processed, type of healthcare provider, sources of those 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 this Regulation concern all categories of those data, irrespective of how they have been collected or who has provided them, 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 provided for in this Regulation 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.

(9) While the rights conferred by Regulation (EU) 2016/679 should continue to apply, the right of access to data by a natural person, established in Regulation (EU) 2016/679, should be further complemented in the healthcare sector. Under that Regulation, 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 that provides access. That situation slows down access to health data by natural persons, and can have a negative impact on them if they need such access immediately due to urgent circumstances pertaining to their health condition. It is therefore necessary to provide for 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 and immediate access, while respecting the need for technological practicability, to specific priority categories of personal electronic health data, such as the patient summary, through an electronic health data access service. That right should apply regardless of the Member State in which the personal electronic health data are processed, the type of healthcare provider, the sources of those data or the Member State of affiliation of the natural person. The scope of that complementary right established under this Regulation and the conditions for exercising it differ in certain ways from the right of access to personal data under Regulation (EU) 2016/679, which covers all personal data held by a controller and is exercised against an individual controller, which has up to one 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 entail an immediate answer. The rights under Regulation (EU) 2016/679 should continue to apply, allowing natural persons to benefit from their rights under both legal frameworks, in particular the right to obtain a paper copy of the electronic health data.

(10) It should be considered that immediate access of natural persons to certain categories of their personal electronic health data could be harmful for the safety of those natural persons or unethical. For example, it could be unethical to inform a patient through an electronic channel about a diagnosis of an incurable disease that is likely to be terminal instead of first providing that information in a consultation with the patient. Therefore, it should be possible to delay the provision of the access to personal electronic health data in such situations for a limited amount of time, for instance until the moment when the health professional can explain the situation to the patient. Member States should be able to establish such an exception where it constitutes a necessary and proportionate measure in a democratic society, in line with restrictions as provided for in Article 23 of Regulation (EU) 2016/679.

(11) 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 be made available in an electronic format prior to the application of this Regulation. This should not affect the obligation to make personal electronic health data, registered after the date of application of this Regulation, available in an electronic format.

(12) In order to complement the information available to them, natural persons should be able to add electronic health data to their EHRs or to store additional information in their separate personal health record which could be accessed by health professionals. However, information inserted by natural persons might 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 health professionals. Therefore, data added by natural persons in their EHR should be clearly distinguishable from data provided by health professionals. That possibility for natural persons to add and complement personal electronic health data should not entitle them to change personal electronic health data which have been provided by health professionals.

(13) Enabling natural persons to more easily and quickly access their personal electronic health data will enable them to notice possible errors such as incorrect information or incorrectly attributed patient records. In such cases, natural persons should be able to request online the rectification of the incorrect personal electronic health data, immediately and free of charge, through an electronic health data access service. Such rectification requests should then be treated by the relevant controllers in line with Regulation (EU) 2016/679, if necessary involving health professionals with a relevant specialisation and responsible for the natural persons' treatment.

(14) Under 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 that Regulation, natural persons have the right to have the personal data transmitted directly from one controller to another only where technically feasible. Regulation (EU) 2016/679, however, does not impose an obligation to make that direct transmission technically feasible. The right to data portability should be complemented under this Regulation, thereby empowering natural persons to provide access to, at least, priority categories of their personal electronic health data to the health professionals of their choice, to exchange such health data with such health professionals 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.

(15) 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 personal 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 application of the rights of natural persons, for example by refusing to take into account personal electronic health data originating from another Member State and which are provided through the interoperable and reliable European electronic health record exchange format.

(16) Access to electronic health records by healthcare providers or other individuals should be transparent to the natural persons concerned. Electronic health data access services should provide detailed information on access to data, such as when and which entity or natural person accessed data and which data were accessed. Natural persons should also be able to enable or disable automatic notifications regarding access to personal electronic health data relating to them through the health professional access services.

(17) Natural persons might not want to allow access to some parts of their personal electronic health data while enabling access to other parts. This could especially be relevant in cases of sensitive health issues such as those related to mental or sexual health, sensitive procedures such as abortions, or data on specific medication which could reveal other sensitive issues. Such selective sharing of personal electronic health data should therefore be supported and implemented through restrictions set by the natural person concerned in the same way within the territory of a given Member State and for cross-border data sharing. Those restrictions should allow for sufficient granularity to restrict parts of datasets, such as elements of the patient summaries. Before setting the restrictions, natural persons should be informed of the risks for patient safety associated with limiting access to health data. Given that the unavailability of the restricted personal electronic health data may impact the provision or quality of health services provided to the natural person, natural persons making use of such access restrictions should assume responsibility for the fact that the healthcare provider cannot take the data into account when providing health services. The restrictions on access to personal electronic health data could have life-threatening consequences and, therefore, access to those data should nevertheless be possible where necessary to protect vital interests in emergency situations. More specific legal provisions on the mechanisms of restrictions placed by natural persons on parts of their personal electronic health data could be provided for by Member States in their national law, in particular as regards medical liability in cases where restrictions have been placed by the natural person concerned.

(18) 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 opt out from access to their personal electronic health data by anyone other than the original controller, without any possibility to override that opt-out in emergency situations. In such a case, Member States should establish the rules and specific safeguards regarding such opt-out mechanisms. Those rules and specific safeguards could also relate to specific categories of personal electronic health data, for example genetic data. The right to opt out means that personal electronic health data relating to the natural person who exercises that right would not be made available through the services set up under the EHDS other than to the healthcare provider that provided the treatment. Member States should be able to require the registration and storage of personal electronic health data in an EHR system used by the healthcare provider who provided the health services and accessible only to that healthcare provider. If a natural person has exercised the right to opt out, healthcare providers will still document the treatment provided in accordance with applicable rules, and will be able to access the data registered by them. Natural persons who exercise the right to opt out should be able to reverse their decision. In such cases, personal electronic health data generated during the period of the opt-out might not be available via the access services and MyHealth@EU.

(19) Timely and full access by 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 both for health systems and for natural persons and can lead to worse health outcomes for natural persons. Electronic health data made available in an interoperable format and 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 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 priority categories are medically relevant in a specific episode of care, health professionals should have a wide access to data. When 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. In accordance with Regulation (EU) 2016/679, in order to limit their access to what is relevant in a specific episode of care, healthcare providers should follow the data minimisation principle when accessing personal electronic health data, limiting the data accessed to data that are strictly necessary and justified for a given service.

Providing health professional access services is a task assigned in the public interest by this Regulation and the performance of such task requires the processing of personal data as referred to in Article 6(1), point (e), of Regulation (EU) 2016/679. This Regulation provides for conditions and safeguards for the processing of electronic health data by the health professional access service in accordance with Article 9(2), point (h), of Regulation (EU) 2016/679, for instance detailed provisions regarding logging of access to personal electronic health data and that aim to provide transparency towards data subjects. However, this Regulation should be without prejudice to national law concerning the processing of health data for the delivery of healthcare, including national law establishing categories of health professionals that can process different categories of electronic health data.

(20) 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. Those services could be provided at national, regional or local level, or by healthcare providers, in the form of an online patient portal, an application for mobile devices or by other means. They should be designed in an accessible way, in particular for persons with disabilities. Providing such a service to enable natural persons to have easy access to their personal electronic health data is a substantial public interest. The processing of personal electronic health data through those services is necessary for the performance of that task assigned by this Regulation in the sense of Article 6(1), point (e), and Article 9(2), point (g), of Regulation (EU) 2016/679. This Regulation lays down the necessary conditions and safeguards for the processing of electronic health data in electronic health data access services, such as electronic identification of natural persons accessing such services.

(21) Natural persons should be able to provide an authorisation to other natural persons of their choice, such as their relatives or other close natural persons, enabling such persons of their choice to access or control the access to the personal electronic health data of the natural persons who provide the authorisation or to use digital health services on their behalf. Such authorisations could also be convenient for other usage by natural persons provided with such an authorisation. Proxy services for enabling and implementing such authorisations should be established by Member States, and be linked to personal electronic health data access services, such as patient portals or patient-facing applications for mobile devices. Those proxy services should also enable guardians to act on behalf of their dependents, including minors; in such situations, authorisations could be automatic. In addition to those proxy services, Member States should also establish easily accessible support services to be provided by adequately trained staff dedicated to assisting natural persons when exercising their rights. In order to take into account cases in which the display of some personal electronic health data of dependent persons to their guardians could be contrary to the interests or the will of their dependents, including minors, Member States should be able to provide in national law for limitations and safeguards as well as for mechanisms for their technical implementation. Personal electronic health data access services, such as patient portals or patient-facing applications for mobile devices, should make use of such authorisations and thus enable authorised natural persons to access personal electronic health data falling within the scope of the authorisation. In order to provide a horizontal solution with increased user-friendliness, digital proxy solutions should be aligned with Regulation (EU) No 910/2014 of the European Parliament and of the Council[7] and the technical specifications of the European Digital Identity Wallet. That alignment would contribute to reducing both the administrative and financial burden for Member States by lowering the risk of developing parallel systems that are not interoperable across the Union.

---

[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).

(22) In some Member States, healthcare is provided by primary care management teams, which are groups of health professionals focused on primary care, such as general practitioners, that carry out their primary care activities based on a healthcare plan that they draw up. Other types of healthcare teams also exist in several Member States for other care purposes. In the context of primary use in the EHDS, access should be provided to the health professionals belonging to such teams.

(23) The supervisory authorities established pursuant to Regulation (EU) 2016/679 are competent for monitoring and enforcing the application of that Regulation, in particular for the monitoring of the processing of personal electronic health data and for handling any complaints lodged by the natural persons concerned. This Regulation establishes additional rights for natural persons regarding primary use, which go beyond and complement access and portability rights enshrined in Regulation (EU) 2016/679. Since those additional rights should also be enforced by the supervisory authorities established pursuant to Regulation (EU) 2016/679, Member States should ensure that those supervisory authorities are provided with the financial and human resources, premises and infrastructure necessary for the effective performance of those additional tasks. The supervisory authority or authorities responsible for the monitoring and enforcement of the processing of personal electronic health data for primary use in compliance with this 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.

(24) Member States ought to 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 the importance of ethical principles, the European ethical principles for digital health provide guidance to practitioners, researchers, innovators, policy-makers and regulators.

(25) The relevance of different categories of electronic health data for different healthcare scenarios varies. Different categories have also achieved different levels of maturity as regards 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 certain categories of electronic health data is needed. Categories of electronic health data such as patient summaries, electronic prescriptions and dispensations, medical imaging studies and related imaging reports, medical test results such as laboratory results and related reports, and discharge 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 categories of data represent groups of electronic health data, this Regulation should apply to both the groups as a whole and to the individual data entries included in those groups. For example, given that vaccination status is part of a patient summary, the rights and requirements linked to the patient summary should also apply to such vaccination status even if it is processed separately from the patient summary as a whole. When further needs for the exchange of additional categories of electronic health data are identified for healthcare purposes, access to and exchange of those additional categories should be possible under this Regulation. The additional categories should be first implemented at Member State level and the exchange on a voluntary basis of such categories of data in cross-border situations between the cooperating Member States should be provided for in this Regulation. Particular attention should be given to 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.

(26) 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 and to control better the access to and sharing of 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 Decision (EU) 2022/2481 of the European Parliament and of the Council[8]. 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 imaging studies and related imaging reports, medical test results and discharge reports, subject to transition periods. Where personal electronic health data are made available to a healthcare provider or a pharmacy by a natural person, or are transmitted by another controller in the European electronic health record exchange format, that format should be accepted, and the recipient should be able to read the data and use them for the provision of healthcare or for dispensation of a medicinal product, thus supporting the provision of the healthcare services or the dispensation of the electronic prescription. The European electronic health record exchange format ought to be designed in a way that facilitates translation of electronic health data communicated using that format into the official languages of the Union, to the extent possible. Commission Recommendation (EU) 2019/243[9] provides the foundations for such a common European electronic health record exchange format. The interoperability of the EHDS should contribute to having European health datasets of a high quality. The use of a European electronic health record exchange format should become more widespread at Union and national level. The European electronic health record exchange format could allow for different profiles for its use at the level of EHR systems and at the level of the national contact points for digital health in MyHealth@EU for cross-border data exchange.

---

[8] 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).

[9] 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).

(27) While EHR systems are widespread, 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 application 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 in accordance with 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.

(28) Telemedicine is becoming an increasingly important tool that can provide patients with access to care and tackle inequities. It 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 the regulation of activities such as online pharmacies, telemedicine and other services that they provide and provide reimbursement for, 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, for example telemedicine and online pharmacy services.

(29) Regulation (EU) No 910/2014 lays down the conditions under which Member 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 secure access to electronic health data, including in cross-border situations. Electronic health data access services and telemedicine services should enable natural persons to exercise their rights regardless of their Member State of affiliation, and should therefore support the identification of natural persons using any electronic identification means recognised pursuant to Regulation (EU) No 910/2014. Given the possibility of challenges regarding identity matching in cross-border situations, it might be necessary for Member States of treatment to provide complementary access mechanisms such as tokens or codes to natural persons who arrive from other Member States and receive healthcare. The Commission should be empowered to adopt implementing acts to determine the requirements for the interoperable and cross-border identification and authentication of natural persons and health professionals, including any complementary mechanisms that are necessary to ensure that natural persons can exercise their rights related to personal electronic health data in cross-border situations.

(30) Member States should designate relevant digital health authorities for the planning and implementation of standards for access to and transmission of electronic health data and the enforcement of the rights of natural persons and health professionals, as separate organisations or as part of already existing authorities. The digital health authority staff should not have any financial or other interests in industries or economic activities which could affect their impartiality. Digital health authorities already exist in most of the Member States and they deal with EHRs, interoperability, security or standardisation. When carrying out their tasks, digital health authorities should cooperate in particular with the supervisory authorities established pursuant to Regulation (EU) 2016/679 and supervisory bodies established pursuant to Regulation (EU) No 910/2014. Digital health authorities can also cooperate with the European Artificial Intelligence Board established by Regulation (EU) 2024/1689 of the European Parliament and of the Council[10], the Medical Device Coordination Group established by Regulation (EU) 2017/745 of the European Parliament and of the Council[11], the European Data Innovation Board established pursuant to Regulation (EU) 2022/868 of the European Parliament and of the Council[12] and the competent authorities under Regulation (EU) 2023/2854 of the European Parliament and of the Council[13].

---

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

[11] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

[12] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1).

[13] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

Member States should facilitate the participation of national actors in the cooperation at Union level, the conveying of expertise and the provision of advice on the design of solutions necessary to achieve the goals of the EHDS.

(31) Without prejudice to any other administrative or non-judicial remedy, any 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 or 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.

(32) Digital health authorities should have sufficient technical skills, possibly by 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 the necessary measures to protect the rights of natural persons by setting up national, regional, and local technical solutions such as national EHR intermediation solutions and patient portals. When taking such necessary protective measures, digital health authorities should apply common standards and specifications in such solutions, promote the application of the standards and specifications in procurement procedures 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 taken. In particular, health professionals should be informed and trained with regard to their rights and obligations under this Regulation. To carry out their tasks, the digital health authorities should cooperate at Union and national level with other entities, including with insurance bodies, healthcare providers, health professionals, manufacturers of EHR systems and of wellness applications, as well as other stakeholders from the 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.

(33) Access to and transmission of electronic health data is relevant in cross-border healthcare situations, as it can 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 who cross the border frequently to get healthcare. In many border regions, some specialised healthcare services might be available closer across the border than in the same Member State. 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 such infrastructure and its funding should be considered. A voluntary infrastructure for that purpose, MyHealth@EU, was established as part of the actions to achieve the objectives set up in Directive 2011/24/EU of the European Parliament and of the Council[14]. Through MyHealth@EU, Member States started to provide natural persons with the possibility of sharing their personal electronic health data with healthcare providers when travelling abroad. Building on that experience, the participation of Member States in MyHealth@EU as established by this Regulation should be mandatory. Technical specifications for MyHealth@EU 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. Those 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. Member States should be required to join MyHealth@EU, comply with its technical specifications and connect healthcare providers, including pharmacies, to it, as this is necessary for enabling natural persons to exercise their rights under this Regulation to access and make use of their personal electronic health data regardless of the Member State where the natural persons are located.

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

(34) 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 the transmission of personal electronic health data through it. Member States are responsible for the organisation of their national contact points for digital health and for the processing of personal data for the purposes of the delivery of healthcare, before and after the transmission of those data through MyHealth@EU. The Commission should monitor through compliance checks the compliance of national contact points for digital health with the necessary requirements regarding the technical development of MyHealth@EU as well as with detailed rules concerning the security, confidentiality and protection of personal electronic health data. In the event of serious non-compliance by a national contact point for digital health, the Commission should be able to suspend the services affected by the non-compliance provided by that national contact point for digital health. The Commission should act as a processor on behalf of the Member States within MyHealth@EU 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 specified by means of implementing acts. Each Member State is solely responsible for data and services in that Member State. This Regulation provides the legal basis for the processing of personal electronic health data in MyHealth@EU as a task carried out in the public interest assigned by Union law referred to in Article 6(1), point (e), of Regulation (EU) 2016/679. That processing is necessary for the provision of healthcare in cross-border situations, as mentioned in Article 9(2), point (h), of that Regulation.

(35) 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 could 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. Such additional use cases would also be 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 national contact points for digital health of relevant third countries and systems established at international level by international organisations in order to contribute to the continuity of healthcare. This is particularly relevant for individuals travelling to and from neighbouring third countries, candidate countries, and the associated overseas countries and territories. The connection of such national contact points for digital health of third countries to MyHealth@EU and the interoperability with digital systems established at international level by international organisations should be subject to a check ensuring the compliance of those contact points and digital systems with the technical specifications, data protection rules and other requirements of MyHealth@EU. In addition, given that the 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 under Chapter V of Regulation (EU) 2016/679 should be put in place. The Commission should be empowered to adopt implementing acts to facilitate the connection of such national contact points for digital health of third countries and systems established at international level by international organisations to MyHealth@EU. When preparing those implementing acts, the Commission should take into account Member States' national security interests.

(36) In order to enable the seamless exchange of electronic health data and ensure respect for the rights of natural persons and health professionals, EHR systems marketed in the internal market 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 conformity self-assessment scheme 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 the 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 software components harmonised by this Regulation, namely the European interoperability software component for EHR systems and the European logging software component for EHR systems (the 'harmonised software components of EHR systems'). The harmonised software components of EHR systems mainly concern data transformation, although they may imply the need for indirect requirements for data registration and data presentation in EHR systems. Technical specifications for the harmonised software components of 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. The harmonised software components of EHR systems should be designed to be reusable and to integrate seamlessly with other components within a larger software system.

The security requirements of the harmonised software components of EHR systems should cover elements specific to EHR systems, as more general security properties should be supported by other mechanisms such as those under Regulation (EU) 2024/2847 of the European Parliament and of the Council[15]. To support that process, European digital testing environments should be set up to provide automated means to test whether the functioning of the harmonised software components of an EHR system is compliant with the requirements laid down in this Regulation. To that end, implementing powers should be conferred on the Commission to determine the common specifications for those environments. The Commission should develop the necessary software for the testing environments and make it available as open source. Member States should be responsible for the operation of the digital testing environments, as they are closer to manufacturers and better placed to support them. Manufacturers should use those digital testing 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 the comparability of EHR systems, the Commission should prepare a uniform template for the technical documentation accompanying such systems.

---

[15] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(37) EHR systems should be accompanied by an information sheet that includes information for its professional users and by clear and complete instructions for use, including in accessible formats for persons with disabilities. If an EHR system is not accompanied by such information, 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.

(38) 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 to be an EHR system, even when used in a healthcare setting, and should therefore not be required to comply with this Regulation. That covers cases such as text-processing software used for writing reports that would then become part of written electronic health records, general-purpose middleware, or database management software that is used as part of data storage solutions.

(39) This Regulation imposes a mandatory conformity self-assessment scheme for the harmonised software 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. That mandatory conformity self-assessment, which would be in the form of an EU declaration of conformity by the manufacturer, should ensure that those requirements are fulfilled in a proportionate way, while avoiding an undue burden on Member States and manufacturers.

(40) Manufacturers should affix in the accompanying documents of the EHR system, and where applicable on its packaging, a CE marking of conformity indicating that the EHR system is in conformity with this Regulation and, in respect of aspects not covered by this Regulation, with other applicable Union law which also requires the affixing of such marking. Member States should build upon existing mechanisms to ensure the correct application of the provisions on the CE marking of conformity under relevant Union law and should take appropriate action in the event of improper use of that marking.

(41) Member States should remain competent to define requirements relating to any other software components of EHR systems and the terms and conditions for connection of healthcare providers to their respective national infrastructures, which could be subject to third-party assessment at national level. In order to facilitate the smooth functioning of the internal market for EHR systems, digital health products and associated services, it is necessary to ensure as much as possible transparency as regards national law establishing requirements for EHR systems and provisions on their conformity assessment in relation to aspects other than the harmonised software components of EHR systems. Therefore, Member States should inform the Commission of those national requirements so it has the necessary information to ensure that they do not adversely affect the harmonised software components of EHR systems.

(42) Certain software components of EHR systems could be considered medical devices under Regulation (EU) 2017/745 or in vitro diagnostic medical devices under Regulation (EU) 2017/746 of the European Parliament and of the Council[16]. Software or modules of software which fall within the definition of a medical device, in vitro diagnostic medical devices or an artificial intelligence (AI) system considered to be high-risk (the 'high-risk AI system') should be certified in accordance with Regulations (EU) 2017/745, (EU) 2017/746 and (EU) 2024/1689, as applicable. While such products are required to fulfil the requirements under the respective Regulation governing those products, 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, an in vitro diagnostic medical device, or a 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 medical devices, in vitro diagnostic medical devices and high-risk AI systems.

[16] 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).

(43) To further support interoperability and security, Member States should be able to maintain or define specific rules for the procurement, reimbursement or financing 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 procurement procedures organised by healthcare providers and national or regional authorities. The mandatory certification of EHR systems at Union level should establish a baseline that can be used in procurement procedures at national level.

(44) In order to guarantee the effective exercise by patients of their rights under this Regulation, healthcare providers developing and using an EHR system 'in-house' to carry out internal activities without placing it on the market in return for payment or remuneration should also comply with this Regulation. In that context, such healthcare providers should comply with all requirements applicable to manufacturers as regards such EHR systems that are developed 'in-house' and that such healthcare providers put into service. However, given that the healthcare providers may need additional time to prepare for compliance with this Regulation, those requirements should only apply to such systems after an extended transitional period.

(45) It is necessary to provide for a clear and proportionate distribution of obligations corresponding to the role of each economic 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.

(46) 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, standards, specifications and profiles for data exchange, as well as requirements and principles related to patient safety and the security, confidentiality, integrity and protection of personal data, and 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, those common specifications should be based on existing harmonised standards for the harmonised software components of EHR systems and be compatible with sectoral law. Where common specifications have a particular importance in relation to personal data protection requirements concerning 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.

(47) In order to ensure there is appropriate and effective enforcement of the requirements and obligations laid down in this Regulation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 of the European Parliament and of the Council[17] 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 of this Regulation or a separate market surveillance authority responsible for EHR systems. While designating digital health authorities as market surveillance authorities could have significant practical advantages for the implementation of health and care, any conflicts of interest should be avoided, for instance by separating different tasks.

(48) The 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 could, 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 conflicts of interest.

---

[17] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

(49) Users of wellness applications, including applications for mobile devices, 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 are 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 also be informed about the compliance of such wellness 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 for which interoperability with EHR systems is claimed should therefore be established as an appropriate mechanism for providing transparency for the users of wellness applications regarding compliance with requirements under this Regulation, thereby supporting users in their choice of appropriate wellness applications with high standards of interoperability and security. The Commission should set out by means of implementing acts the details regarding the format and content of such label.

(50) Member States should remain free to regulate other aspects of the use of wellness applications, provided that the corresponding rules are in compliance with Union law.

(51) 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 do not fall within the scope of Regulations (EU) 2017/745 and (EU) 2024/1689, 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 for registration of 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 (EU) 2024/1689, but the compliance with interoperability requirements should be indicated by manufacturers when they claim such compliance, in order to provide information to procurers.

(52) Without hindering or replacing contractual arrangements 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 that mechanism, health data holders should make the data they hold available on the basis of a data permit or a health data request. For the purpose of processing electronic health data for secondary use, one of the legal bases referred to in Article 6(1), points (a), (c), (e) or (f), of Regulation (EU) 2016/679 in conjunction with Article 9(2) thereof is required. Accordingly, this Regulation provides for a legal basis for the secondary use of personal electronic health data, including the safeguards required under Article 9(2), points (g) to (j), of Regulation (EU) 2016/679 to allow the processing of special categories of data, 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 processing environment, as well as arrangements for data processing, set out in the data permit. Consequently, Member States should no longer be able to 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, with the exception of the introduction of stricter measures and additional safeguards at national level aimed at safeguarding the sensitivity and value of certain data as laid down in this Regulation. Health data applicants should also demonstrate a legal basis referred to in Article 6 of Regulation (EU) 2016/679 that allows them to request access to electronic health data pursuant to this Regulation and should fulfil the conditions set out in Chapter IV thereof.

In addition, the health data access body should assess the information provided by the health data applicant, based on which it 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. For processing of electronic health data held by the health data holders, this Regulation creates the legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679, in accordance with Article 9(2), points (i) and (j), of that Regulation, for the health data holder to make available the personal electronic health data to health data access bodies, while the legal basis for the purpose of the initial processing, for example the delivery of healthcare, is unaffected. This Regulation also assigns tasks in the public interest within the meaning 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) to (j), as applicable, of that Regulation. If the health data user relies upon a legal basis set out in Article 6(1), point (e) or (f), of Regulation (EU) 2016/679, this Regulation should provide for the safeguards required under Article 9(2) of Regulation (EU) 2016/679.

(53) Electronic health data used for secondary use 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 that goal, it is important that datasets made available for secondary use pursuant to this Regulation be as complete as possible. This Regulation provides the necessary safeguards to mitigate certain risks involved in the achievement 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.

(54) To balance the need of health data users to have exhaustive and representative datasets with the need for autonomy of natural persons over personal electronic health data of theirs that are considered particularly sensitive, natural persons should be able to make the decision as to whether their personal electronic health data can be processed for secondary use under this Regulation, in the form of a right to opt out from having those data being made available for secondary use. An easily understandable and accessible user-friendly mechanism to exercise that right to opt out should be provided for. 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 entailed by exercising that 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, taking into account their national context, mechanisms to provide access to personal electronic health data of natural persons who have exercised their 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. The 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 the public interest in relation to legitimate scientific and societal objectives.

Such overrides should only be available to health data users that are public sector bodies, or relevant Union institutions, bodies, offices or agencies, entrusted with the performance of tasks in the area of public health, or to another entity entrusted with the performance of public tasks in the area of public health or acting on behalf of or commissioned by a public authority, and only where the data cannot be obtained by alternative means in a timely and effective manner. Those health data users should justify that the use of the override is necessary for an individual health data access application or health data request. When such an override is applied, the safeguards under Chapter IV should continue to be applied by health data users, in particular the prohibition of re-identification or attempting to re-identify the natural persons concerned.

(55) In the context of the EHDS, electronic health data already exist and are being collected by, among others, healthcare providers, professional associations, public institutions, regulators, researchers and insurers in the course of their activities. Those data should also be made available for secondary use, that is to say for processing of data for purposes other than those for which they were collected or produced, however, many of such data are not made available for processing for such purposes. 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 exploit the benefits of secondary use, 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.

(56) 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, for example electronic health records, claims data, dispensation data, data from disease registries or genomic data, as well as data with an impact on health, for example data on consumption of different substances, socio-economic status or behaviour, and data on environmental factors such as pollution, radiation or the use of certain chemical substances. The categories of electronic health data for secondary use include some categories of data that were initially collected for other purposes such as research, statistics, patient safety, regulatory activities or policy making, for example, policy-making registries or registries concerning the side effects of medicinal products or medical devices. European databases that facilitate use or reuse of data are available in some areas, such as cancer (the European Cancer Information System) or rare diseases (for example, the European Platform on Rare Disease Registration and European reference networks (ERN) registries). The categories of electronic health data that can be processed for secondary use should also include automatically generated data from medical devices and person-generated data, such as data from wellness applications. Data on clinical trials and clinical investigations should also be included in the categories of electronic health data for secondary use when the clinical trial or clinical investigation has ended, without affecting any voluntary data sharing by the sponsors of ongoing trials and investigations. Electronic health data for secondary use should be made available preferably in a structured electronic format that facilitates their processing by computer systems. Examples of structured electronic formats include records in a relational database, XML documents or CSV files and free text, audios, videos and images provided as computer-readable files.

(57) Health data users who benefit from access to datasets provided for under this Regulation could enrich the data in those datasets with various corrections, annotations and other improvements, for instance by supplementing missing or incomplete data, thus improving the accuracy, completeness or quality of the data in the datasets. Health data users should be encouraged to report critical errors in datasets to health data access bodies. To support the improvement of the initial database and further use of the enriched dataset, Member States should be able to establish rules for the processing and the use of electronic health data containing improvements related to the processing of those data. The improved dataset should be made available free of charge to the original health data holder together with a description of the improvements. The health data holder should make the new dataset available, unless it provides a justified notification to the health data access body for not doing so, for instance in cases in which the enrichment by the health data user is of low quality. It should be ensured that non-personal electronic health data are available for secondary use. In particular, pathogen genomic data hold significant value for human health, as shown during the COVID-19 pandemic during which timely access to and sharing of such data proved to be essential for the rapid development of detection tools, medical countermeasures and responses to public health threats. The greatest benefit from pathogen genomics efforts will be achieved when public health and research processes share datasets and cooperate to inform and improve each other.

(58) 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 such 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 implementation of the EHDS and further dataset improvements should be conducted in a manner that prioritises the datasets that are the most suitable for creating such value and quality.

(59) Public or private entities often receive public funding from national or Union funds to collect and process electronic health data for research, official or unofficial statistics, or other similar purposes, including in areas where the collection of such data is fragmented or difficult, such as in relation to rare diseases or cancer. 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, benefiting 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 should therefore be entities that are healthcare providers or care providers or carry out research with regard to the healthcare or care sectors, or develop products or services intended for the healthcare or care sectors. Such entities can be public, not for profit or private. In line with this definition, nursing homes, day-care centres, entities providing services for people with disabilities, entities carrying out 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 considered health data holders. Union institutions, bodies, offices or agencies that process those categories of health and healthcare data as well as mortality registries should also be considered health data holders.

In order to avoid a disproportionate burden for natural persons and microenterprises, they should be, as a general rule, exempted from the obligations on health data holders. Member States should, however, be able to extend the obligations of health data holders to natural persons and microenterprises in their national law. To reduce the administrative burden, and in light of the effectiveness and efficiency principles, Member States should be able to require in their national law that health data intermediation entities carry out the duties of certain categories of health data holders. Such health data intermediation entities should be legal persons able to process, make available, register, provide, restrict access to, and exchange electronic health data for secondary use provided by health data holders. Such health data intermediation entities perform tasks that differ from those of data intermediation services under Regulation (EU) 2022/868.

(60) 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, it is important to encourage the sharing of clinical trials and clinical investigations data through the EHDS for secondary use. Clinical trials and clinical investigations data should be made available to the extent possible, while taking all necessary measures to protect intellectual property rights and trade secrets. 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, including for clinical trials and clinical investigations data. Health data access bodies should assess how to preserve such protection while enabling access to such data for health data users to the extent possible. If a health data access body is unable to provide access to such data, it should inform the health data user and explain why it is not possible to provide such access. Legal, organisational and technical measures to protect intellectual property rights or trade secrets could include common electronic health data access contractual arrangements, specific obligations within the data permit in relation to such rights, pre-processing the data to generate derived data that protect a trade secret but nonetheless have a utility for the health data user or configuration of the secure processing environment so that such data are not accessible to the health data user.

(61) The secondary use of health data under the EHDS should enable public, private and 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 as set out in this Regulation. Access to data for secondary use should contribute to the general interest of society. In particular, the secondary use of health data for research and development purposes should contribute to benefiting society in the form of new medicines, medical devices, and healthcare 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 could include using the electronic health data for tasks carried out by public sector bodies, such as the exercise of public duty, including public health surveillance, planning and reporting duties, health policy making, and ensuring patient safety, quality of care and the sustainability of healthcare systems. Public sector bodies and Union institutions, bodies, offices and agencies might need to have regular access to electronic health data for an extended period of time, including in order to fulfil their mandate, as is provided for in this Regulation. Public sector bodies could carry out such research activities by using third parties, including sub-contractors, as long as the public sector body remains at all time the supervisor of those 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 technological development and demonstration, fundamental research, applied research and privately funded research.

Activities related to scientific research include innovation activities such as training of AI algorithms that could be used in healthcare or the care of natural persons, as well as the evaluation and further development of existing algorithms and products for such purposes. It is necessary that the EHDS also contribute to fundamental research, and, although its benefits to end-users and patients might be less direct, such fundamental 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 contribute to the diagnosis or treatment of other natural persons. There is a need for public sector bodies to go beyond the scope of 'exceptional need' of Chapter V of Regulation (EU) 2023/2854. However, health data access bodies should be allowed to provide support to public sector bodies when processing or linking data. This Regulation provides for a channel for public sector bodies to obtain access to information that they require for fulfilling the tasks assigned to them by law, but does not extend the mandate of such public sector bodies.

(62) Any attempt to use electronic health data for measures detrimental to natural persons, such as to increase insurance premiums, to engage in activities potentially detrimental to natural persons related to employment, pensions or banking, including mortgaging of properties, to advertise products or treatments, to automate individual decision-making, to re-identify natural persons or to develop harmful products should be prohibited. That prohibition should also apply to activities contrary to ethical provisions under national law, with the exception of ethical provisions relating to consent to the processing of personal data and ethical provisions relating to the right to opt out, since this Regulation takes precedence over national law in accordance with the general principle of the primacy of Union law. It should also be prohibited to provide access to, or otherwise make available, 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 pursuant to this Regulation to access 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.

(63) This Regulation does not create an empowerment for the secondary use of health data for the purpose of law enforcement. The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties by the 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 health data users for 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. Moreover, the powers of the competent authorities for the prevention, investigation, detection and prosecution of criminal offences established by law to obtain electronic health data are unaffected by this Regulation. Likewise, electronic health data held by courts for the purpose of judicial proceedings are outside the scope of this Regulation.

(64) The establishment of one or more health data access bodies, supporting access to electronic health data in Member States, is essential to promoting the secondary use of health-related data. Member States should therefore establish one or more health data access bodies to reflect, inter alia, their constitutional, organisational and administrative structure. However, one of those health data access bodies should be designated as a coordinator in the event there is more than one health data access body. Where a Member State establishes several health data access bodies, it should lay down rules at national level to ensure the coordinated participation of those bodies in the European Health Data Space Board (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 could vary in terms of organisation and size, spanning from a dedicated fully fledged organisation to a unit or department in an existing organisation. Health data access bodies should not be influenced in their decisions on access to electronic data for secondary use and should avoid any conflicts of interest. Therefore, members of the governance and decision-making bodies of each health data access body and its staff should refrain from any action that is incompatible with their duties and should not engage in any incompatible occupation.

However, the independence of the health data access bodies should not mean that they cannot be subject to control or monitoring mechanisms regarding their 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. The members of the governance and decision-making bodies of health data access bodies and their staff should have the necessary qualifications, experience and skills. Each health data access body should have a separate public annual budget, which could 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.

(65) 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, health data access bodies should cooperate with each other and with the Commission. Health data access bodies should also cooperate with stakeholders, including patient organisations. Health data access bodies should support health data holders that are small enterprises in accordance with Commission Recommendation 2003/361/EC[18], 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 Regulations (EU) 2016/679 and (EU) 2018/1725 apply and the supervisory authorities under those Regulations should remain the only authorities competent for enforcing those provisions. Health data access bodies should inform the data protection authorities of any penalties imposed and any potential issues related to 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 are 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 for the health data user as required under 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 pseudonymisation and anonymisation of micro datasets. When relevant, the Commission should set out the procedures and requirements, and provide technical tools, for a unified procedure for pseudonymising and anonymising electronic health data.

---

[18] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

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

(67) Natural persons should be informed by the health data holders about significant findings related to their health made 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 on the arrangements for the provision by the health data holders of such information to the natural persons concerned and on the exercise of the right not to be informed. Member States should be able, in accordance with Article 23(1), point (i), of Regulation (EU) 2016/679, to restrict the scope of the obligation to inform 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 concerned information that potentially can have an impact on their health.

(68) In order to promote transparency, health data access bodies should also publish activity reports, every two years, 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 every two years. Activity reports should follow a structure agreed by the EHDS Board and provide an overview of activities, including information regarding decisions on applications, audits and engagement with relevant stakeholders. Such stakeholders can include representatives of natural persons, patient organisations, health professionals, researchers and ethical committees.

(69) In order to support secondary use, health data holders should refrain from withholding the data, requesting unjustified fees that are not transparent or proportionate to the costs of making the data available or, where relevant, to marginal costs of data collection, requesting the health data users to co-publish the research or other practices that could dissuade the health 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, the evaluation related to ethical approval should be based on its own merits.

(70) Health data access bodies should be allowed to charge fees, taking into account the horizontal rules provided by Regulation (EU) 2022/868, in relation to their tasks. Such fees could take into account the situation and interest of small and medium-sized enterprises (SMEs), individual researchers or public sector bodies. In particular, Member States should be able to establish measures for health data access bodies in their jurisdiction which make it possible to charge certain categories of health data users reduced fees. Health data access bodies should be able to cover the costs of their operations with fees set up in a proportionate, justified and transparent manner. This could result in higher fees for some health data users, if handling their health data access applications and health data requests requires more work. Health data holders should be allowed to also ask for fees for making data available, which reflect their costs. Health data access bodies should decide on the amount of such fees, which could also include the fees requested by health data holders. The health data user ought to be charged such fees by the health data access body in a single invoice. The health data access body should then transfer the relevant part of the paid fees to the health data holder. In order to ensure a harmonised approach concerning fee policies and structure, implementing powers should be conferred on the Commission. Article 10 of Regulation (EU) 2023/2854 should apply to fees charged under this Regulation.

(71) In order to strengthen the enforcement of the rules on secondary use, appropriate measures that can lead to administrative fines or enforcement measures by health data access bodies or temporary or definitive exclusions from the EHDS framework of health data users or health data holders that do not comply with their obligations should be envisaged. Health data access bodies should be empowered to verify compliance of health data users and health data holders and give them the opportunity to reply to any findings and to remedy any infringement. When deciding on the amount of the administrative fine or on an enforcement measure for each individual case, health data access bodies should take into account the cost margins and the criteria set out in this Regulation, ensuring that those fines or measures are proportionate.

(72) Given the sensitivity of electronic health data, it is necessary to reduce risks for the privacy of natural persons by applying the data minimisation principle. Therefore, non-personal electronic health data should be made available in all cases where the provision of such data is sufficient. If the health data user needs to use personal electronic health data, it should clearly indicate in its request the justification for the use of that type of data and the health data access body should assess whether that justification is valid. The personal electronic health data should only be made available in pseudonymised format. Taking into account the specific purposes of the processing, personal electronic health data should be pseudonymised or anonymised as early as possible in the process of making data available for secondary use. It should be possible for pseudonymisation and anonymisation to be carried out by health data access bodies or by health data holders. As controllers, health data access bodies and health data holders should be allowed to delegate those tasks to processors. When providing access to a pseudonymised or anonymised dataset, a health data access body should use state-of-the-art pseudonymisation or anonymisation 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 pseudonymisation or anonymisation should be further developed. Health data users should not attempt to re-identify natural persons from the dataset provided under this Regulation, and where they do so they should be subject to administrative fines and enforcement measures laid down in this Regulation or possible criminal penalties, where national law so provides. Moreover, a health data applicant should be able to request a response to a health data request in an anonymised statistical format. In such cases, the health data user will only process non-personal data, and the health data access body will remain sole controller for any personal data necessary to provide the response to the health data request.

(73) In order to ensure that all health data access bodies issue data 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 health data applicant should provide health data access bodies with several elements of information that would help the body evaluate the health data access application and decide if the health data applicant can receive a data permit, and coherence should be ensured between different health data access bodies. The information provided as part of the health data access application should comply with the requirements established under this Regulation in order to enable it to be thoroughly assessed, as a data permit should only be issued if all the necessary conditions set out in this Regulation are met. In addition, where relevant, that information should include a declaration by the health data applicant that the intended use of the health data requested does not pose a risk of stigmatisation, or of causing harm to the dignity, of natural persons or groups to which the dataset requested relates. An ethical assessment could be requested based on national law. In that case, it should be possible for existing ethics bodies to carry out such assessments for the health data access body. Existing ethics bodies of Member States should make their expertise available to the health data access body for that purpose. Alternatively, Member States should be able to provide for ethics bodies to be 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 health data applicant needs data in an anonymised statistical format, it should submit a health data request, requiring the health data access body to provide the result directly. A refusal of a data permit by the health data access body should not preclude the health data applicant from submitting a new health data access application. In order to ensure a harmonised approach between health data access bodies and to limit the 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. In justified cases, such as in the case of a complex and burdensome request, the health data access body should be allowed to extend the time period for health data holders to make the requested electronic health data available to it.

(74) As their resources are limited, health data access bodies should be allowed to apply prioritisation rules, for instance prioritising public institutions over private entities, but they should not discriminate between the national organisations and organisations from other Member States within the same category of priorities. A 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 publications or to enable additional analysis of the dataset based on the initial findings. This should require an amendment of the data permit and could be subject to an additional fee. However, in all cases, the data permit should reflect such additional uses of the dataset. Preferably, the health data user should mention them in their initial health data access application. In order to ensure a harmonised approach between health data access bodies, the Commission should support the harmonisation of data permits.

(75) 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 provided for in 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 could be required in specific Member States or throughout the whole territory of the Union. Such Union institutions, bodies, offices and agencies should be able to benefit from an accelerated procedure for having data made available, ordinarily in less than two months, with a possibility of prolonging the timeline by one month in more complex cases.

(76) Member States should be able to designate trusted health data holders for which the data permit issuing procedure can be performed in a simplified manner, in order to alleviate the administrative burden for health data access bodies of managing requests for the data processed by them. Trusted health data holders should be allowed to assess the health data access applications submitted under this simplified procedure, based on 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 health data holder. Health data intermediation entities should not be designated as trusted health data holders.

(77) Given the sensitivity of electronic health data, health data users should not have 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 there are strong technical and security safeguards in place for the electronic health data, the health data access body or, where relevant, the trusted health 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 processing environment should comply with Regulation (EU) 2016/679, including, where the secure processing environment is managed by a third party, the requirements of Article 28 of that Regulation and, where applicable, Chapter V thereof. 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 health data users. The health data access body or the health data holder providing that service should remain at all times in control of the access to the electronic health data, and the access granted to the health data users should be determined by the conditions of the issued data permit. Only non-personal electronic health data which do not contain any personal electronic health data should be downloaded by the health data users from such secure processing environment. Thus, such a secure processing environment 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 States in developing common security standards in order to promote the security and interoperability of the various secure processing environments.

(78) 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 referred to in that Regulation. Where such rules provide for the use of a secure processing environment for that sector, such secure processing environment should comply with the criteria established in this Regulation. The health data access bodies should cooperate with the competent authorities designated under Regulation (EU) 2022/868 to supervise the activity of data altruism organisations in the health or care sector.

(79) For the processing of electronic health data in the scope of a data permit or a health data request, health data holders, including trusted health data holders, health data access bodies and health data users should be deemed each of them, in turn, controllers for a specific part of the process and according to their respective roles therein. Health data holders should be deemed controllers for the disclosure of the requested personal electronic health data to the health data access bodies, while the health data access bodies should in turn be deemed controllers for the processing of the personal electronic health data when preparing the data and making them available to the health data users. Health data users should be deemed controllers for the processing of personal electronic health data in pseudonymised form in the secure processing environment pursuant to their data permits. Health data access bodies should be deemed processors on behalf of the health data user for the 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 a response to a health data request. Similarly, trusted health data holders should be deemed controllers for their 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 health data request. The trusted health data holders should be deemed processors for the health data user when providing data through a secure processing environment.

(80) In order to achieve an inclusive and sustainable framework for multi-country secondary use, a cross-border infrastructure should be established ('HealthData@EU'). HealthData@EU should accelerate secondary use while increasing legal certainty, respecting the privacy of natural persons and being interoperable. Due to the sensitivity of health data, principles such as 'privacy by design' and 'privacy by default' and the concept of bringing questions to data instead of moving those data should be respected whenever possible. Member States should designate national contact points for secondary use, as organisational and technical gateways for health data access bodies, and connect those contact points to HealthData@EU. The Union health data access service should also be connected to HealthData@EU. In addition, authorised participants in HealthData@EU could be research infrastructures established as a European Research Infrastructure Consortium ('ERIC') under Council Regulation (EC) No 723/2009[19], as a European digital infrastructure consortium ('EDIC') under Decision (EU) 2022/2481 or similar infrastructures established under other Union legal acts, as well as other types of entities, including infrastructures under the European Strategy Forum on Research Infrastructures (ESFRI) or infrastructures federated under the European Open Science Cloud (EOSC). Third countries and international organisations could also become authorised participants in HealthData@EU, provided that they are compliant with the requirements in this Regulation.

[19] 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).

The Commission communication of 19 February 2020 entitled 'A European strategy for data' promoted 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 those relating to the environment, agriculture and social sector. Such interoperability between the health sector and other sectors such as the environmental, agricultural or social sectors could be relevant for obtaining 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 in HealthData@EU for the handling of cross-border access requests, maintaining catalogues of electronic health data available through the infrastructure, network discoverability and metadata queries, connectivity and compliance services. The Commission could also set up a secure processing 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, such as those being built for the exchange of evidence under the 'once-only' technical system of Regulation (EU) 2018/1724 of the European Parliament and of the Council[20].

[20] 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).

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

(82) In the 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 of the Member State where the coordinator of the registry is located should be responsible for providing access to data.

(83) The authorisation process to gain access to personal electronic health data in different Member States can be repetitive and cumbersome for health data users. Whenever possible, synergies should be established to reduce the burden and barriers for health data users. One way to achieve that aim is to adhere to the 'single application' principle whereby, with one application, the health data user can obtain authorisation from multiple health data access bodies in different Member States or authorised participants in HealthData@EU.

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

(85) 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 and recommendations for data collection and data exchange, such as FAIR principles, also benefits health data holders, health professionals, natural persons and the Union economy overall. A data quality and utility label for datasets would inform health 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 health data holders and health 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 by frameworks created pursuant to Article 10 of Regulation (EU) 2024/1689 and the relevant technical documentation specified in Annex IV to that Regulation 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 those activities. The use of datasets could be prioritised by their users according to their usefulness and quality.

(86) The EU dataset catalogue should minimise the administrative burden for the health data holders and other database users, be user-friendly, accessible and cost-effective, connect national dataset catalogues and avoid redundant registration of datasets. Without prejudice to the requirements set out in Regulation (EU) 2022/868, the EU dataset catalogue could be aligned with the data.europa.eu initiative. Interoperability should be ensured between the EU dataset catalogue, the national dataset catalogues and the dataset catalogues from European research infrastructures and other relevant data sharing infrastructures.

(87) 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, for instance registries. That 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 the supply of such data for secondary use in a consistent way. Such datasets could include data from registries of rare diseases, orphan drugs databases, cancer registries and registries of highly relevant infectious diseases. Member States should work towards ensuring that European electronic health systems and services and interoperable applications deliver sustainable economic and social benefits, 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 that are useful for defining and implementing data standards and interoperability and should be leveraged to enable continuity and to build on existing expertise.

(88) The Commission should support Member States in building capacity and enhancing effectiveness in the area of digital health systems for primary use and secondary use. 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 that respect. Those activities should take into account the specific circumstances of different categories of stakeholders, such as representatives of civil society, researchers, medical societies and SMEs.

(89) Improving digital health literacy for both natural persons and health professionals is essential to trust and safety and appropriate use of health data and thus is essential to achieving a successful implementation of this Regulation. Health professionals are faced with profound changes in the context of digitalisation and will be offered further digital tools as part of the implementation of the EHDS. Consequently, health professionals need to develop their digital health literacy and digital skills and Member States should provide access for health professionals to digital literacy courses so that they can prepare to work with EHR systems. Such courses should allow 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 training courses 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, actively manage their health and care, and understand the implications of the management of such data for both primary use 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.

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

(91) The implementation of the EHDS requires appropriate investment in capacity-building and training and a well-funded commitment to public consultation and engagement both at Union and national level. The economic costs of implementing this Regulation will need to be borne at both Union and national level, and a fair sharing of that burden between Union and national funds will need to be found.

(92) Certain categories of electronic health data can remain particularly sensitive even when they are in anonymised format and thus non-personal, as already specifically provided for in Regulation (EU) 2022/868. Even where state-of-the-art anonymisation techniques are used, 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, that is to say a life-threatening or chronically debilitating condition affecting not more than 5 in 10 thousand persons in the Union, where the limited numbers of cases reduce the possibility of fully aggregating 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. Such residual risk can affect different categories of health data and can lead to the re-identification of the data subjects using means that are beyond those reasonably likely to be used. Such risk depends on the level of granularity, on the description of the characteristics of data subjects, on the number of people affected, for instance in cases of data included in electronic health records, disease registries, biobanks and person-generated data, where the range of identification characteristics is broader, and on the possible combination with other information, for example in very small geographical areas, or through the technological evolution of methods which had not been available at the moment of anonymisation. Such re-identification of natural persons would present a major concern and would be likely to put the acceptance of the 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 is the case 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 those categories of health data, there remains a risk of re-identification after the anonymisation or aggregation, which cannot be reasonably mitigated initially. This falls within the criteria indicated in Article 5(13) of Regulation (EU) 2022/868. Those types of health data would thus fall within the empowerment set out in Article 5(13) of that Regulation for transfer to third countries. The special conditions provided for under the empowerment set out in Article 5(13) of Regulation (EU) 2022/868 will be detailed in the context of the delegated act adopted under that empowerment, and need to be proportional to the risk of re-identification and to take into account the specificities of different data categories or of different anonymisation or aggregation techniques.

(93) The processing of large amounts of personal electronic health data for the purposes of the EHDS, as part of data processing activities in the context of handling health data access applications, data permits and health data requests entails higher risks of unauthorised access to such personal data, as well as the possibility of cybersecurity incidents. Personal electronic health data are particularly sensitive as they often contain 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 this Regulation, to guarantee a particularly high level of protection and security, and to reduce the risk of unlawful access to those personal electronic health data, this Regulation allows Member States to require that personal electronic health data be stored and processed solely within the Union for the purpose of carrying out the tasks provided for in this Regulation, unless an adequacy decision adopted pursuant to Article 45 of Regulation (EU) 2016/679 applies.

(94) Access to electronic health data for health data users established in third countries or for international organisations should take place only on the basis of the reciprocity principle. Making electronic health data available to a third country should be allowed to take place only where the Commission has established, by means of an implementing act, that the third country concerned allows access to electronic health data originating from that third country by Union entities under the same conditions and with the same safeguards as would be the case if they were accessing electronic health data within the Union. The Commission should monitor and carry out a periodic review of the situation in those third countries and for international organisations and list those implementing acts. Where the Commission finds that a third country no longer ensures access on the same terms, it should revoke the corresponding implementing act.

(95) In order to promote the consistent application of this Regulation, including as regards cross-border interoperability of electronic health data, a European Health Data Space 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 States to coordinate the use of electronic health data for healthcare and certification, but also concerning secondary use, and the funding for those activities. This could also include sharing information on risks and incidents in the secure processing environments. The sharing of that kind of information 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 primary use may be different from the health data access bodies dealing with secondary use, the functions are different and there is a need for distinct cooperation in each of those areas, the EHDS Board should be able to set up subgroups dealing with those two functions, as well as other subgroups, as needed. In order for there to be an efficient working method, the digital health authorities and health data access bodies should create networks and links at national level with 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 (EU) 2022/868, (EU) 2023/2854 and (EU) 2024/1689 and Regulation (EU) 2019/881 of the European Parliament and of the Council[21]. The EHDS Board should operate independently, in the public interest and in line with its code of conduct.

[21] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

(96) Where issues that are considered by the EHDS Board to be of specific relevance are discussed, it should be able to invite observers, for instance the EDPS, representatives of Union institutions, including of the European Parliament, and other stakeholders.

(97) A stakeholder 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 stakeholder forum should be composed, inter alia, of representatives of patient and consumer organisations, 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.

(98) In order to ensure proper day-to-day management of the cross-border infrastructures for primary use and secondary use, it is necessary to create steering groups consisting of Member State representatives. These steering groups should take operational decisions on the technical day-to-day management of the cross-border 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 should not include contributing to the development of implementing acts affecting those infrastructures. The steering groups should also be able to invite representatives of other authorised participants in HealthData@EU as observers to their meetings and should consult relevant experts when carrying out their tasks.

(99) 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 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, information on the progress made in dealing with the complaint 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 should cooperate to handle and resolve complaints, including by exchanging all relevant information by electronic means, without undue delay.

(100) 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 constituted in accordance with national law, having statutory public interest objectives and active in the field of the protection of personal data, to lodge a complaint on his or her behalf.

(101) The digital health authority, health data access body, health data holder or health data user should compensate any damage which a natural or legal person suffers as a result of an infringement of this Regulation. The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union, 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 provisions in Union or national law. Natural persons should receive full and effective compensation for the damage they have suffered.

(102) 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 health data access bodies 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.

(103) It is appropriate to lay down provisions enabling health data access bodies to apply administrative fines for certain infringements of this Regulation which should be considered under this Regulation to be serious infringements, such as the re-identification of natural persons, downloading personal electronic health data outside of the secure processing environment or processing of data for prohibited uses or uses not covered by a data permit. This Regulation should specify those 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, having due regard in particular to the nature, gravity and duration of the infringement and 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. For the purposes of the imposition of administrative fines under this Regulation, the concept of undertaking should be understood in accordance with Articles 101 and 102 TFEU. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning should not affect the enforcement of other powers of the health data access bodies or of other penalties under this Regulation.

(104) In order to ensure that the EHDS fulfils its objectives, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the modification, addition or removal in Annex I of the main characteristics of the priority categories of personal electronic health data, the list of required data to be entered by the manufacturers of EHR systems and wellness applications into the EU database for registration of EHR systems and wellness applications as well as the modification, addition or removal of elements to be covered by the data quality and utility label. 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[22]. 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.

[22] OJ L 123, 12.5.2016, p. 1.

(105) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission as regards:

– technical specifications for the interoperability of the proxy services of the Member States,

– data quality requirements for the registration of personal electronic health data in an EHR system,

– cross-border specifications for priority categories of personal electronic health data,

– technical specifications for the categories of personal electronic health data, setting out the European electronic health record exchange format,

– updates of the European electronic health record exchange format to integrate relevant revisions of the healthcare coding systems and nomenclatures,

– technical specifications to extend the European electronic health record exchange format to additional categories of personal electronic health data,

– requirements for the interoperable, cross-border identification and authentication mechanism for natural persons and health professionals, in accordance with Regulation (EU) No 910/2014,

– requirements for the technical implementation of the rights of natural persons in relation to the primary use of their personal electronic health data,

– 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,

– rules regarding the requirements of cybersecurity, technical interoperability, semantic interoperability, operations and service management in relation to the processing by the Commission and its responsibilities towards the controllers,

– technical aspects of supplementary services provided through MyHealth@EU,

– technical aspects of exchanges of personal electronic health data between MyHealth@EU and other services or infrastructures,

– connection and disconnection of other infrastructures, of national contact points for digital health of third countries or of systems established at international level by international organisations to or from the central interoperability platform of MyHealth@EU,

– common specifications in respect of the essential requirements laid down in Annex II,

– common specifications for the European digital testing environment,

– justifications of national measures taken by market surveillance authorities in the case of non-compliance by EHR systems,

– format and content of the label of wellness applications,

– principles for the fee policies and fee structures regarding the fees that health data access bodies and trusted health data holders can charge for making electronic health data available for secondary use,

– the architecture of an IT tool aimed at supporting and making transparent to health data access bodies enforcement measures,

– the logo for acknowledging the contribution of the EHDS,

– templates for the health data access application, the data permit and the health data request,

– technical, organisational, information security, confidentiality, data protection and interoperability requirements for the secure processing environments,

– templates for agreements between controllers and processors,

– decisions on the compliance of a national contact point for secondary use of a third country or a system established at international level by international organisations with the requirements of HealthData@EU for the purposes of secondary use of health data, on the compliance with Chapter IV and on whether that national contact point for secondary use or that system provides equivalent access for health data users located in the Union to the electronic health data it has access to,

– HealthData@EU's requirements, technical specifications and IT architecture; conditions and compliance checks to join and remain connected to HealthData@EU; minimum criteria to be met by national contact points for secondary use and the authorised participants in HealthData@EU; responsibilities of the controllers and processors which participate in HealthData@EU; responsibilities of the controllers and processors for the secure processing environment managed by the Commission; and common specifications for the architecture of HealthData@EU and for its interoperability with other common European data spaces,

– decisions to connect individual authorised participants to HealthData@EU,

– minimum elements for datasets and the characteristics of those elements to be provided by health data holders,

– visual characteristics and technical specifications of the data quality and utility label,

– minimum specifications for datasets of high impact for secondary use,

– decisions on whether a third country allows Union health data applicants to access electronic health data in that third country under conditions that are not more restrictive than those provided for in this Regulation,

– necessary measures for the establishment and operation of the EHDS Board.

Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[23].

---

[23] 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).

(106) Member States should take all measures necessary 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 limits and criteria set out in this Regulation. Re-identification of natural persons should be considered a serious breach of this Regulation.

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

(108) 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 targeted evaluation of this Regulation within eight years of its entry into force, and an overall evaluation within 10 years of its entry into force. 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.

(109) For a successful cross-border implementation of the EHDS, the European Interoperability Framework, the scope of which was updated and extended by the Commission communication of 23 March 2017 entitled 'European Interoperability Framework – Implementation Strategy' to take on board new or revised interoperability requirements, should be considered as a common reference to ensure legal, organisational, semantic and technical interoperability.

(110) Since the objectives of this Regulation, namely to empower natural persons by providing them with increased control over their personal electronic health data and supporting their freedom of movement by ensuring that their health data follow them, to foster a genuine internal market for digital health services and products and 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 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 use and secondary use, 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.

(111) The evaluation of the digital aspects of Directive 2011/24/EU shows that the effectiveness of the eHealth Network is limited, but also that there is strong potential for work at Union level in the area of digital health, as demonstrated by the work carried out during the COVID-19 pandemic. Directive 2011/24/EU should therefore be amended accordingly.

(112) This Regulation complements the essential cybersecurity requirements laid down in Regulation (EU) 2024/2847. EHR systems which are products with digital elements within the meaning of Regulation (EU) 2024/2847 should therefore also comply with the essential cybersecurity requirements set out in that Regulation. The manufacturers of those EHR systems should demonstrate conformity as required by this Regulation. To facilitate that conformity, manufacturers should be allowed to draw up a single set of technical documents containing the elements required by both legal acts. It should be possible to demonstrate conformity of EHR systems with essential cybersecurity requirements laid down in Regulation (EU) 2024/2847 through the assessment framework under this Regulation. However, the parts of the conformity assessment procedure under this Regulation which relate to the use of testing environments should not be applied, since those testing environments do not allow for an assessment of conformity with the essential cybersecurity requirements. As Regulation (EU) 2024/2847 does not cover Software as a Service (SaaS) directly as such, EHR systems offered through the SaaS licensing and delivery model do not fall within the scope of that Regulation. Similarly, EHR systems that are developed and used in-house do not fall within the scope of that Regulation, as they are not placed on the market.

(113) The EDPS and the EDPB were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered their joint opinion on 12 July 2022.

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

(115) Given the need for technical preparation, this Regulation should apply from … [24 months from the date of entry into force]. In order to support the successful implementation of the EHDS and the creation of effective conditions for European health data cooperation, the implementation should take place in stages,

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

2. This Regulation:

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

   (b) lays down common rules for electronic health record systems (‘EHR systems’) in relation to two mandatory harmonised software components, namely the European interoperability software component for EHR systems and the European logging software component for EHR systems, as defined in Article 2(2), points (n) and (o) respectively, and for wellness applications which are claimed to be interoperable with EHR systems in relation to those two harmonised software components, as regards primary use of electronic health data;

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

(f) establishes governance and coordination mechanisms at Union and national level for both primary use of electronic health data and secondary use of electronic health data.

3. This Regulation shall be without prejudice to other Union legal acts regarding access to, and sharing of or secondary use of, electronic health data, or Union requirements related to the processing of data in relation to electronic health data, in particular Regulations (EC) No 223/2009[24], (EU) No 536/2014[25], (EU) 2016/679, (EU) 2018/1725, (EU) 2022/868 and (EU) 2023/2854 of the European Parliament and of the Council and Directives 2002/58/EC[26] and (EU) 2016/943[27] of the European Parliament and of the Council.

4. References in this Regulation 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, as regards Union institutions, bodies, offices and agencies.

---

[24] 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).

[25] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 32).

[27] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

5. This Regulation shall be without prejudice to Regulations (EU) 2017/745, (EU) 2017/746 and (EU) 2024/1689, as regards the security of medical devices, in vitro diagnostic medical devices and artificial intelligence (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 to Union or national law regarding the granting of access to and disclosure of official documents.

7. 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 Member States' public sector bodies, by Union institutions, bodies, offices 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.

8. 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.

9. This Regulation does not apply to the processing of personal data in the following cases:

(a) where the processing is carried out in the course of an activity which falls outside the scope of Union law;

(b) where the processing is carried out 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 apply:

(a) the definitions of ‘personal data’, ‘processing’, ‘pseudonymisation’, ‘controller’, ‘processor’, ‘third party’, ‘consent’, ‘genetic data’, ‘data concerning health’ and ‘international organisation’ laid down in Article 4, points (1), (2), (5), (7), (8), (10), (11), (13), (15) and (26), respectively, of 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’ laid down in Article 3, points (a), (c), (d), (f), (g), (i) and (k), respectively, of Directive 2011/24/EU;

(c) the definitions of ‘data’, ‘access’, ‘data altruism’, ‘public sector body’ and ‘secure processing environment’ laid down in Article 2, points (1), (13), (16), (17) and (20), respectively, 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’ laid down in Article 3, points (1), (2), (3), (4), (7), (8), (9), (10), (13), (16), (22) and (23), respectively, of Regulation (EU) 2019/1020;

(e) the definitions of ‘medical device’, ‘intended purpose’, ‘instructions for use’, ‘performance’, ‘health institution’ and ‘common specifications’ laid down in Article 2, points (1), (12), (14), (22), (36) and (71), respectively, of Regulation (EU) 2017/745;

(f) the definitions of ‘electronic identification’ and ‘electronic identification means’ laid down in Article 3, points (1) and (2), respectively, of Regulation (EU) No 910/2014;

(g) the definition of ‘contracting authorities’ laid down in Article 2(1), point (1), of Directive 2014/24/EU of the European Parliament and of the Council[28];

(h) the definition of ‘public health’ laid down in Article 3, point (c), of Regulation (EC) No 1338/2008 of the European Parliament and of the Council[29].

---

[28] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

[29] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

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

(a) ‘personal electronic health data’ means data concerning health and genetic data, processed in an electronic form;

(b) ‘non-personal electronic health data’ means electronic health data other than personal electronic health data, including both data that have been anonymised so that they no longer relate to an identified or identifiable natural person (the ‘data subject’) and data that have never related to a data subject;

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

(d) ‘primary use’ means the processing of electronic health data for the provision of healthcare, in order to assess, maintain or restore the state of health of the natural person to whom those data relate, 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’ means the processing of electronic health data for the 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 of software applications or devices from the same manufacturer or different manufacturers, to interact through the processes they support, involving the exchange of information and knowledge, without changing the content of the data, between those organisations, software applications or devices;

(g) ‘registration of electronic health data’ means the recording of health data in an electronic format, through the manual entry of such data, through the collection of such 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;

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

(i) ‘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;

(j) ‘electronic health record’ or ‘EHR’ 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;

(k) ‘electronic health record system’ or ‘EHR system’ means any system whereby the software, or a combination of the hardware and the software of that system, allows personal electronic health data that belong to the priority categories of personal electronic health data established under this Regulation to be stored, intermediated, exported, imported, converted, edited or viewed, and intended by the manufacturer to be used by healthcare providers when providing patient care or by patients when accessing their electronic health data;

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

(m) ‘software component’ means a discrete part of software which provides a specific functionality or performs specific functions or procedures and which can operate independently or in conjunction with other components;

(n) ‘European interoperability software component for EHR systems’ means a software component of the EHR system which provides and receives personal electronic health data under a priority category for primary use established under this Regulation in the European electronic health record exchange format provided for in this Regulation and which is independent of the European logging software component for EHR systems;

(o) ‘European logging software component for EHR systems’ means a software component of the EHR system which provides logging information related to access by health professionals or other individuals to priority categories of personal electronic health data established under this Regulation, in the format defined in point 3.2. of Annex II thereto, and which is independent of the European interoperability software component for EHR systems;

(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 law providing for its affixing pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council[30];

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

(r) ‘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 harm to a natural person’s health;

(ii) serious prejudice to a natural person’s rights;

---

[30] 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).

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

(s) ‘care’ means a professional service the purpose of which is to address the specific needs of a natural 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 his or her personal autonomy;

(t) ‘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 where necessary, 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, that has either:

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

(ii) the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data;

(u) ‘health data user’ means a natural or legal person, including Union institutions, bodies, offices or agencies, which has been granted lawful access to electronic health data for secondary use pursuant to a data permit, a health data request approval or an access approval by an authorised participant in HealthData@EU;

(v) ‘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;

(w) ‘dataset’ means a structured collection of electronic health data;

(x) ‘dataset of high impact for secondary use’ means a dataset the re-use of which is associated with significant benefits due to its relevance for health research;

(y) ‘dataset catalogue’ means a collection of dataset descriptions, arranged in a systematic manner and including a user-oriented public part, in which information concerning individual dataset parameters is accessible by electronic means through an online portal;

(z) ‘data quality’ means the degree to which the elements of electronic health data are suitable for their intended primary use and secondary use;

(aa) ‘data quality and utility label’ means a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset;

(ab) ‘wellness application’ means any software, or any combination of hardware and software, intended by the manufacturer to be used by a natural person, for the processing of electronic health data, specifically for providing information on the health of natural persons, or the delivery of care for purposes other than the provision of healthcare.

# Chapter II
# Primary use

## SECTION 1
## RIGHTS OF NATURAL PERSONS IN RELATION TO THE PRIMARY USE OF THEIR PERSONAL ELECTRONIC HEALTH DATA, AND RELATED PROVISIONS

*Article 3*

*Right of natural persons to access their personal electronic health data*

1. Natural persons shall have the right to access at least personal electronic health data relating to them that belong to the priority categories referred to in Article 14 and are processed for the provision of healthcare through the electronic health data access services referred to in Article 4. Access shall be provided immediately after the personal electronic health data have been registered in an EHR system, while respecting the need for technological practicability, and shall be provided free of charge and in an easily readable, consolidated and accessible format.

2. Natural persons, or their representatives referred to in Article 4(2), shall have the right to download free of charge an electronic copy of at least the personal electronic health data in the priority categories referred to in Article 14 related to those natural persons, through the electronic health data access services referred to in Article 4, in the European electronic health record exchange format referred to in Article 15.

3. In accordance with Article 23 of Regulation (EU) 2016/679, Member States may restrict the scope of rights provided for in paragraphs 1 and 2 of this Article, in particular whenever those restrictions are necessary to protect natural persons, on the basis of patient safety and ethical considerations by delaying access to their personal electronic health data for a limited period of time until a health professional is able to properly communicate and explain to the natural persons concerned information that can have a significant impact on their health.

*Article 4*

*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, thereby enabling natural persons to access their personal electronic health data and exercise their rights provided for in Articles 3 and 5 to 10. Such electronic health data access services shall be free of charge for the natural persons and their representatives referred to in paragraph 2 of this Article.

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

   (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 limited or unlimited period and, if needed, for a specific purpose only, and to manage those authorisations; and

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

Member States shall establish rules regarding the authorisations referred to in point (a) of the first subparagraph and actions of guardians and other legal representatives.

3. The proxy services referred to in paragraph 2 shall provide authorisations in a transparent and easily understandable way, free of charge, and electronically or on paper. Natural persons and their representatives shall be informed about their authorisation rights, including about how to exercise those rights, and about the authorisation process.

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

4. The proxy services referred to in paragraph 2 of this Article shall be interoperable among Member States. The Commission shall, by means of implementing acts, lay down the technical specifications for the interoperability of the proxy services of the Member States. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

5. The electronic health data access services and the proxy services shall be easily accessible for persons with disabilities, vulnerable groups and persons with low digital literacy.

*Article 5*

*Right of natural persons to insert information in their own EHR*

Natural persons, or their representatives referred to in Article 4(2), shall have the right to insert information in the EHR of those natural persons through electronic health data access services or applications linked to those services as referred to in that Article. That information shall be clearly distinguishable as having been inserted by the natural person or by his or her representative. Natural persons, or their representatives referred to in Article 4(2), shall not be able to directly alter the electronic health data and related information inserted by health professionals.

*Article 6*

*Right of natural persons to rectification*

Electronic health data access services referred to in Article 4 shall enable natural persons to easily request online the rectification of their personal electronic health data in accordance with Article 16 of Regulation (EU) 2016/679. Where appropriate, the controller shall verify with a relevant health professional the accuracy of the information provided in the request.

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

*Article 7*

*Right to data portability for natural persons*

1. Natural persons shall have the right to give access to, or to request a healthcare provider to transmit, all or part of their personal electronic health data to another healthcare provider of their choice immediately, free of charge and without hindrance from the healthcare provider or from the manufacturers of the systems used by that healthcare provider.

2. Natural persons shall have the right, where the healthcare providers are located in different Member States, to request the transmission of their personal electronic health data in the European electronic health record exchange format referred to in Article 15 through the cross-border infrastructure referred to in Article 23. The receiving healthcare provider shall accept such data and shall be able to read them.

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

4. Where natural persons have downloaded an electronic copy of their priority categories of personal electronic health data in accordance with Article 3(2) they shall be able to transmit those data to healthcare providers of their choice in the European electronic health record exchange format referred to in Article 15. The receiving healthcare provider shall accept such data and be able to read them, as applicable.

*Article 8*

*Right to restrict access*

Natural persons shall have the right to restrict the access of health professionals and healthcare providers to all or parts of their personal electronic health data as referred to in Article 3.

When exercising the right referred to in the first paragraph, natural persons shall be made aware that restricting access might impact the provision of healthcare to them.

The fact that a natural person has restricted access under the first paragraph shall not be visible to healthcare providers.

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

*Article 9*

*Right to obtain information on accessing data*

1. 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 obtained in the context of healthcare, including access provided in accordance with Article 11(5).

2. The information referred to in paragraph 1 shall be provided free of charge and without delay through electronic health data access services and shall be available for at least three years from each date of access to the data. That information shall include at least the following:

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

   (b) the date and time of access;

   (c) which personal electronic health data were accessed.

3. Member States may provide for restrictions to the right referred to in paragraph 1 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 10*

*Right of natural persons 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 4 and 12. In such cases, Member States shall ensure that the exercise of that right is reversible.

2. If a Member State provides for a right referred to in paragraph 1 of this Article, it shall establish the rules and specific safeguards regarding the opt-out mechanism. In particular, Member States may provide for a healthcare provider or health professional to be able 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), point (c), of Regulation (EU) 2016/679, even if the patient has exercised the right to opt out in primary use.

*Article 11*

*Access by health professionals to personal electronic health data*

1. Where health professionals process data in an electronic format, they 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 12, irrespective of the Member State of affiliation and the Member State of treatment.

2. Where the Member State of affiliation of the natural person under treatment and the Member State of treatment of such natural person differ, cross-border access to the personal electronic health data of the natural person under treatment shall be provided through the cross-border infrastructure referred to in Article 23.

3. The access referred to in paragraphs 1 and 2 of this Article shall include at least the priority categories of personal electronic health data referred to in Article 14.

In line with the principles provided for in Article 5 of Regulation (EU) 2016/679, Member States shall establish rules providing for the categories of personal electronic health data accessible by different categories of health professionals or for different healthcare tasks. Such rules shall take into account the possibility of restrictions imposed under Article 8 of this Regulation.

4. In the case of treatment in a Member State other than the Member State of affiliation, the rules referred to in paragraph 3 shall be those of the Member State of treatment.

5. Where access to personal electronic health data has been restricted by a natural person pursuant to Article 8, the healthcare provider or health professional shall not be informed of the restricted content of those data.

By way of derogation from the first paragraph of Article 8, where necessary in order to protect the vital interests of the data subject, the healthcare provider or health professional may be granted access to the restricted electronic health data. Such cases shall be logged in a clear and understandable format and shall be easily accessible for the data subject.

Member States may provide for additional safeguards.

*Article 12*

*Health professional access services*

For the provision of healthcare, Member States shall ensure that health professionals are able to access free of charge the priority categories of personal electronic health data referred to in Article 14, including for cross-border care, through health professional access services.

The services referred to in the first paragraph of this Article shall be accessible only to health professionals who are in possession of electronic identification means which are recognised pursuant to Article 6 of Regulation (EU) No 910/2014 or other electronic identification means compliant with common specifications referred to in Article 36 of this Regulation.

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

*Article 13*

*Registration of personal electronic health data*

1. Member States shall ensure that, where electronic health data are processed for the provision of healthcare, healthcare providers register the relevant personal electronic health data falling fully or partially under at least the priority categories of personal electronic health data referred to in Article 14 in an electronic format in an EHR system.

2. When processing data in an electronic format, healthcare providers shall ensure that the personal electronic health data of the natural persons under their treatment are updated with information related to the healthcare.

3. Where personal electronic health data are registered in a Member State of treatment that differs from the Member State of affiliation of the natural 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.

4. By … [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, determine data quality requirements, including in relation to semantics, uniformity, consistency, accuracy and completeness, for the registration of personal electronic health data in an EHR system as relevant. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

When personal electronic health data are registered or updated, the electronic health records shall identify the health professional and healthcare provider that carried out such registration or update, and the time at which such registration or update was carried out. Member States may require other aspects of data registration to be recorded.

*Article 14*

*Priority categories of personal electronic health data for primary use*

1. For the purposes of this Chapter, where data are 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; and

   (f) discharge reports.

   The main characteristics of the priority categories of personal electronic health data for primary use shall be as set out in Annex I.

Member States may provide in their national law for additional categories of personal electronic health data to 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 the categories of personal electronic health data referred to in the third subparagraph of this paragraph pursuant to Article 15(3) and Article 23(8). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. The Commission is empowered to adopt delegated acts in accordance with Article 97 to amend this Regulation by amending Annex I through the addition, modification or removal of the main characteristics of the priority categories of personal electronic health data as referred to in paragraph 1, provided that the amendments are aimed at adapting the priority categories of personal electronic health data to technical developments and international standards. Moreover, additions and modifications of those characteristics shall satisfy both of the following criteria:

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

(b) the characteristic is used in the majority of Member States according to the most recent information.

*Article 15*

*European electronic health record exchange format*

1. By … [two years from the date of entry into force of this Regulation], 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 14(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. Such format shall support transmission of structured and unstructured health data and 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.

   The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. The Commission shall, by means of implementing acts, provide regular updates of the European electronic health record exchange format to integrate relevant revisions of the healthcare coding systems and nomenclatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

3. The Commission may, by means of implementing acts, lay down technical specifications to extend the European electronic health record exchange format to additional categories of personal electronic health data referred to in Article 14(1), third subparagraph. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

4. Member States shall ensure that the priority categories of personal electronic health data referred to in Article 14 are issued in the European electronic health record exchange format referred to in paragraph 1 of this Article. Where such data are transmitted by automated means for primary use, the receiving provider shall accept the format of the data and be able to read them.

*Article 16*

*Identification management*

1. Where natural persons use electronic health data access services referred to in Article 4, those natural persons shall have the right to identify themselves electronically using any electronic identification means which are 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. That 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 98(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 infrastructure referred to in Article 23.

4. The Member States' competent authorities and the Commission shall implement the interoperable, cross-border identification and authentication mechanism at Member State and Union level, respectively.

*Article 17*

*Requirements for technical implementation*

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 98(2).

*Article 18*

*Compensation for making personal electronic health data available*

Providers receiving data under this Chapter shall not be required to compensate the healthcare provider for making personal electronic health data available. A healthcare provider or a third party shall not directly or indirectly charge data subjects a fee or costs, or require compensation, for sharing or accessing data.

## SECTION 2

## GOVERNANCE FOR PRIMARY USE

*Article 19*

*Digital health authorities*

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 States shall inform the Commission of the identity of the digital health authorities by … [the date of entry into force of this Regulation + 24 months]. Where a Member State designates more than one digital health authority or where the digital health authority consists of multiple organisations, the Member State concerned shall communicate to the Commission a description of the distribution of tasks between those various authorities or organisations. Where a Member State designates several digital health authorities, it shall designate one digital health authority to act as coordinator. The Commission shall make that information publicly available.

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

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

(b) ensuring that complete and up-to-date information about the implementation of rights and obligations provided for in this Chapter and Chapter 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) of this paragraph, ensuring that such technical solutions comply with this Chapter, Chapter III and Annex II;

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

(e) facilitating persons with disabilities to exercise their rights under this Chapter in accordance with Directive (EU) 2019/882 of the European Parliament and of the Council[31];

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

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

---

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

(h) contributing at Union level to the development of the European electronic health record exchange format, to the elaboration of common specifications, in accordance with Article 36, which address quality, interoperability, security, safety, ease of use, accessibility, non-discrimination or fundamental right concerns, and to the elaboration of the specifications of the EU database for registration of EHR systems and wellness applications referred to in Article 49;

(i) where applicable, performing market surveillance activities in accordance with Article 43, while ensuring that any conflicts of interest are avoided;

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

(k) cooperating with market surveillance authorities, participating in the activities related to handling of risks posed by EHR systems and of serious incidents and supervising the implementation of corrective action in accordance with Article 44;

(l) cooperating with other relevant entities and bodies at local, regional, national or Union level, to ensure interoperability, portability and security of electronic health data;

(m) cooperating with supervisory authorities in accordance with Regulations (EU) No 910/2014 and (EU) 2016/679 and Directive (EU) 2022/2555 of the European Parliament and of the Council[32] and with other relevant authorities, including those competent for cybersecurity and electronic identification.

---

[32] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

3. 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.

4. In the performance of its tasks, each digital health authority shall avoid any conflicts of interest. Each member of staff of the digital health authority shall act in the public interest and in an independent manner.

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

*Article 20*

*Reporting by digital health authorities*

Digital health authorities designated pursuant to Article 19 shall publish an activity report every two years, which shall contain a comprehensive overview of their activities. If a Member State designates more than one digital health authority, one of them shall be responsible for the drawing up of the report and, in doing so, it shall request the necessary information from the other digital health authorities. That activity report shall follow a structure agreed at Union level within the European Health Data Space Board (the 'EHDS Board') referred to in Article 92. That activity report shall contain at least information concerning:

(a) the measures taken to implement this Regulation;

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

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

(d) the number of healthcare providers of different types, including pharmacies, hospitals and other points of care, connected to MyHealth@EU calculated:

(i) in absolute terms;

(ii) as a share of all healthcare providers of the same type; and

(iii) as a share of natural persons that are able to use the services;

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

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

*Article 21*

*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 in relation to the provisions laid down in this Chapter, individually or, where relevant, collectively, with the competent digital health authority, provided that their rights or interests are negatively affected.

2. Where the complaint concerns the rights of natural persons pursuant to Articles 3 and 5 to 10 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 the assessment and investigation of the complaint.

3. The competent digital health authority with which the complaint has been lodged shall inform, in accordance with national law, the complainant of the progress made in dealing with the complaint, of the decision taken on the complaint, of any referral of the complaint to the competent supervisory authority under Regulation (EU) 2016/679 and, in cases of such a referral, that that supervisory authority is, from that moment on, to be the sole point of contact for the complainant in that matter.

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

5. Digital health authorities shall facilitate the submission of complaints and provide easily accessible tools for the submission of complaints.

*Article 22*

*Relationship with supervisory authorities under Regulation (EU) 2016/679*

The supervisory authority or supervisory authorities responsible for monitoring and enforcing the application of Regulation (EU) 2016/679 shall also be competent for monitoring and enforcing the application of Articles 3 and 5 to 10 of this Regulation. The relevant provisions of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. Supervisory authorities shall be empowered to impose administrative fines up to the amount referred to in Article 83(5) of Regulation (EU) 2016/679.

The supervisory authorities referred to in the first paragraph of this Article and digital health authorities referred to in Article 19 shall, where relevant, cooperate in the enforcement of this Regulation, within the remit of their respective competences.

## SECTION 3

## CROSS-BORDER INFRASTRUCTURE

## FOR PRIMARY USE OF PERSONAL ELECTRONIC HEALTH DATA

*Article 23*

*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 the 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. Each national contact point for digital health shall be connected to all other national contact points for digital health in other Member States and to the central interoperability platform for digital health in the cross-border infrastructure MyHealth@EU. Where a national contact point for digital health is an entity consisting of multiple organisations responsible for implementing different services, the Member State concerned shall communicate to the Commission a description of the distribution of tasks between the organisations. Each Member State shall inform the Commission of the identity of its national contact point for digital health by … [the date of entry into force of this Regulation + 24 months]. The national contact point for digital health may be designated within the digital health authority referred to in Article 19. Member States shall inform the Commission of any subsequent modification of the identity of those national contact points for digital health. The Commission and the Member States shall make that 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 14(1) with national contact points for digital health in other Member States through MyHealth@EU. That exchange shall be based on the European electronic health record exchange format.

Where Member States provide for additional categories of personal electronic health data under Article 14(1), third subparagraph, the national contact point for digital health shall enable the exchange of the additional categories of personal electronic health data referred to in Article 14(1), third subparagraph, insofar as the Member State concerned has provided for those additional categories of personal electronic health data to be accessed and exchanged in accordance with Article 14(1), third subparagraph.

4. By … [two years from the date of entry into force of this Regulation], 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 98(2).

5. Member States shall ensure the connection of all healthcare providers to their national contact points for digital health. Member States shall ensure that connected healthcare providers are able to perform two-way exchanges 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 able to dispense electronic prescriptions issued in other Member States, under the conditions laid down in Article 11 of Directive 2011/24/EU.

Pharmacies shall access and accept electronic prescriptions transmitted to them from other Member States through MyHealth@EU, provided that the conditions laid down in Article 11 of Directive 2011/24/EU are fulfilled.

Following the dispensation of medicinal products based on an electronic prescription from another Member State, the pharmacy concerned shall report through MyHealth@EU such dispensation to the national contact point for digital health of the Member State in which that prescription was issued.

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. The Commission shall, by means of implementing acts, 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 98(2).

9. The national contact points for digital health shall fulfil the conditions to join and to remain connected to MyHealth@EU as laid down in the implementing acts referred to in paragraph 4. The compliance of the national contact points for digital health with those conditions shall be verified by the Commission through compliance checks.

*Article 24*

*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 existing translations of their 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 supplementary services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(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 in 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 examination procedure referred to in Article 98(2).

The connection and disconnection of another infrastructure to the central platform for digital health shall be subject to a decision of the Commission adopted by means of an implementing act, based on the result of compliance checks of the technical aspects of exchanges as referred to in the first subparagraph of this paragraph. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

3. A national contact point for digital health of a third country or a system established at international level by an international organisation may become an authorised participant in MyHealth@EU provided that it fulfils the requirements of MyHealth@EU for the purposes of the personal electronic health data exchange as referred to in Article 23, that the transfer stemming from the connection to MyHealth@EU complies with the rules in Chapter V of Regulation (EU) 2016/679, and that the requirements concerning legal, organisational, operational, semantic, technical and cybersecurity measures are equivalent to those applicable to Member States in the operation of MyHealth@EU services. Those requirements shall be verified by the Commission through compliance checks.

Based on the outcome of the compliance checks referred to in the first subparagraph of this paragraph, the Commission may, by means of implementing acts, decide to connect or disconnect the national contact point for digital health of the third country or the system established at international level by an international organisation, as applicable, to or from MyHealth@EU. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

The Commission shall establish and maintain a list of national contact points for digital health of third countries or of systems established at international level by international organisations which are 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 25*

*Harmonised software components of EHR systems*

1. EHR systems shall include a European interoperability software component for EHR systems and a European logging software component for EHR systems (the 'harmonised software components of EHR systems'), 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 26*

*Placing on the market and putting into service*

1. EHR systems shall 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, as well as EHR systems offered as a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council[33] to a natural or legal person established in the Union, shall be considered as having been put into service.

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

*Article 27*

*Relation to Union law governing medical devices, in vitro diagnostic medical devices and AI systems*

1. Manufacturers of medical devices or in vitro diagnostic medical devices, as defined in Article 2, point (1), of Regulation (EU) 2017/745 and Article 2, point (2), of Regulation (EU) 2017/746 respectively, that claim interoperability of those medical devices or in vitro diagnostic medical devices with the harmonised software components of EHR systems shall prove compliance with the essential requirements on the European interoperability software component for EHR systems and the European logging software component for EHR systems, laid down in Section 2 of Annex II to this Regulation. Article 36 of this Regulation shall apply to those medical devices and in vitro diagnostic medical devices.

---

[33] 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).

2. Providers of AI systems considered to be high-risk in accordance with Article 6 of Regulation (EU) 2024/1689 (the ‘high-risk AI system’) and which do not fall within the scope of Regulation (EU) 2017/745 or (EU) 2017/746, that claim interoperability of those high-risk AI systems with the harmonised software components of EHR systems, shall prove compliance with the essential requirements on the European interoperability software component for EHR systems and the European logging software component for EHR systems, as laid down in Section 2 of Annex II to this Regulation. Article 36 of this Regulation shall apply to those high-risk AI systems.

*Article 28*

*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 in Article 3, point (8), of Regulation (EU) 2018/1807 with regard to their 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 to form part of the intended purpose in the technical documentation.

*Article 29*

*Procurement, reimbursement and financing*

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

## SECTION 2

## OBLIGATIONS OF ECONOMIC OPERATORS WITH REGARD TO EHR SYSTEMS

*Article 30*

*Obligations of manufacturers of EHR systems*

1. Manufacturers of EHR systems shall:

   (a) ensure that the harmonised software components of their EHR systems and the EHR systems themselves, 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 36;

   (b) ensure that the harmonised software components of their EHR systems are not adversely affected by other software components of the same EHR system;

(c) draw up the technical documentation of their EHR systems in accordance with Article 37 before placing those EHR systems on the market, and subsequently keep it up to date;

(d) ensure that their EHR systems are accompanied, free of charge for the user, by the information sheet provided for in Article 38 and clear and complete instructions for use;

(e) draw up the EU declaration of conformity in accordance with Article 39;

(f) affix the CE marking of conformity in accordance with Article 41;

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

(h) comply with the registration obligations in Article 49;

(i) take without undue delay any necessary corrective action in respect of their EHR systems, where they consider or have reason to believe that such systems are not or are no longer in conformity with the essential requirements laid down in Annex II, or recall or withdraw such systems; the manufacturers of EHR systems shall subsequently inform the national authorities of the Member States in which they made their EHR systems available on the market or put them into service of the non-conformity, of any corrective action taken, including the timetable for implementation, and of the date at which the harmonised software components of their EHR systems have been brought into conformity or been recalled or withdrawn;

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

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

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

(m) cooperate with market surveillance authorities, at their request, on any action taken to bring the EHR systems which they have placed on the market or put into service into conformity with the essential requirements laid down in Annex II and with any requirements adopted pursuant to Article 42 in an official language of the Member State concerned;

(n) establish channels of complaint and keep distributors informed thereof;

(o) keep a register of complaints and a register of non-conforming EHR systems and keep distributors informed thereof.

2. Manufacturers of EHR systems shall ensure that procedures are in place to ensure that the design, development and deployment of the harmonised software components of an EHR system continue to comply with the essential requirements laid down in Annex II and the common specifications referred to in Article 36. Changes in EHR system design or characteristics with regard to the harmonised software components of an EHR system shall be adequately taken into account and reflected in the technical documentation.

3. Manufacturers of EHR systems shall keep the technical documentation referred to in Article 37 and the EU declaration of conformity referred to in Article 39 for 10 years after the EHR system covered by the EU declaration of conformity has been placed on the market.

Manufacturers of EHR systems shall make available the source code or the programming logic included in the technical documentation, upon a reasoned request, to the relevant authorities, if that source code or programming logic is necessary in order for those authorities to be able to check compliance with the essential requirements laid down in Annex II.

4. 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 31(2).

5. Manufacturers of EHR systems shall, upon 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 laid down in Annex II and the common specifications referred to in Article 36, in a language which can be easily understood by that market surveillance authority. The manufacturers of EHR systems shall cooperate with the market surveillance authority, at its request, on any measures taken to eliminate the risks posed by an EHR system which they have placed on the market or put into service.

*Article 31*

*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 referred to in Article 37 at the disposal of market surveillance authorities for the period referred to in Article 30(3);

(b) further to a reasoned request from a market surveillance authority, provide authorities of the Member State concerned with a copy of the mandate and 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 referred to in Article 36;

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

(d) inform without undue delay the manufacturer about any complaint received from consumers or professional users;

(e) cooperate with the market surveillance authorities, at their request, on any corrective action taken in relation to the EHR systems covered by their mandate;

(f) terminate the mandate if the manufacturer does not comply with its obligations under this Regulation;

(g) ensure that the technical documentation referred to in Article 37 can be made available to relevant authorities, upon request.

3. In the event of a change of the authorised representative, the detailed arrangements for such change shall address at least the following:

(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.

4. Where the manufacturer is established outside the Union and has not complied with the obligations laid down in Article 30, the authorised representative shall be jointly and severally liable for non-compliance with this Regulation on the same basis as the manufacturer.

*Article 32*

*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 referred to in Article 36.

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

(a) the manufacturer has drawn up the technical documentation referred to in Article 37 and the EU declaration of conformity;

(b) the manufacturer is identified and an authorised representative has been appointed in accordance with Article 31;

(c) the EHR system bears the CE marking of conformity referred to in Article 41 after the conformity assessment procedure has been completed;

(d) the EHR system is accompanied by the information sheet referred to in Article 38 with clear and complete instructions for use, including for its maintenance, in accessible formats.

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

4. Importers shall ensure that, while an EHR system is under their responsibility, the EHR system is not altered in such a way that its conformity with the essential requirements laid down in Annex II and with any requirements adopted pursuant to Article 42 is jeopardised.

5. Where an importer considers or has reason to believe that an EHR system is not or is no longer in conformity with the essential requirements laid down in Annex II and with any requirements adopted pursuant to Article 42, it shall not make that EHR system available on the market, or, if that EHR system was already placed on the market, shall recall or withdraw it, until the EHR system has been brought into conformity. In the event of such recall or withdrawal, 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 of such recall or withdrawal, giving details, in particular, of the non-conformity and of any corrective measures 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 authorities of the Member State in which it 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 30(3) and ensure that the technical documentation referred to in Article 37 can be made available to those authorities, upon request.

7. Importers shall, further to a reasoned request from market surveillance authorities of the Member States concerned, provide them with all the information and documentation necessary to demonstrate the conformity of an EHR system. Importers shall cooperate with those authorities, at their request, and with the manufacturer and, where applicable, with the authorised representative in an official language of the Member State where the market surveillance authority is located. Importers shall cooperate with those authorities, at their request, on any action taken to bring their EHR systems into conformity with the essential requirements in relation to the harmonised software components as laid down in Annex II or to ensure that the EHR systems which are not in conformity with those essential requirements are recalled or withdrawn.

8. Importers shall establish reporting channels and ensure that they are accessible to allow users to submit complaints, and shall keep a register of complaints, of non-conforming EHR systems and EHR system recalls and withdrawals. Importers shall verify whether the channels of complaint established pursuant to Article 30(1), point (n), are publicly available allowing users to submit complaints and to receive any communication concerning any risk related to their health and safety or to other aspects of public interest protection and allowing users to be informed of any serious incident involving an EHR system. Where such channels of complaint were not established, the importers shall establish them and take into account the accessibility needs of vulnerable groups and persons with disabilities.

9. Importers shall investigate complaints and follow up on information received on incidents involving an EHR system they made available on the market. Importers shall register those complaints, any recalls or withdrawals of EHR systems and any corrective measure taken to bring the EHR system into conformity, in the register referred to in Article 30(1), point (o), 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 and follow-up carried out and of the results of the investigation and follow-up.

*Article 33*

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

(d) where applicable, the importer has complied with the requirements set out in Article 32(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 and with any requirements adopted pursuant to Article 42 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 and with any requirements adopted pursuant to Article 42, it shall not make that EHR system available on the market until it has been brought into conformity. 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 or is to be 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 authorities 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 an EHR system into conformity with the essential requirements laid down in Annex II and with any requirements adopted pursuant to Article 42 or to recall or withdraw it.

*Article 34*

*Cases in which obligations of manufacturers of an EHR system apply to other entities or individuals*

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 30 where they:

(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 might be affected; or

(c) modify an EHR system in such a way that it leads to changes in the intended purpose declared by the manufacturer.

*Article 35*

*Identification of economic operators*

Economic operators shall, on request, identify the following to the market surveillance authorities, for 10 years from the date when 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; and

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

## SECTION 3

## CONFORMITY OF THE HARMONISED SOFTWARE COMPONENTS OF EHR SYSTEMS

*Article 36*

*Common specifications*

1. By … [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, adopt common specifications in respect of the essential requirements laid down in Annex II, including a common template and a time limit for implementing those common specifications. Where relevant, those common specifications shall take into account the specificities of medical devices and high-risk AI systems referred to in Article 27(1) and (2), respectively, 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 98(2).

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

   (a) their scope;

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

   (c) their version;

(d) their validity period;

(e) a normative part;

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

3. The common specifications referred to in paragraph 1 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 potential 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 patient safety and the security, confidentiality, integrity 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 25 and 27 that are in conformity with the common specifications referred to in paragraph 1 of this Article shall be considered to be in conformity with the essential requirements covered by those common specifications or parts thereof, laid down in Annex II, and covered by those common specifications or the relevant parts thereof.

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 legal acts, such as Regulation (EU) 2017/745, (EU) 2017/746 or (EU) 2024/1689, the adoption of those common specifications may be preceded by a consultation with the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745 or the European Artificial Intelligence Board established by Article 65 of Regulation (EU) 2024/1689 and the European Data Protection Board (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 legal acts, such as Regulation (EU) 2017/745, (EU) 2017/746 or (EU) 2024/1689, affect EHR systems, the Commission shall ensure that the adoption of those common specifications is preceded by a consultation with the EHDS Board and the EDPB, as applicable.

*Article 37*

*Technical documentation*

1. Manufacturers shall draw up technical documentation before the EHR system is placed on the market or put into service, and shall keep that documentation up to date.

2. The technical documentation referred to in paragraph 1 of this Article shall 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. That technical documentation shall contain, as a minimum, the elements set out in Annex III and a reference to the results obtained from a European digital testing environment referred to in Article 40.

3. The technical documentation referred to in paragraph 1 shall be drawn up in an official language of the Member State concerned or a language that is easily understandable in that Member State. 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 an 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, the manufacturer shall provide such technical documentation or translation within 30 days of the date of the request, 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 of this Article, 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 36.

*Article 38*

*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 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) the intended purpose of the EHR system;

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

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

3. As an alternative to supplying the information sheet referred to in paragraph 1 of this Article with the EHR system, manufacturers may enter the information referred to in paragraph 2 of this Article into the EU database for registration of EHR systems and wellness applications referred to in Article 49.

*Article 39*

*EU declaration of conformity*

1. The EU declaration of conformity referred to in Article 30(1), point (e), shall state that the manufacturer of an EHR system has demonstrated that the essential requirements laid down in Annex II have been fulfilled.

2. Where an EHR system is subject to other Union legal acts in respect of aspects not covered by this Regulation, which also require an EU declaration of conformity by the manufacturer in which it is stated that the fulfilment of the requirements of those legal acts has been demonstrated, a single EU declaration of conformity shall be drawn up in respect of all Union legal acts applicable to the EHR system. That EU declaration of conformity shall contain all the information required for the identification of the Union legal acts to which it 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 States in which the EHR system is made available.

4. Where an EU declaration of conformity is drawn up in a digital format, it shall be made accessible online for the expected lifetime of the EHR system and, in any event, for at least 10 years from the placing on the market or the putting into service of the EHR system.

5. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the harmonised software components of the EHR system with the requirements laid down in this Regulation when it is placed on the market or put into service.

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

*Article 40*

*European digital testing environment*

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

2. Member States shall operate digital testing environments for the assessment of harmonised software components of EHR systems. Such digital testing environments shall comply with the common specifications for the European digital testing environment laid down pursuant to 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 digital testing environments referred to in paragraphs 1 and 2 of this Article for the assessment of harmonised software components of EHR systems. The results of that assessment shall be included in the technical documentation referred to in Article 37. The elements in relation to which the results of the assessment are positive shall be presumed to be in conformity with this Regulation.

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 98(2).

*Article 41*

*CE marking of conformity*

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

2. The CE marking of conformity shall be affixed before placing the EHR system on the market.

3. The CE marking of conformity shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

*Article 42*

*National requirements and reporting to the Commission*

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

2. The national requirements or provisions referred to in paragraph 1 shall not adversely affect the harmonised software components of EHR systems.

3. When Member States adopt requirements or provisions in accordance with paragraph 1, they shall inform the Commission thereof.

## SECTION 4

## MARKET SURVEILLANCE OF EHR SYSTEMS

*Article 43*

*Market surveillance authorities*

1. Regulation (EU) 2019/1020 shall apply to EHR systems in relation to the requirements applicable to, and risks posed by, EHR systems covered by this Chapter.

2. Member States shall designate the market surveillance authority or authorities responsible for the implementation of this Chapter. Member States shall entrust their market surveillance authorities with the necessary powers and shall provide them with the human, financial and technical resources, the equipment and the knowledge necessary for the proper performance of their tasks pursuant to this Regulation. Market surveillance authorities shall be empowered to take the market surveillance measures referred to in Article 16 of Regulation (EU) 2019/1020 to enforce the obligations laid down in this Chapter. Member States shall communicate the identity of the market surveillance authorities they designate to the Commission. The Commission and the Member States shall make that information publicly available.

3. Market surveillance authorities designated pursuant to paragraph 2 of this Article may be the same authorities as the digital health authorities designated pursuant to Article 19. Where a digital health authority carries out tasks of a market surveillance authority, Member States shall ensure that any conflicts of interest are avoided.

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

5. Where a manufacturer or another economic operator fails to cooperate with a market surveillance authority or where the information and documentation they have provided is incomplete or incorrect, the market surveillance authority may take all appropriate measures to prohibit or restrict the relevant EHR system from being made available on the market until the manufacturer or the economic operator concerned cooperates or provides complete and correct information, or to recall or withdraw such EHR system from the market.

6. The market surveillance authorities of the Member States shall cooperate with each other and with the Commission. The Commission shall enable the organisation of exchanges of information necessary for such cooperation.

7. For medical devices, in vitro diagnostic medical devices or high-risk AI systems referred to in Article 27(1) and (2), 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 70 of Regulation (EU) 2024/1689, as applicable.

*Article 44*

*Handling of risks posed by EHR systems and of serious incidents*

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

2. Where the market surveillance authorities of a Member State consider that the non-compliance of the EHR system is not limited to their national territory, they shall inform the Commission and the other Member States' market surveillance authorities of the results of the evaluation referred to in paragraph 1 of this Article and of the corrective action which they have required the economic operator to take pursuant to Article 16(2) of Regulation (EU) 2019/1020.

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

4. The economic operator concerned 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 the market throughout the Union.

5. 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 corrective action referred to in paragraph 2. 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.

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

7. 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 of the Member States where such EHR systems are placed on the market or put into service. That reporting shall also include a description of the corrective action taken or envisaged by the manufacturer. Member States may provide for users of EHR systems placed on the market or put into service to be able to report such incidents.

The reporting required pursuant to the first subparagraph of this paragraph shall be carried out, 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 three days after the manufacturer becomes aware of the serious incident involving the EHR system.

8. The market surveillance authorities referred to in paragraph 7 shall inform the other market surveillance authorities, without delay, of the serious incident and the corrective action taken or envisaged by the manufacturer or required of it to minimise the risk of recurrence of the serious incident.

9. Where its tasks are not performed by the digital health authority, the market surveillance authority shall cooperate with the digital health authority. The market surveillance authority 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, and of any recall or withdrawal of such EHR systems.

10. In the event of incidents putting at risk patient safety or information security, the market surveillance authorities may take immediate action and require the manufacturer of the EHR system concerned, its authorised representative and other economic operators, if applicable, to take immediate corrective action.

*Article 45*

*Handling of non-compliance*

1. Where a market surveillance authority makes a finding of non-compliance, it shall require the manufacturer of the EHR system concerned, its authorised representative and all other relevant economic operators to take, by a specific deadline, adequate corrective action to bring the EHR system into conformity. Such findings of non-compliance include, but are not limited to, the following:

(a) the EHR system is not in conformity with essential requirements laid down in Annex II or with the common specifications referred to in Article 36;

(b) the technical documentation is not available, not complete or not in accordance with Article 37;

(c) the EU declaration of conformity has not been drawn up or has not been drawn up correctly in accordance with Article 39;

(d) the CE marking of conformity has been affixed in breach of Article 41 or has not been affixed;

(e) the registration obligations of Article 49 have not been fulfilled.

2. Where the manufacturer of the EHR system concerned, its authorised representative or any other 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 from being made available on the market of their Member States, or to recall or withdraw the EHR system from that market.

The market surveillance authorities shall inform the Commission and the other Member States' market surveillance authorities, without delay, of those provisional measures. That information shall include all available details, in particular the data necessary for the identification of the non-compliant 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 measures taken by the market surveillance authorities and the arguments put forward by the relevant economic operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to any of the following:

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

(b) shortcomings regarding the common specifications referred to in Article 36.

3. Market surveillance authorities other than the market surveillance authorities initiating the procedure under this Article shall inform without delay the Commission and the other Member States' market surveillance authorities of any measures adopted, 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.

4. Where, within three months of receipt of the information referred to in the second subparagraph of paragraph 2, no objection has been raised by either a market surveillance authority from another Member State or the Commission in respect of a provisional measure taken by a market surveillance authority, that measure shall be deemed justified.

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

*Article 46*

*Union safeguard procedure*

1. Where, under Article 44(2) and Article 45(3), objections are raised against a national measure taken by a market surveillance authority, or where the Commission considers a national measure to be contrary to Union law, the Commission shall without delay enter into consultations with that market surveillance authority and the relevant economic operators and shall evaluate the national measure concerned. On the basis of the results of that evaluation, the Commission shall adopt an implementing decision determining whether the national measure is justified. That implementing decision shall be adopted in accordance with the examination procedure referred to in Article 98(2). The Commission shall address its implementing decision to all Member States and shall immediately communicate it to them and to the relevant economic operators.

2. If the national measure referred to in paragraph 1 is considered justified by the Commission, all Member States concerned 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 referred to in paragraph 1 is considered unjustified by the Commission, the Member State concerned shall revoke that measure.

## SECTION 5

## OTHER PROVISIONS ON INTEROPERABILITY

*Article 47*

*Labelling of wellness applications*

1. Where a manufacturer of a wellness application claims interoperability with an EHR system in relation to the harmonised software components of EHR systems and therefore compliance with the common specifications referred to in Article 36 and essential requirements laid down in Annex II, such wellness application shall be accompanied by a label, clearly indicating its compliance with those specifications and requirements. That label shall be issued by the manufacturer of the wellness application.

2. The label referred to in paragraph 1 shall indicate the following information:

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

(b) a reference to common specifications to demonstrate compliance;

(c) the validity period of the label.

3. The Commission shall, by means of implementing acts, determine the format and content of the label referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

4. The label shall be drawn-up in one or more official languages of the Union or in an easily understandable language determined by the Member State in which the wellness application is placed on the market or put into service.

5. The validity of the label shall not exceed three years.

6. If the wellness application is an integral part of a device or is embedded in a device after it has been put into service, the accompanying label shall be shown in the application itself or placed on that device. Where the wellness application consists only of software, the label shall have a digital format and shall be shown in the application itself. 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 by 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 48*

*Interoperability of wellness applications with EHR systems*

1. Manufacturers of wellness applications may claim interoperability with an EHR system, provided that the relevant common specifications and essential requirements referred to in Article 36 and Annex II, respectively, are met. In the event of such claim, those manufacturers shall duly inform users of the interoperability of such wellness applications and the effects of such interoperability.

2. The interoperability of wellness applications with EHR systems shall not entail the automatic sharing of all or part of the health data from the wellness application with, or automatic transmission of all or part of such data to, the EHR system. The sharing or transmission of such data shall only be possible if it is in accordance with Article 5 and after consent is given by the natural person concerned and interoperability shall be limited exclusively to those purposes. The manufacturers of wellness applications claiming interoperability with an EHR system shall ensure that the natural person concerned is able to choose which categories of health data from the wellness application are to be inserted in the EHR system and the circumstances for the sharing or transmission of those categories of data.

## SECTION 6

## REGISTRATION OF EHR SYSTEMS AND WELLNESS APPLICATIONS

*Article 49*

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

1. The Commission shall establish and maintain a publicly available EU database with data on EHR systems for which an EU declaration of conformity has been issued pursuant to Article 39 and wellness applications for which a label has been issued pursuant to Article 47 (the 'EU database for registration of EHR systems and wellness applications').

2. Before placing on the market or putting into service an EHR system referred to in Article 26 or a wellness application referred to in Article 47, the manufacturer of such EHR system or wellness application or, where applicable, its authorised representative shall enter the required data as referred to in paragraph 4 of this Article into the EU database for registration of EHR systems and wellness applications, including, in the case of EHR systems, the results of the assessment referred to in Article 40.

3. Medical devices, in vitro diagnostic medical devices or high-risk AI systems referred to in Article 27(1) and (2) of this Regulation shall also be registered in the databases established pursuant to Regulation (EU) 2017/745, (EU) 2017/746 or (EU) 2024/1689, as applicable. In such cases, the data to be entered shall also be forwarded to the EU database for registration of EHR systems and wellness applications.

4. The Commission is empowered to adopt delegated acts in accordance with Article 97 to supplement this Regulation by determining the list of required data to be entered into the EU database for registration of EHR systems and wellness applications by the manufacturers of EHR systems and wellness applications pursuant to paragraph 2 of this Article.

# Chapter IV
# Secondary use

## SECTION 1
## GENERAL CONDITIONS WITH REGARD TO SECONDARY USE

*Article 50*
*Applicability to health data holders*

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

   (a) natural persons, including individual researchers;

   (b) legal persons that qualify as microenterprises as defined in Article 2(3) of the Annex to Commission Recommendation 2003/361/EC.

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

3. Member States may provide in their national law that the duties of certain categories of health data holders are to be fulfilled by health data intermediation entities. In that case, the data shall nevertheless be considered as being made available by several health data holders.

4. Member States shall notify to the Commission the national law referred to in paragraphs 2 and 3 by … [date of entry into force of this Regulation + 48 months]. Any subsequent law or amendment affecting such law shall be notified to the Commission without delay.

*Article 51*

*Minimum categories of electronic health data for secondary use*

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

   (a) electronic health data from EHRs;

   (b) data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health;

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

   (d) data on pathogens that impact human health;

(e) healthcare-related administrative data, including on dispensations, reimbursement claims and reimbursements;

(f) human genetic, epigenomic and genomic data;

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

(h) personal electronic health data automatically generated through medical devices;

(i) data from wellness applications;

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

(k) data from population-based health data registries such as public health registries;

(l) data from medical registries and mortality registries;

(m) data from clinical trials, clinical studies, clinical investigations and performance studies subject to Regulation (EU) No 536/2014, Regulation (EU) 2024/1938 of the European Parliament and of the Council[34], Regulation (EU) 2017/745 and Regulation (EU) 2017/746;

(n) other health data from medical devices;

---

[34] Regulation (EU) 2024/1938 of the European Parliament and of the Council of 13 June 2024 on standards of quality and safety for substances of human origin intended for human application and repealing Directives 2002/98/EC and 2004/23/EC (OJ L 2024/1938, 17.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1938/oj).

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

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

(q) health data from biobanks and associated databases.

2. Member States may provide in their national law that additional categories of electronic health data are to be made available for secondary use pursuant to this Regulation.

3. Member States may establish rules for the processing and use of electronic health data containing improvements related to the processing of those data, such as correction, annotation or enrichment, based on a data permit pursuant to Article 68.

4. Member States may introduce stricter measures and additional safeguards at national level aimed at safeguarding the sensitivity and value of the data that fall under paragraph 1, points (f), (g), (i) and (q). Member States shall notify the Commission of those measures and safeguards and, without delay, of any subsequent amendment affecting them.

*Article 52*

*Intellectual property rights and trade secrets*

1. Electronic health data protected by intellectual property rights, trade secrets or covered by the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC of the European Parliament and of the Council[35] or Article 14(11) of Regulation (EC) No 726/2004 of the European Parliament and of the Council[36] shall be made available for secondary use in accordance with the rules laid down in this Regulation.

2. Health data holders shall inform the health data access body of any electronic health data containing content or information protected by intellectual property rights, trade secrets or covered by the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004. Health data holders shall identify which parts of the datasets are concerned and justify the need for the specific protection of the data. Health data holders shall provide that information when communicating to the health data access body the description of the dataset they hold pursuant to Article 60(3) of this Regulation or, at the latest, following a request received from the health data access body.

---

35 Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

36 Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Union procedures for the authorisation and supervision of medicinal products for human use and establishing a European Medicines Agency (OJ L 136, 30.4.2004, p. 1).

3. Health data access bodies shall take all specific appropriate and proportionate measures, including of a legal, organisational and technical nature, they deem necessary to protect the intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) 726/2004. Health data access bodies shall remain responsible for determining whether such measures are necessary and appropriate.

4. When issuing data permits in accordance with Article 68, health data access bodies may make the access to certain electronic health data conditional on legal, organisational and technical measures, which may include contractual arrangements between health data holders and health data users for the sharing of data containing information or content protected by intellectual property rights or trade secrets. The Commission shall develop and recommend non-binding models of contractual terms for such arrangements.

5. Where the granting of access to electronic health data for secondary use entails a serious risk of infringing intellectual property rights, trade secrets or the regulatory data protection right laid down in Article 10(1) of Directive 2001/83/EC or Article 14(11) of Regulation (EC) No 726/2004 which cannot be addressed in a satisfactory manner, the health data access body shall refuse access to the health data applicant to such data. The health data access body shall inform the health data applicant of, and provide to the health data applicant a justification for, that refusal. Health data holders and health data applicants shall have the right to lodge a complaint in accordance with Article 81 of this Regulation.

*Article 53*

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

1. Health data access bodies shall only grant access to electronic health data referred to in Article 51 for secondary use to a health data user where the processing of the data by that health data user is necessary for one of the following purposes:

   (a) the public interest in the areas of public or occupational health, such as activities to protect against serious cross-border threats to health, 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, bodies, offices or agencies, including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates;

   (c) statistics as defined in Article 3, point (1), of Regulation (EU) No 223/2009, such as national, multi-national and Union-level official statistics, related to health or care sectors;

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

(e) scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators, including:

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

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

(f) improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare, based on the electronic health data of other natural persons.

2. Access to electronic health data for the purposes referred to in paragraph 1, points (a), (b) and (c), shall be reserved for public sector bodies and Union institutions, bodies, offices and agencies exercising the tasks conferred on them by Union or national law, including where processing of data for carrying out those tasks is done by a third party on behalf of that public sector body or of Union institutions, bodies, offices and agencies.

*Article 54*

*Prohibited secondary use*

Health data users shall only process electronic health data for secondary use on the basis of and in accordance with the purposes contained in a data permit issued pursuant to Article 68, health data requests approved pursuant to Article 69 or, in situations referred to in Article 67(3), an access approval from the relevant authorised participant in HealthData@EU referred to in Article 75.

In particular, seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 68 or a health data request approved pursuant to Article 69 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' for the purposes of this point, they have to produce legal, social or economic effects or similarly significantly affect those natural persons;

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

(c) carrying out advertising or marketing activities;

(d) developing products or services that may harm individuals, public health or society at large, such as 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, contravene public order or cause a risk for human health;

(e) carrying out activities in conflict with ethical provisions laid down in national law;

## SECTION 2

## GOVERNANCE AND MECHANISMS FOR SECONDARY USE

### *Article 55*

### *Health data access bodies*

1. Member States shall designate one or more health data access bodies responsible for carrying out the tasks and obligations set out in Articles 57, 58 and 59. 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 set out in Article 57 may be distributed 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 territory of that Member State and in other Member States.

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

2. In order to support the effective performance of the tasks and the exercise of the powers of the health data access bodies, Member States shall ensure that each health data access body is provided with the following elements:

(a) the necessary human, financial and technical resources;

(b) the necessary expertise; and

(c) the necessary premises and infrastructure.

Where an assessment by ethics 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 to form part of the health data access body.

3. Member States shall ensure that any conflicts of interest between the organisational parts of health data access bodies performing the different tasks of such bodies is avoided by, for example, providing for organisational safeguards such as segregation between health data access bodies' different functions, including assessing applications, the reception and preparation of datasets, for example pseudonymisation and anonymisation of datasets, and the provision of data in secure processing environments.

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

5. In the performance of their tasks and exercise of their powers, 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.

6. Member States shall inform the Commission of the identity of the health data access bodies designated pursuant to paragraph 1 by … [the date of entry into force of this Regulation + 24 months]. They shall also inform the Commission of any subsequent modification of the identity of those bodies. The Commission and the Member States shall make that information publicly available.

*Article 56*

*Union health data access service*

1. The Commission shall perform the tasks set out in Articles 57 and 59 where the health data holders 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 for the effective performance of the tasks set out in Articles 57 and 59 and the exercise of its duties.

3. Unless otherwise explicitly excluded, references to health data access bodies in this Regulation in relation to the performance of tasks and exercise of duties shall be understood to also apply to the Commission, where the health data holders are Union institutions, bodies, offices or agencies.

*Article 57*

*Tasks of health data access bodies*

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

(a) deciding on health data access applications pursuant to Article 67 of this Regulation, authorising and issuing data permits pursuant to Article 68 of this Regulation to access electronic health data falling within their remit for secondary use and deciding on health data requests submitted pursuant to Article 69 of this Regulation in accordance with this Chapter and Chapter II of Regulation (EU) 2022/868, including with regard to:

(i) providing access to electronic health data to health data users pursuant to a data permit in a secure processing environment in accordance with Article 73;

(ii) monitoring and supervising compliance by health data users and health data holders with the requirements laid down in this Regulation;

(iii) requesting electronic health data referred to in Article 51 from relevant health data holders pursuant to a data permit issued or a health data request approved;

(b) processing electronic health data referred to in Article 51 such as by receiving, combining, preparing and compiling such data when requested from health data holders and the pseudonymisation or anonymisation of those data;

(c) taking all measures necessary to preserve the confidentiality of intellectual property rights, for regulatory data protection and to preserve the confidentiality of trade secrets as provided for in Article 52, taking into account the relevant rights of both the health data holder and health data user;

(d) cooperating with and supervising health data holders to ensure the consistent and accurate implementation of the provisions on data quality and utility label in Article 78;

(e) maintaining a management system to record and process health data access applications, health data requests, decisions on those applications and requests and the data permits issued and health data requests handled, providing at least information on the name of the health data applicant, the purpose of access, the date of issuance, the duration of the data permit and a description of the health data access application or the health data request;

(f) maintaining a public information system to comply with the obligations laid down in Article 58;

(g) cooperating 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;

(h) cooperating at Union and national level and providing advice to the Commission on techniques and best practices for secondary use and the management of electronic health data;

(i) facilitating cross-border access to electronic health data for secondary use hosted in other Member States through HealthData@EU referred to in Article 75 and cooperating closely with each other and with the Commission;

(j) making public, through electronic means:

(i) a national dataset catalogue that includes details about the source and nature of electronic health data, in accordance with Articles 77, 78 and 80, and the conditions for making electronic health data available;

(ii) any health data access application and health data request without undue delay after initial reception;

(iii) all data permits issued or health data requests approved as well as refusal decisions, including their justification, within 30 working days of the issuance, approval or refusal;

(iv) measures related to non-compliance pursuant to Article 63;

(v) results communicated by health data users pursuant to Article 61(4);

(vi) an information system to comply with the obligations laid down in Article 58;

(vii) information, at a minimum on an easily accessible website or web portal, on the connection to HealthData@EU of national contact points for secondary use of a third country, or of a system established at international level by an international organisation, as soon as the third country or the international organisation becomes an authorised participant in HealthData@EU.

(k) fulfilling obligations towards natural persons pursuant to Article 58;

(l) fulfilling any other tasks related to making possible the secondary use of electronic health data in the context of this Regulation.

The national dataset catalogue referred to in point (j)(i) of this paragraph shall also be made available to single information points under Article 8 of Regulation (EU) 2022/868.

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;

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

(c) cooperate with other national competent bodies, including the national competent authorities supervising data altruism organisations under Regulation (EU) 2022/868, the competent authorities under Regulation (EU) 2023/2854 and the national competent authorities under Regulations (EU) 2017/745, (EU) 2017/746 and (EU) 2024/1689, where relevant.

3. Health data access bodies may provide assistance to public sector bodies where those public sector bodies access electronic health data in accordance with Article 14 of Regulation (EU) 2023/2854.

4. Health data access bodies may provide support to a public sector body where it obtains data in the circumstances referred to in Article 15, point (a) or (b), of Regulation (EU) 2023/2854, in accordance with the rules laid down in that Regulation, by providing technical support to process those data or combining them with other data for joint analysis.

*Article 58*

*Obligations of health data access bodies towards natural persons*

1. Health data access bodies shall make information on the conditions under which electronic health data are made available for secondary use publicly available, easily searchable through electronic means and accessible for natural persons. That information shall cover the following:

(a) the legal basis under which access to electronic health data 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;

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

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

(f) who has been granted access to datasets of electronic health data and to which datasets they were granted access and details of the data permit regarding the purposes for processing such data as referred to in Article 53(1);

(g) 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 71 to be exercised through 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 that 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 61(5), the health data access body shall inform the health data holder about that finding. The health data holder shall, under the conditions laid down by national law, inform the natural person or health professional treating the natural person concerned. 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 59*

*Reporting by health data access bodies*

1. Each health data access body shall publish an activity report every two years 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 55(1) shall be responsible for the activity report and request the necessary information from the other health data access bodies. That activity report shall follow a structure agreed by the EHDS Board pursuant to Article 94(2), point (d), and contain at least the following categories of information:

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

(b) 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;

(c) information on audits carried out on health data users to ensure compliance of the processing they carry out in the secure processing environment pursuant to Article 73(1), point (e);

(d) 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 73(3);

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

(f) a description of the health data access body's activities carried out in relation to engagement with and consultation of relevant stakeholders;

(g) revenues from data permits and health data requests;

(h) the average number of days between health data access applications or health data requests and access to data;

(i) the number of data quality labels issued by health data holders, disaggregated per quality category;

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

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

2. The activity report referred to in paragraph 1 shall be submitted to the Commission and the EHDS Board within six months of the end of the second year of the relevant reporting period. The activity report shall be accessible via the Commission's website.

*Article 60*

*Duties of health data holders*

1. Health data holders shall make relevant electronic health data referred to in Article 51 available upon request to the health data access body, in accordance with a data permit issued pursuant to Article 68, or upon a health data request approved pursuant to Article 69.

2. Health data holders 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 and no later than three months from the receipt of the request by the health data access body. In justified cases, the health data access body may extend that period by a maximum of three months.

3. The health data holder shall communicate to the health data access body a description of the dataset it holds in accordance with Article 77. The health data holder shall, at a minimum on an annual basis, check that its dataset description in the national dataset catalogue is accurate and up to date.

4. Where a data quality and utility label accompanies the dataset pursuant to Article 78, the health data holder shall provide sufficient documentation to the health data access body for that body to verify the accuracy of the label.

5. Health data holders of non-personal electronic health data shall provide 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 robust, transparent and sustainable governance and a transparent model of user access.

*Article 61*

*Duties of health data users*

1. Health data users may access and process the electronic health data referred to in Article 51 for secondary use only in accordance with a data permit issued pursuant to Article 68, a health data request approved pursuant to Article 69 or, in situations referred to in Article 67(3), an access approval from the relevant authorised participant in HealthData@EU referred to in Article 75.

2. When processing electronic health data within the secure processing environments referred to in Article 73, health data users shall not provide access to the electronic health data, or make those data available, to third parties not mentioned in the data permit.

3. Health data users shall not re-identify or attempt to re-identify the natural persons to whom the electronic health data obtained by the health data users on the basis of a data permit, a health data request or an access approval by an authorised participant in HealthData@EU relate.

4. Health data users shall make public the results or output of secondary use, including information relevant for the provision of healthcare, within 18 months of the completion of the processing of the electronic health data in the secure processing environment or of having received the response to the health data request referred to in Article 69.

   In justified cases related to the permitted purposes of the processing of electronic health data, the period referred to in the first subparagraph may 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.

   The results or output of secondary use shall contain only anonymous data.

   Health data users shall inform the health data access bodies from which a data permit was obtained about the results or output of secondary use and assist them to make that information public on health data access bodies' websites. Such publication shall be without prejudice to publication rights in scientific journals or other scientific publications.

When health data users use electronic health data in accordance with this Chapter, they shall acknowledge the sources of the electronic health data and the fact that the electronic health data have been obtained in the framework of the EHDS.

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

6. Health data users shall cooperate with health data access bodies in those bodies' performance of their tasks.

*Article 62*

*Fees*

1. Health data access bodies, including the Union health data access service, or trusted health data holders referred to in Article 72 may charge fees for making electronic health data available for secondary use.

The fees shall be in proportion to the cost of making the data available and they shall not restrict competition.

The fees shall cover all or part of the costs related to the procedure for assessing a health data access application or a health data request, for issuing, refusing or amending a data permit pursuant to Articles 67 and 68 or for providing a response to a health data request submitted pursuant to Article 69, including costs related to the consolidation, preparation, pseudonymisation, anonymisation and provision of the electronic health data.

Member States may establish reduced fees for certain types of health data users located in the Union, such as public sector bodies or Union institutions, bodies, offices and agencies with a legal mandate in the field of public health, university researchers or microenterprises.

2. The fees referred to in paragraph 1 of this Article 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. In such cases, the health data holder shall provide an estimate of such costs to the health data access body. Where the health data holder is a public sector body, Article 6 of Regulation (EU) 2022/868 shall not apply. The part of the fees linked to the health data holder's costs shall be paid to the health data holder.

3. Any fees charged to health data users pursuant to this Article shall be transparent and non-discriminatory.

4. Where health data holders and health data users do not agree on the level of the fees within one month of the data permit being issued, the health data access body may set the fees in proportion to the cost of making electronic health data available for secondary use. Where health data holders or health data users disagree with the fee set by the health data access body, they shall have access to dispute settlement bodies in accordance with Article 10 of Regulation (EU) 2023/2854.

5. Before issuing a data permit pursuant to Article 68 or providing a response to a health data request submitted pursuant to Article 69, the health data access body shall inform the health data applicant of the estimated fees. The health data applicant shall be informed about the option to withdraw the health data access application or health data request. If the health data applicant withdraws its application or request, the health data 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 referred to in paragraph 1, fourth subparagraph, of this Article in order to support consistency and transparency between Member States regarding such fee policies and fee structures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

*Article 63*

*Enforcement by health data access bodies*

1. When carrying out their monitoring and supervisory tasks, as referred to in Article 57(1), point (a)(ii), health data access bodies shall have the right to request and receive all the necessary information from health data users and health data holders to verify compliance with this Chapter.

2. 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 concerned shall give the health data user or health data holder concerned the opportunity to state their views within a reasonable period that shall not exceed four weeks.

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

3. With regard to non-compliance by health data users, health data access bodies shall have the power to revoke the data permit issued pursuant to Article 68 and stop without undue delay the affected electronic health data processing operation carried out by the health data user, and shall take appropriate and proportionate measures aimed at ensuring compliant processing by the health data user.

As part of such enforcement measures, the health data access bodies may also, where appropriate, exclude, or initiate proceedings to exclude, in accordance with national law, the health data user concerned from any access to electronic health data within the EHDS in the context of secondary use for a period of up to five years.

4. With regard to non-compliance by health data holders, where a health data holder withholds the electronic health data from health data access bodies with the manifest intention of obstructing the use of electronic health data, or does not respect the deadlines set out in Article 60(2), the health data access body shall have the power to fine the health data holder for each day of delay with a 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 the event 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 to exclude, in accordance with national law, the health data holder concerned from submitting health data access applications pursuant to this Chapter for a period of up to five years. During the period of that exclusion, the health data holder shall remain obliged to make data accessible under this Chapter, where applicable.

5. The health data access body shall communicate the enforcement measures taken pursuant to paragraphs 3 and 4, and the reasons on which they are based, to the health data user or health data holder concerned, without delay, and shall lay down a reasonable period for the health data user or health data holder to comply with those measures.

6. Any enforcement measures taken by the health data access body pursuant to paragraph 3 shall be notified to other health data access bodies through the IT tool referred to in paragraph 7. Health data access bodies may make that information publicly available on their websites.

7. The Commission shall, by means of implementing acts, set out the architecture of an IT tool, as part of the infrastructure of HealthData@EU referred to in Article 75, aimed at supporting and making transparent to other health data access bodies the enforcement measures referred to in this Article, especially periodic penalty payments, the revoking of data permits and exclusions. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

8. The Commission shall issue guidelines, by … [the date of entry into force of this Regulation + 84 months], in close cooperation with the EHDS Board, on enforcement measures including periodic penalty payments and other measures to be taken by the health data access bodies.

*Article 64*

*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 is effective, proportionate and dissuasive in each individual case.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, enforcement measures referred to in Article 63(3) and (4). Health data access bodies shall decide whether to impose an administrative fine and the amount of the administrative fine in each individual case by giving due regard to the following circumstances:

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

   (b) whether any penalties or administrative fines have already been imposed 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 that health data user pursuant to Article 67(2), point (g), and Article 67(4);

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

(g) the degree of cooperation of the health data holder or health data user with the health data access body as regards remedying the infringement and mitigating its possible adverse effects;

(h) the manner in which the health data access body became aware of the infringement, in particular whether, and to what extent, the health data user notified it of the infringement;

(i) compliance with any enforcement measures referred to in Article 63(3) and (4) which have been ordered previously against the controller or processor concerned with regard to the same subject matter;

(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, through the infringement.

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

4. In accordance with paragraph 2 of this Article, infringements of the duties of the health data holder or health data user pursuant to Article 60 and Article 61(1), (5) and (6) shall be subject to administrative fines of a maximum of EUR 10 000 000 or, in the case of an undertaking, of a maximum of 2 % of its total worldwide annual turnover in the preceding financial year, whichever is higher.

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

(a) health data users processing electronic health data obtained via a data permit issued pursuant to Article 68 for the uses referred to in Article 54;

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

(c) re-identifying or attempting to re-identify the natural persons to whom the electronic health data obtained by the health data users on the basis of a data permit or a health data request pursuant to Article 61(3) relate;

(d) non-compliance with enforcement measures taken by the health data access body pursuant to Article 63(3) and (4).

6. Without prejudice to the powers of health data access bodies pursuant to Article 63, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and public sector bodies established in that Member State.

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

8. Where the legal system of a Member State does not provide for administrative fines, this Article may be applied in a manner that, in accordance with its 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. The Member State concerned shall notify the Commission of the provisions of the laws which it adopts pursuant to this paragraph by … [the date of entry into force of this Regulation + 48 months] and, without delay, of any subsequent law amending such provisions or amendments affecting such provisions.

*Article 65*

*Relationship with supervisory authorities under Regulation (EU) 2016/679*

The supervisory authority or authorities responsible for monitoring and enforcing the application of Regulation (EU) 2016/679 shall also be competent for monitoring and enforcing the application of the right to opt out from the processing of personal electronic health data for secondary use pursuant to Article 71. Those supervisory authorities shall be empowered to impose administrative fines up to the amount referred to in Article 83 of Regulation (EU) 2016/679.

The supervisory authorities referred to in the first paragraph of this Article and the health data access bodies referred to in Article 55 of this Regulation shall, where relevant, cooperate in the enforcement of this Regulation, within the remit of their respective competences. The relevant provisions of Regulation (EU) 2016/679 shall apply *mutatis mutandis*.

## SECTION 3

## ACCESS TO ELECTRONIC HEALTH DATA FOR SECONDARY USE

### *Article 66*

### *Data minimisation and purpose limitation*

1. Where health data access bodies receive a health data access application, they shall ensure that access is only provided to electronic health data that are adequate, relevant and limited to what is necessary in relation to the purpose of processing indicated in the health data access application by the health data user and in line with the data permit issued pursuant to Article 68.

2. 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 accordance with Article 68(1), point (c), 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 an entity that acts as a trusted third party in accordance with national law.

*Article 67*

*Health data access applications*

1. A natural or legal person may submit a health data access application for the purposes referred to in Article 53(1) to a health data access body.

2. The health data access application shall include:

   (a) the health data applicant's identity, a description of that health data applicant's professional functions and activities, including the identity of the natural persons who would have access to the electronic health data if a data permit were issued; the health data applicant shall notify the health data access body of any update of the list of natural persons;

   (b) the purposes referred to in Article 53(1) for which access to data is applied for;

(c) a detailed explanation of the intended use of the electronic health data and expected benefit related to that use and how that benefit would contribute to the purposes referred to in Article 53(1);

(d) a description of the requested electronic health data, including their scope, time range, format, sources and, where possible, the geographical coverage where such data are requested from health data holders in several Member States or from authorised participants in HealthData@EU referred to in Article 75;

(e) a description explaining whether the electronic health data need to be made available in a pseudonymised or anonymised format; in the case of a pseudonymised format, a justification as to why the processing cannot be carried out using anonymised data;

(f) where the health data applicant intends to bring datasets already held by that health data applicant into the secure processing environment, a description of those datasets;

(g) a description of the safeguards, which are to be 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;

(h) a justified indication of the period during which the electronic health data are needed for processing in a secure processing environment;

(i) a description of the tools and computing resources needed for a secure processing environment;

(j) where applicable, information on any assessment of ethical aspects of the processing, required under national law, which may serve to replace the health data applicant's own ethics assessment;

(k) where the health data applicant intends to make use of an exception under Article 71(4), the justification required by national law pursuant to that Article.

3. When seeking access to electronic health data held by health data holders established in more than one Member State or from the relevant authorised participants in HealthData@EU referred to in Article 75, the health data applicant shall submit a single health data access application through the health data access body of the Member State where the main establishment of the health data applicant is located, through the health data access body of the Member State in which one of those health data holders is established or through the services provided by the Commission in HealthData@EU referred to in Article 75. The health data access application shall be automatically forwarded to the relevant authorised participants in HealthData@EU and to the health data access bodies of the Member States where the health data holders identified in the health data access application are established.

4. When seeking access to the personal electronic health data in a pseudonymised format, the health data applicant shall provide, together with the health data access application, a description of how the processing would comply with applicable Union and national law on data protection and privacy, in particular with Regulation (EU) 2016/679 and, more specifically, with Article 6(1) thereof.

5. Public sector bodies and Union institutions, bodies, offices and agencies shall provide the same information as required under paragraphs 2 and 4, except for paragraph 2, point (h), in which case they shall submit instead 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 68*

*Data permit*

1. For the purposes of granting access to electronic health data, the health data access bodies shall assess whether all the following criteria are fulfilled:

   (a) the purposes described in the health data access application correspond to one or more of the purposes listed in Article 53(1);

   (b) the requested data are necessary, adequate and proportionate for the purposes described in the health data access application, taking into account data minimisation and purpose limitation requirements provided for in Article 66;

(c) the processing complies with Article 6(1) of Regulation (EU) 2016/679 and, in the case of pseudonymised data, there is sufficient justification that the purpose cannot be achieved with anonymised data;

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

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

(f) the information on the assessment of ethical aspects of the processing, referred to in Article 67(2), point (j), where applicable, complies with national law;

(g) where the health data applicant intends to make use of an exception under Article 71(4), the justification required by national law adopted pursuant to that Article has been provided;

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

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

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

(b) the risk of undermining the confidentiality of data in governmental databases of regulatory authorities.

3. Where the health data access body concludes that the requirements in paragraph 1 are fulfilled and the risks referred to in paragraph 2 are sufficiently mitigated, the health data access body shall grant access to electronic health data by issuing a data permit. Health data access bodies shall refuse all health data access applications where the requirements in this Chapter are not fulfilled.

Where the requirements for issuing a data permit are not met, but the requirements to provide a response in an anonymised statistical format under Article 69 are, the health data access body may decide to provide such response, on condition that providing that response would mitigate the risks and, if the purpose of the health data access application can be fulfilled in this manner, that the health data applicant agrees to receiving a response in an anonymised statistical format under Article 69.

4. By way of derogation from Regulation (EU) 2022/868, the health data access body shall issue or refuse a data permit within three months of receiving a complete health data access application. If the health data access body finds that the health data access application is incomplete, it shall notify the health data applicant, who shall be given the possibility of completing that application. If the health data applicant does not complete the health data access application within four weeks, the data permit shall not be issued.

The health data access body may extend the period for responding to a health data access application by three additional months where necessary, taking into account the urgency and complexity of the health data access application and the volume of health data access applications submitted for decision. In such cases, the health data access body shall notify the health data applicant as soon as possible that more time is needed for examining the health data access application, together with the reasons for the delay.

5. When handling a health data access application for cross-border access to electronic health data referred to in Article 67(3), health data access bodies and relevant authorised participants in HealthData@EU referred to in Article 75 shall remain responsible for adopting decisions to grant or refuse access to electronic health data within their remit in accordance with this Chapter.

The health data access bodies and authorised participants in HealthData@EU concerned shall inform each other of their decisions. They may take that information into consideration when deciding on granting or refusing access to electronic health data.

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

6. Member States shall provide for an accelerated health data access 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 electronic health data is to be carried out for the purposes established in Article 53(1), points (a), (b) and (c).

When such accelerated procedure applies, the health data access body shall issue or refuse a data permit within two months of receiving a complete health data access application. The health data access body may extend the period for responding to a health data access application by one additional month where necessary.

7. 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 two months of receiving them from the health data holders, unless the health data access body specifies that the data are to be provided within a longer specified timeframe.

8. In cases referred to in paragraph 5, first subparagraph, the health data access bodies and authorised participants in HealthData@EU which issued a data permit or access approval, respectively, may decide to provide access to the electronic health data in the secure processing environment provided by the Commission as referred to in Article 75(9).

9. Where the health data access body refuses to issue a data permit, it shall provide a justification for that refusal to the health data applicant.

10 When issuing a data permit, the health data access body shall set out in that data permit the general conditions applicable to the health data user. The data permit shall contain the following:

(a) the categories, specification and format of the electronic health data to be accessed, which are covered by the data permit, including their sources and an indication of whether the electronic health data are to be accessed in a pseudonymised format in the secure processing environment;

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

(c) where a mechanism to implement an exception is provided for and applicable under Article 71(4), information on whether it has been applied and the reason for the related decision;

(d) the identity of authorised persons, in particular the identity of the principal investigator, with access rights to the electronic health data in the secure processing environment;

(e) the duration of the data permit;

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

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

(h) any specific conditions.

11. Health 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 issued to them on the basis of this Regulation.

12. A data permit shall be issued for the duration necessary to fulfil the requested purposes and that duration shall not exceed 10 years. That duration may be extended once for a period which does not exceed 10 years, at the request of the health data user, based on arguments and documents to justify that extension which shall be provided one month before the expiry of the data permit. The health data access body may charge fees which increase to reflect the costs and risks of storing electronic health data for a period 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 a 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 six months of the expiry of the data permit. At the request of the health data user, the formula for the creation of the requested dataset may be stored by the health data access body.

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

14. The Commission may, by means of an 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 98(2).

*Article 69*

*Health data request*

1. The health data applicant may submit a health data request for the purposes referred to in Article 53 with the aim of obtaining a response only in an anonymised statistical format. A health data access body shall not provide a response 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 that response.

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

   (a) the identity of the health data applicant and a description of that health data applicant's professional functions and activities;

   (b) a detailed explanation of the intended use of the electronic health data, including the purposes referred to in Article 53(1) for which the health data request is submitted;

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

(d) a description of the statistical content;

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

(f) a description of how the processing would comply with Article 6(1) of Regulation (EU) 2016/679 or Article 5(1) and Article 10(2) of Regulation (EU) 2018/1725;

(g) where the health data applicant intends to make use of an exception under Article 71(4), the justification required in that regard by national law pursuant to that Article.

3. The health data access body shall assess if the health data request is complete and take into account the risks referred to in Article 68(2).

4. The health data access body shall assess the health data request within three months of receipt of the request and, where possible, subsequently provide the response to the health data user within a further three months.

*Article 70*

*Templates to support access to electronic health data for secondary use*

By … [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, set out the templates for the health data access application, the data permit and the health data request referred to in Articles 67, 68 and 69, respectively. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

*Article 71*

*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 providing any reason, from the processing of personal electronic health data relating to them for secondary use under this Regulation. The exercise of that right shall be reversible.

2. Member States shall provide for an accessible and easily understandable opt-out mechanism to exercise the right established in paragraph 1, whereby natural persons may explicitly state that they do not wish to have their personal electronic health data processed for secondary use.

3. Once natural persons have exercised the right to opt out, and where personal electronic health data relating to them can be identified in a dataset, personal electronic health data relating to those natural persons shall not be made available or otherwise processed pursuant to data permits issued under Article 68 or health data requests under Article 69 approved after the natural person has exercised the right to opt out.

   The first subparagraph of this paragraph shall not affect the processing for secondary use of personal electronic health data relating to those natural persons pursuant to data permits or health data requests that were issued or approved before the natural persons exercised their right to opt out.

4. By way of exception from the right to opt out provided for in paragraph 1, a Member State may provide in its national law for a mechanism to make data for which a right to opt out has been exercised available provided that all the following conditions are fulfilled:

(a) the health data access application or health data request is submitted by a public sector body or a Union institution, body, office or agency with a mandate to carry 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 the processing of those data is necessary for any of the following purposes:

(i) the purposes referred to in Article 53(1), points (a), (b) and (c);

(ii) scientific research for important reasons of public interest;

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

(c) the health data applicant has provided the justification referred to in Article 68(1), point (g), or in Article 69(2), point (g).

The national law providing for such a mechanism shall provide for specific and suitable measures in order to protect the fundamental rights and the personal data of natural persons.

Where a Member State has provided in its national law for the possibility to request access to data for which a right to opt out has been exercised and the conditions referred to in the first subparagraph of this paragraph are fulfilled, those data may be included when carrying out the tasks under Article 57(1), points (a)(i), (a)(iii) and (b).

5. The rules on any mechanism to implement exceptions provided for under paragraph 4 by way of exception from paragraph 1 shall respect the essence of the fundamental rights and freedoms and shall be a necessary and proportionate measure in a democratic society to fulfil purposes of public interest in the area of legitimate scientific and societal objectives.

6. Any processing carried out in accordance with a mechanism to implement exceptions provided for under paragraph 4 of this Article shall comply with the requirements of this Chapter, in particular the prohibition on re-identifying or attempting to re-identify natural persons in accordance with Article 61(3). Any legislative measure providing for a mechanism in national law as referred to in paragraph 4 of this Article shall include specific provisions for the safety, and the protection of the rights, of natural persons.

7. Member States shall notify without delay the Commission of the provisions of their national law which they adopt pursuant to paragraph 4 and of any subsequent amendment affecting them.

8. When the purposes of the processing of personal electronic health data by a health data holder do not or no longer require the identification of a data subject by the controller, that 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 72*

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

1. Where a health data access body receives a health data access application pursuant to Article 67 or a health data request pursuant to Article 69 that only covers electronic health data held by a trusted health data holder designated in accordance with paragraph 2 of this Article, the procedure set out in paragraphs 4 to 6 of this Article shall apply.

2. Member States may establish a procedure whereby health data holders can apply to be designated as trusted health data holders, provided the health data holders meet the following conditions:

   (a) they are able to provide access to health data through a secure processing environment that complies with Article 73;

   (b) they have the necessary expertise to assess health data access applications and health data requests;

   (c) they provide the necessary guarantees to ensure compliance with this Regulation.

Member States shall designate trusted health data holders following an assessment of the fulfilment of those 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 those conditions.

Health data access bodies shall indicate the trusted health data holders in the dataset catalogue referred to in Article 77.

3. Health data access applications and health 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.

4. Following receipt of a health data access application or health data request pursuant to paragraph 3 of this Article, the trusted health data holder shall assess the health data access application or health data request against the criteria listed in Article 68(1) and (2) or Article 69(2) and (3), as applicable.

5. The trusted health data holder shall submit the assessment it carries out pursuant to paragraph 4, accompanied by a proposal for decision, to the health data access body within two months of receipt of the health data access application or health data request from the health data access body. Within two months of receipt of the assessment, the health data access body shall issue a decision on the health data access application or health data request. The health data access body shall not be bound by the proposal submitted by the trusted health data holder.

6. Following the health data access body's decision to issue the data permit or to approve the health data request, the trusted health data holder shall carry out the tasks referred to in Article 57(1), points (a)(i) and (b).

7. The Union health data access service referred to in Article 56 may designate health data holders that are Union institutions, bodies, offices or agencies which comply with the conditions laid down in paragraph 2, first subparagraph, points (a), (b) and (c), of this Article as trusted health data holders. Where it does so, paragraph 2, third and fourth subparagraphs, and paragraphs 3 to 6 of this Article shall apply *mutatis mutandis*.

*Article 73*

*Secure processing environment*

1. Health data access bodies shall provide access to electronic health data pursuant to a data permit only through a secure processing environment which is subject to technical and organisational measures and security and interoperability requirements. In particular, the secure processing environment shall comply with the following security measures:

   (a) the restriction of access to the secure processing environment to authorised natural persons listed in the data permit issued pursuant to Article 68;

   (b) the minimisation of 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) the limitation of 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) ensuring 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) the keeping of identifiable logs of access to and activities in the secure processing environment for the period necessary to verify and audit all processing operations in that environment; logs of access shall be kept for at least one year;

(f) ensuring compliance and monitoring the security measures referred to in this paragraph to mitigate potential security threats.

2. Health data access bodies shall ensure that electronic health data from health data holders in the format specified in the data permit can be uploaded by those health data holders and can be accessed by the health data user in a secure processing environment.

Health data access bodies shall review the electronic health data included in a download request to ensure that 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. Health data access bodies shall ensure that audits of the secure processing environments are carried out on a regular basis, including by third parties, and shall take corrective action for any shortcomings, risks or vulnerabilities identified by those audits in the secure processing environments.

4. Where recognised data altruism organisations under Chapter IV of Regulation (EU) 2022/868 process personal electronic health data using a secure processing environment, those environments shall also comply with the security measures set out in paragraph 1, points (a) to (f), of this Article.

5. By … [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, lay down the technical, organisational, information security, confidentiality, data protection and interoperability requirements for the secure processing environments, including with regard to the technical characteristics and tools available to the health data user within the secure processing environments. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

*Article 74*

*Controllership*

1. The health data holder shall be deemed controller for the making available of personal electronic health data requested pursuant to Article 60(1) to the health data access body.

   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 second subparagraph of this paragraph, the health data access body shall be deemed to act as a processor on behalf of the health data user acting as a controller for the processing of the personal electronic health data pursuant to a data permit issued under Article 68 in the secure processing environment when providing data through such environment or for the processing of such data pursuant to a health data request approved under Article 69 for a response to be generated.

2. In situations referred to in Article 72(6), the trusted health data holder shall 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 health data request. The trusted health data holder shall be deemed to act as a processor on behalf of the health data user when providing data through a secure processing environment.

3. The Commission may, by means of implementing acts, establish a template for agreements between controllers and processors under paragraphs (1) and (2) of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 98(2).

## SECTION 4

## CROSS-BORDER INFRASTRUCTURE FOR SECONDARY USE

*Article 75*

*HealthData@EU*

1. Each Member State shall designate one national contact point for secondary use. That national contact point for secondary use shall be an organisational and technical gateway, enabling and responsible for the making available of electronic health data for secondary use in a cross-border context. The national contact point for secondary use may be the coordinator health data access body pursuant to Article 55. Each Member State shall inform the Commission of the name and contact details of the national contact point for secondary use by … [the date of entry into force of this Regulation + 24 months]. The Commission and the Member States shall make that information publicly available.

2. The Union health data access service shall act as the contact point of the Union's institutions, bodies, offices and agencies for secondary use and shall be responsible for making electronic health data available for secondary use.

3. The national contact points for secondary use referred to in paragraph 1 and the Union health data access service referred to in paragraph 2 shall connect to the cross-border infrastructure for secondary use, namely HealthData@EU. The national contact points for secondary use and the Union health data access service shall facilitate the cross-border access to electronic health data for secondary use for different authorised participants in HealthData@EU. The national contact points for secondary use shall cooperate closely with each other and with the Commission.

4. Health-related research infrastructures or similar infrastructures whose functioning is based on Union law and which provide support for the use of electronic health data for research, policy making, statistical, patient safety or regulatory purposes may become authorised participants in HealthData@EU and connect to it.

5. Third countries or international organisations may become authorised participants in HealthData@EU where they comply with the rules of this Chapter and provide access to health data users located in the Union, on equivalent terms and conditions, to the electronic health data available to their health data access bodies, subject to compliance with Chapter V of Regulation (EU) 2016/679.

The Commission may, by means of implementing acts, determine that a national contact point for secondary use of a third country or a system established at international level by an international organisation is compliant with the requirements of HealthData@EU for the purposes of secondary use of health data, is compliant with this Chapter and provides access to health data users located in the Union to the electronic health data it has access to on terms and conditions equivalent to those of HealthData@EU. Compliance with those legal, organisational, technical and security requirements, including with the requirements for secure processing environments provided for in Article 73 of this Regulation, shall be checked under the control of the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2) of this Regulation. The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available.

6. Each national contact point for secondary use and each authorised participant in HealthData@EU 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 HealthData@EU and to allow them to connect to it.

7. 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 and authorised participants in HealthData@EU and the central platform referred to in paragraph 8.

8. 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 HealthData@EU. The Commission shall only process electronic health data on behalf of the controllers as a processor.

9. Where requested by two or more national contact points for secondary use, the Commission may provide a secure processing environment which is compliant with the requirements of Article 73 for data from more than one Member State. Where two or more national contact points for secondary use or authorised participants in HealthData@EU 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.

10. The national contact points for secondary use shall act as joint controllers of the processing operations carried out in HealthData@EU in which they are involved and the Commission shall act as processor on behalf of those national contact points for secondary use, without affecting the tasks of health data access bodies prior to and following those processing operations.

11. Member States and the Commission shall seek to ensure that HealthData@EU is interoperable with other relevant common European data spaces as referred to in Regulations (EU) 2022/868 and (EU) 2023/2854.

12. By … [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, set out:

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

(b) conditions and compliance checks required to be able 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 infringements;

(c) the minimum criteria that need to be met by the national contact points for secondary use and the authorised participants in HealthData@EU;

(d) the responsibilities of the controllers and processors participating in HealthData@EU;

(e) the responsibilities of the controllers and processors for the secure processing environment managed by the Commission;

(f) common specifications for the architecture of HealthData@EU and for its interoperability with other common European data spaces.

The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 98(2).

13. Where there is a positive outcome of the compliance check referred to in paragraph 5 of this Article, the Commission may, by means of implementing acts, take decisions to connect individual authorised participants to HealthData@EU. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

*Article 76*

*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 with which the health data holder for the specific registry or database is registered shall be competent to decide on health 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 decides on the health data access applications to be used to provide access to electronic health data shall be the health data access body of 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 or databases may designate a coordinator to ensure the provision of data from the registries' or databases' network for secondary use. The health data access body of the Member State in which the coordinator of the network is established shall be competent to decide on the health data access applications to be used 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 77*

*Dataset description and dataset catalogue*

1. Health data access bodies shall, through a publicly available and standardised machine-readable dataset catalogue, provide a description in the form of metadata of the available datasets and their characteristics. The description of each dataset shall include information concerning the source, scope, main characteristics, and nature of the electronic health data in the dataset and the conditions for making those data available.

2. The dataset descriptions in the national dataset catalogue shall be available in at least one official language of the Union. The dataset catalogue for Union institutions, bodies, offices and agencies provided by the Union health data access service shall be available in all official languages of the Union.

3. The dataset catalogue shall be made available to single information points established or designated under Article 8 of Regulation (EU) 2022/868.

4. By … [two years from the date of entry into force of this Regulation], the Commission shall, by means of implementing acts, set out the minimum elements health data holders are to provide for datasets and the characteristics of those elements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

*Article 78*

*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 covering 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: metadata, support documentation, the data dictionary, the format and standards used, the source of the data and, where applicable, the data model;

   (b) for assessment of technical quality: completeness, uniqueness, accuracy, validity, timeliness and consistency of the data;

(c) for data quality management processes: the level of maturity of the data quality management processes, including review and audit processes, and bias examination;

(d) for assessment of coverage: the period, population coverage and, where applicable, representativity of the population sampled, and the average timeframe in which a natural person appears in a dataset;

(e) for information on access and provision: the time between the collection of the electronic health data and their addition to the dataset and the time needed to provide electronic health data following the issuing of a data permit or a health data request approval;

(f) for information on data modifications: merging and adding data to an existing dataset, including links with other datasets.

4. Where a health data access body has reason to believe that a data quality and utility label might be inaccurate, it shall assess whether the dataset covered by the label meets the quality requirements forming part of the elements of the data quality and utility label as referred to in paragraph 3 and, in the event the dataset does not meet the quality requirements, shall revoke the label.

5. The Commission is empowered to adopt delegated acts in accordance with Article 97 to amend this Regulation by modifying, adding or removing elements to be covered by the data quality and utility label provided for in paragraph 3.

6. By … [two years from the date of entry into force of this Regulation], 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 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2) of this Regulation. Those implementing acts shall take into account the requirements in Article 10 of Regulation (EU) 2024/1689 and any adopted common specifications or harmonised standards supporting those requirements, where applicable.

*Article 79*

*EU dataset catalogue*

1. The Commission shall establish an EU dataset catalogue connecting the national dataset catalogues established by the health data access bodies in each Member State as well as the dataset catalogues of authorised participants in HealthData@EU.

2. The EU dataset catalogue, the national dataset catalogues and the dataset catalogues of authorised participants in HealthData@EU shall be made publicly available.

*Article 80*

*Minimum specifications for datasets of high impact*

The Commission may, by means of implementing acts, determine the minimum specifications for datasets of high impact for secondary use, 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 98(2).

## SECTION 6

## COMPLAINTS

*Article 81*

*Right to lodge a complaint with a health data access body*

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint in relation to the provisions laid down in this Chapter, individually or, where relevant, collectively, with a health data access body, provided that their rights or interests are negatively affected.

2. The health data access body with which the complaint has been lodged shall inform the complainant of the progress made in dealing with the complaint and of the decision taken on the complaint.

3. Health data access bodies shall provide easily accessible tools for the submission of complaints.

4. Where the complaint concerns the rights of natural persons pursuant to Article 71 of this Regulation, the complaint shall be transmitted to the competent supervisory authority under Regulation (EU) 2016/679. The relevant 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 V
# Additional actions

*Article 82*
*Capacity building*

The Commission shall support the sharing of best practices and expertise to build capacity within Member States to strengthen digital health systems for primary use and secondary use taking into account the specific circumstances of the different categories of stakeholders involved. To support that capacity building, the Commission shall in close cooperation and consultation with Member States establish indicators for self-assessment for primary use and secondary use.

*Article 83*

*Training programmes and information for health professionals*

1. Member States shall develop and implement or provide access to training programmes and provide access to information for health professionals in order for them to understand and effectively carry out their role in the primary use of and in the accessing of electronic health data, including in relation to Articles 11, 13 and 16. The Commission shall support Member States in that regard.

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

*Article 84*

*Digital health literacy and digital health access*

1. Member States shall promote and support digital health literacy and the development of relevant competences and skills for patients. The Commission shall support Member States in this regard. Awareness-raising campaigns or programmes shall aim, in particular, to inform patients and the public at large about primary use and secondary use in the framework of the EHDS, including the rights arising from it, as well as the advantages, risks and potential gains for science and society of primary use and secondary use.

2. The awareness-raising campaigns and programmes referred to in paragraph 1 shall be tailored to the needs of specific groups and shall be developed, reviewed and, where necessary, updated.

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

*Article 85*

*Additional requirements for public procurement and Union funding*

1. 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 15, 23, 36, 73, 75 and 78 for public procurement procedures 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 86*

*Storage of personal electronic health data for primary use*

In accordance with the general principles of Union law, which include the fundamental rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, Member States shall ensure that a particularly high level of protection and security is in place 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, taking into account the national context, that, in cases where personal electronic health data are processed by healthcare providers for the provision of healthcare or by the national contact points for digital health connected to MyHealth@EU, the storage of personal electronic health data referred to in Article 14 of this Regulation for the purpose of primary use be located within the Union, in compliance with Union law and international commitments.

*Article 87*

*Storage of personal electronic health data by health data access bodies and secure processing environments*

1. Health data access bodies, trusted health data holders and the Union health data access service shall store and process personal electronic health data in the Union when performing pseudonymisation, anonymisation and any other personal data processing operations referred to in Articles 67 to 72, through secure processing environments within the meaning of Article 73 and Article 75(9) or through HealthData@EU. That requirement shall apply to any entity performing those tasks on behalf of such bodies, holders or service.

2. By way of exception from paragraph 1 of this Article, the data referred to in that paragraph may be stored and processed in a third country, or a territory or one or more specified sectors within that third country, where such country, territory or sector is covered by an adequacy decision adopted pursuant to Article 45 of Regulation (EU) 2016/679.

*Article 88*

*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 under a data permit issued pursuant to Article 68 of this Regulation or a health data request approved pursuant to Article 69 of this Regulation, to authorised participants in a third country or to an international organisation, and based on a natural person's electronic health data falling within one of the categories referred to in Article 51, shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation (EU) 2022/868 where the transfer of such non-personal electronic data 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 to whom those data relate, 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 of this Article shall be detailed in a delegated act referred to in Article 5(13) of Regulation (EU) 2022/868.

*Article 89*

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

1. Digital health authorities, health data access bodies, authorised participants in the cross-border infrastructures provided for in Articles 23 and 75 and health data users shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent the transfer of non-personal electronic health data held in the Union to a third country or an international organisation, including for governmental access in a third country, 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 health 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, where a digital health authority, a health data access body or a health data user is the addressee of a decision or judgment of a third-country court or tribunal or of a decision of a third-country administrative authority requiring them to transfer or to give access to non-personal data within the scope of this Regulation held in the Union, and compliance with such a decision or judgment would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, the transfer to, or accessing of such data by, that third-country court, tribunal or administrative authority shall only take place or be provided where:

(a) the third-country legal 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 by the national law of the 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, a digital health authority, a health data access body or a data altruism organisation 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 and health data users shall inform the health 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 compliance is necessary to preserve the effectiveness of the law enforcement activity.

*Article 90*

*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 Article 9(4) of Regulation (EU) 2016/679, in addition to the requirements laid down in Article 24(3) and Article 75(5) of this Regulation and in Chapter V of Regulation (EU) 2016/679.

*Article 91*

*Health data access applications and health data requests from third countries*

1. Without prejudice to Articles 67, 68 and 69, health data access applications and health data requests submitted by a health data applicant established in a third country shall be considered eligible by health data access bodies and the Union health data access service if the third country concerned:

   (a) is an authorised participant on the basis of having a national contact point for secondary use covered by an implementing act referred to in Article 75(5); or

   (b) allows Union health data applicants access to electronic health data in that third country under conditions that are not more restrictive than those provided for in this Regulation, and therefore such access is covered by an implementing act referred to in paragraph 2 of this Article.

2. By means of implementing acts, the Commission may determine that a third country meets the requirement set out in paragraph 1, point (b), of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2). The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available.

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

Where the Commission considers that a third country no longer meets the requirement laid down in paragraph 1, point (b), of this Article, it shall adopt an implementing act repealing the implementing act referred to in paragraph 2 of this Article relating to that third country that benefits from access. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

# Chapter VI
# European governance and coordination

*Article 92*
*European Health Data Space Board*

1. A European Health Data Space Board (the '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, namely 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.

2. 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.

3. Market surveillance authorities referred to in Article 43, the EDPB and the European Data Protection Supervisor, the European Medicines Agency, the European Centre for Disease Prevention and Control and the European Union Agency for Cybersecurity (ENISA) shall be invited to attend the meetings, where relevant according to the EHDS Board.

4. The EHDS Board may invite national authorities, experts and observers as well as Union institutions, bodies, offices and agencies, in addition to those referred to in paragraph 3, and research infrastructures and other similar infrastructures to attend its meetings.

5. The EHDS Board may cooperate with external experts where appropriate.

6. Depending on the functions related to the use of electronic health data, the EHDS Board may work in subgroups for certain topics, in which digital health authorities or health data access bodies shall be represented. Those subgroups shall support the EHDS Board with specific expertise and may have joint meetings, as required.

7. The EHDS Board shall adopt its 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 referred to in paragraph 6 of this Article and the cooperation of the EHDS Board with the stakeholder forum referred to in Article 93.

   The EHDS Board shall adopt decisions by consensus as far as possible. If a consensus cannot be reached, the EHDS Board shall adopt decisions by a majority of two-thirds of the Member States.

8. The EHDS Board shall cooperate with other relevant bodies, entities and experts, such as the European Data Innovation Board established by Article 29 of Regulation (EU) 2022/868, competent authorities designated in accordance with Article 37 of Regulation (EU) 2023/2854, supervisory bodies designated in accordance with Article 46b of Regulation (EU) No 910/2014, the EDPB established by Article 68 of Regulation (EU) 2016/679, cybersecurity bodies, including ENISA, and the European Open Science Cloud, with a view to reaching advanced solutions towards findable, accessible, interoperable and reusable (FAIR) data usage in research and innovation.

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

10. The EHDS Board shall publish its meeting dates and the minutes of its deliberations, and publish an activity report every two years.

11. The Commission shall, by means of implementing acts, adopt the necessary measures for the establishment and operation of the EHDS Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

*Article 93*

*Stakeholder forum*

1. A stakeholder forum is hereby established for the purpose of facilitating the exchange of information and promoting cooperation among stakeholders in relation to the implementation of this Regulation.

2. The stakeholder forum shall have a balanced composition and be composed of relevant stakeholders, including representatives of patient organisations, health professionals, industry, consumer organisations, scientific researchers and academia, and shall represent their views. Where commercial interests are represented in the stakeholder forum, the representation of such interests shall be based on a balanced combination of large companies, small and medium-sized enterprises and start-ups. The tasks of the stakeholder forum shall encompass equally primary use and secondary use.

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 stakeholder forum shall make an annual declaration of interests which shall be made publicly available and updated, when relevant.

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 adopt its rules of procedure.

5. The stakeholder forum shall hold regular meetings which shall be chaired by a Commission representative.

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

*Article 94*

*Tasks of the EHDS Board*

1. The EHDS Board shall have the following tasks relating to primary use in accordance with Chapters II and III:

   (a) assisting Member States in coordinating practices of digital health authorities;

   (b) issuing written contributions and exchanging best practices on matters related to the coordination of the implementation at Member State level, taking into account the regional and local level, of this Regulation and of the delegated and implementing acts adopted pursuant to it, in particular as regards:

      (i) the provisions set out in Chapters II and III;

      (ii) the development of online services facilitating secure access, including secure electronic identification, to electronic health data for health professionals and natural persons;

      (iii) other aspects relating to primary use;

   (c) facilitating cooperation between digital health authorities through capacity building, establishing the framework for activity-reporting referred to in Article 20(1) and the exchange of information;

(d) sharing among its members information concerning risks posed by EHR systems and serious incidents as well as the handling of such risks and incidents;

(e) facilitating the exchange of views on primary use with the stakeholder forum referred to in Article 93, as well as with regulators and policy makers in the health sector.

2. The EHDS Board shall have the following tasks related to secondary use in accordance with Chapter IV:

(a) assisting Member States in coordinating practices of health data access bodies in the implementation of provisions set out in Chapter IV, to ensure a consistent application of this Regulation;

(b) issuing written contributions and exchanging 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 for promoting data quality and interoperability improvement;

(iv) policies concerning fees to be charged by the health data access bodies and health data holders;

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

(vi) other aspects of secondary use;

(c) creating, in consultation and cooperation with relevant stakeholders, including representatives of patients, health professionals and researchers, guidelines in order to help health data users to fulfil their duties under Article 61(5), and in particular to determine whether their findings are clinically significant;

(d) facilitating cooperation between health data access bodies through capacity building, establishing the framework for activity-reporting referred to in Article 59(1), and the exchange of information;

(e) sharing information concerning risks and incidents related to secondary use, as well as the handling of such risks and incidents;

(f) facilitating the exchange of views on secondary use with the stakeholder forum referred to in Article 93, as well as with health data holders, health data users, regulators and policy makers in the health sector.

*Article 95*

*Steering groups for MyHealth@EU and HealthData@EU*

1. The MyHealth@EU steering group and the HealthData@EU steering group (the 'steering groups') are hereby established for the cross-border infrastructures provided for in Articles 23 and 75. Each steering group shall be composed of one representative per Member State appointed from the relevant national contact points.

2. The steering groups shall take operational decisions concerning the development and operation of MyHealth@EU and HealthData@EU.

3. The steering groups shall take decisions by consensus. Where a consensus cannot be reached, a decision shall be adopted by two-thirds of the members. For the adoption of the decisions, each Member State shall have one vote.

4. The steering groups shall adopt rules of procedure, setting out their composition, organisation, functioning and cooperation.

5. Other authorised participants may be invited to exchange information and views on relevant matters related to MyHealth@EU and HealthData@EU. Where those authorised participants are invited, they shall have an observer role.

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

7. The steering groups shall elect chairs for their meetings.

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

*Article 96*

*Roles and responsibilities of the Commission regarding the functioning of the EHDS*

1. In addition to its role in making available electronic health data held by Union institutions, bodies, offices or agencies, in accordance with Article 55, Article 56 and Article 75(2), and its tasks under Chapter III, in particular Article 40, the Commission shall develop, maintain, host and operate the infrastructures and central services required to support the functioning of the EHDS, for all relevant connected entities, by means of:

   (a) an interoperable, cross-border identification and authentication mechanism for natural persons and health professionals, in accordance with Article 16(3) and (4);

   (b) the central services and infrastructures for digital health of MyHealth@EU, in accordance with Article 23(1);

   (c) compliance checks for connecting authorised participants to MyHealth@EU, in accordance with Article 23(9);

   (d) the supplementary cross-border digital health services and infrastructures referred to in Article 24(1);

(e) as part of HealthData@EU, a service to submit health data access applications seeking access to electronic health data held by health data holders in more than one Member State or by other authorised participants in HealthData@EU and to automatically forward the health data access applications to the relevant contact points, in accordance with Article 67(3);

(f) the central services and infrastructures of HealthData@EU in accordance with Article 75(7) and (8);

(g) a secure processing environment in accordance with Article 75(9), in which health data access bodies can decide to make data available in accordance with Article 68(8);

(h) compliance checks for connecting authorised participants to HealthData@EU, in accordance with Article 75(5);

(i) a federated EU dataset catalogue connecting the national dataset catalogues, in accordance with Article 79;

(j) a secretariat for the EHDS Board, in accordance with Article 92(9);

(k) a secretariat for the steering groups, in accordance with Article 95(8).

2. The services referred to in paragraph 1 of this Article shall meet sufficient quality standards in terms of availability, security, capacity, interoperability, maintenance, monitoring and development to ensure the EHDS functions effectively. The Commission shall provide those services in accordance with the operational decisions of the relevant steering groups established in Article 95.

3. The Commission shall prepare a report on the infrastructures and services supporting the EHDS that it provides in accordance with paragraph 1 every two years and make it publicly available.

# Chapter VII
# Delegation of powers and committee procedure

*Article 97*
*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 Article 14(2), Article 49(4) and Article 78(5) shall be conferred on the Commission for an indeterminate period of time from … [date of entry into force of this Regulation].

3. The power to adopt delegated acts referred to in Article 14(2), Article 49(4) and Article 78(5) 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 Interinstitutional 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 Article 14(2), Article 49(4) or Article 78(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three 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 three months at the initiative of the European Parliament or of the Council.

*Article 98*

*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.

# Chapter VIII

# Miscellaneous

*Article 99*

*Penalties*

Member States shall lay down the rules on penalties applicable to infringements of this Regulation, in particular for infringements which are not subject to administrative fines pursuant to Articles 63 and 64, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by … [the date of entry into force of this Regulation + 24 months], notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

Member States shall take into account the following non-exhaustive and indicative criteria for the imposition of penalties for infringements of this Regulation, where appropriate:

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

(b) any action taken by the infringer to mitigate or remedy the damage caused by the infringement;

(c) any previous infringements by the infringer;

(d) the financial benefits gained or losses avoided by the infringer due to the infringement, insofar as such benefits or losses can be reliably established;

(e) any other aggravating or mitigating factors applicable to the circumstances of the case;

(f) the infringer's annual turnover in the Union in the preceding financial year.

*Article 100*

*Right to receive compensation*

Any natural or legal person that 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 Union and national law.

*Article 101*

*Representation of a natural person*

Where a natural person considers that his or her rights under this Regulation have been infringed, he or she shall have the right to mandate a not-for-profit body, organisation or association, constituted in accordance with national law, having statutory public interest objectives and active in the field of the protection of personal data, to lodge a complaint on his or her behalf or to exercise the rights referred to in Articles 21 and 81.

*Article 102*

*Evaluation, review and progress report*

1. By … [eight years from the date of 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, the Council, the European Economic and Social Committee and the Committee of the Regions, accompanied, where appropriate, by a proposal for its amendment. That evaluation shall cover the following:

   (a) the possibilities of further extending 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 referred to in Article 51 and the purposes listed in Article 53(1);

(c) the implementation and use by natural persons of the mechanisms to opt out from secondary use referred to in Article 71, in particular on the impact of those mechanisms on public health, scientific research and fundamental rights;

(d) the use and implementation of any stricter measures introduced pursuant to Article 51(4);

(e) the exercise and implementation of the right referred to in Article 8;

(f) an assessment of the certification framework for EHR systems established in Chapter III and the need to introduce further tools regarding conformity assessment;

(g) an assessment of the functioning of the internal market for EHR systems;

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

(i) the application of fees as referred to in Article 62.

2. By … [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, 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. That 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(7), 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 the reports referred to in paragraphs 1 and 2 and the Commission shall take that information duly into account in those reports.

4. Every year following … [date of the entry into force of this Regulation] until the end of the year in which all provisions of this Regulation apply as provided for in Article 105, the Commission shall submit a progress report to the Council on the preparations for the full implementation of this Regulation. That progress report shall contain information about the degree of progress and the readiness of the Member States in relation to the implementation of this Regulation, including an assessment of the feasibility of reaching the timeframes laid down in Article 105 and may also contain recommendations for Member States to improve preparedness for the application of this Regulation.

*Article 103*

*Amendment to Directive 2011/24/EU*

Article 14 of Directive 2011/24/EU is deleted with effect from … [six years from the date of entry into force of this Regulation].

*Article 104*

*Amendment to Regulation (EU) 2024/2847*

Regulation (EU) 2024/2847 is amended as follows:

(1) in Article 13, paragraph 4 is replaced by the following:

‘4. When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment referred to in paragraph 3 of this Article in the technical documentation required pursuant to Article 31 and Annex VII. For products with digital elements as referred to in Article 12 and Article 32(5a), which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.’;

(2) in Article 31, paragraph 3 is replaced by the following:

‘3. For products with digital elements as referred to in Article 12 and Article 32(5a), which are also subject to other Union legal acts which provide for technical documentation, a single set of technical documentation shall be drawn up containing the information referred to in Annex VII and the information required by those Union legal acts.’;

(3) in Article 32, the following paragraph is inserted:

‘5a. Manufacturers of products with digital elements that are classified as EHR systems under Regulation (EU) 2024/…[*+] of the European Parliament and of the Council shall demonstrate conformity with the essential requirements set out in Annex I to this Regulation using the relevant conformity assessment procedure provided for in Chapter III of Regulation (EU) 2024/…[++].

---

[*] Regulation (EU) 2024/… of the European Parliament and of the Council of … on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ …, ELI: …).’.

---

[+] OJ: Please insert in the text the number of the Regulation contained in document PE-CONS 76/24 (2022/0140(COD)) and insert the number, date, title and OJ reference of that Regulation in the footnote.

[++] OJ: Please insert in the text the number of the Regulation contained in document PE-CONS 76/24 (2022/0140(COD)).

# Chapter IX
# Deferred application, transitional and final provisions

*Article 105*

*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 from … [two years from the date of entry into force of this Regulation].

However, Articles 3 to 15, Article 23(2) to (6), Articles 25, 26, 27, 47, 48 and 49 shall apply as follows:

(a) from … [four years from the date of entry into force of this Regulation] to priority categories of personal electronic health data referred to in Article 14(1), points (a), (b) and (c), and to EHR systems intended by the manufacturer to process such categories of data;

(b) from … [six years from the date of entry into force of this Regulation] to priority categories of personal electronic health data referred to in Article 14(1), points (d), (e) and (f), and to EHR systems intended by the manufacturer to process such categories of data;

(c) from one year from the date established in a delegated act to be adopted pursuant to Article 14(2) for each amendment of the main characteristics of personal electronic health data set out in Annex I, provided that that date is subsequent to the date of application referred to in points (a) and (b) of this subparagraph for the categories of personal electronic health data concerned.

Chapter III shall apply to EHR systems put into service in the Union referred to in Article 26(2) from … [six years from the date of entry into force of this Regulation].

Chapter IV shall apply from … [four years from the date of entry into force of this Regulation]. However, Article 55(6), Article 70, Article 73(5), Article 75(1), Article 75(12), Article 77(4) and Article 78(6) shall apply from … [two years from the date of entry into force of this Regulation], Article 51(1), points (b), (f), (g), (m) and (p), shall apply from … [six years from the date of entry into force of this Regulation], and Article 75(5) shall apply from … [10 years from the date of entry into force of this Regulation].

The implementing acts referred to in Article 13(4), Article 15(1), Article 23(4) and Article 36(1) shall apply from the dates referred to in the third paragraph of this Article depending on the categories of personal electronic health data referred to in Article 14(1), points (a), (b) and (c), or Article 14(1), points (d), (e) and (f), respectively.

The implementing acts referred to in Article 70, Article 73(5), Article 75(12), Article 77(4) and Article 78(6) shall apply from … [four years from the date of entry into force of this Regulation].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at …,

| | |
|---|---|
| *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 summaries | Electronic health data that include significant clinical facts related to an identified natural person and that are essential for the provision of safe and efficient healthcare to that person. The following information is part of a patient summary:<br>1. Personal details.<br>2. Contact information.<br>3. Information on insurance.<br>4. Allergies.<br>5. Medical alerts.<br>6. Vaccination/prophylaxis information, possibly in the form of a vaccination card.<br>7. Current, resolved, closed or inactive problems, including in an international classification coding.<br>8. Textual information related to medical history.<br>9. Medical devices and implants.<br>10. Medical or care procedures.<br>11. Functional status.<br>12. Current and relevant past medicines.<br>13. Social history observations related to health.<br>14. Pregnancy history.<br>15. Patient-provided data.<br>16. Observation results pertaining to the health condition.<br>17. Plan of care.<br>18. Information on a rare disease, such as details about the impact or characteristics of the disease. |

| Electronic health data category | Main characteristics of electronic health data included under the category |
|---|---|
| 2. Electronic prescriptions | Electronic health data constituting a prescription for a medicinal product as defined in Article 3, point (k), of Directive 2011/24/EU. |
| 3. Electronic dispensations | Information on the supply of a medicinal product to a natural person by a pharmacy based on an electronic prescription. |
| 4. Medical imaging studies and related imaging reports | 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. Medical test results, including laboratory and other diagnostic results and related reports | Electronic health data representing results of studies performed in particular 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 reports | 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 software components of EHR systems and for products for which interoperability with EHR systems has been claimed

The essential requirements laid down in this Annex shall apply *mutatis mutandis* to medical devices, in vitro diagnostic medical devices, AI systems and wellness applications claiming interoperability with EHR systems.

1. General requirements

1.1. The harmonised software components of an 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 software components of the EHR system shall be designed and developed in such a way that the EHR 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.

1.4. The harmonised software 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 harmonised software components of an EHR system.

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 software component for EHR systems.

2.2. 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 software component for EHR systems.

2.3. 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 software component for EHR systems.

2.4. An EHR system that includes a functionality for entering structured personal electronic health data shall enable the entry of data with sufficient granularity to enable the provision of the entered personal electronic health data in the European health record exchange format.

2.5. The harmonised software components of an EHR system shall not include features that prohibit, restrict or place an undue burden on authorised access, personal electronic health data sharing or use of personal electronic health data for permitted purposes.

2.6. The harmonised software components of an EHR system shall not include features that prohibit, restrict or place an 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 logging.

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

3.2. The European logging software component of an EHR system designed to enable access by healthcare 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 healthcare provider or other individuals having accessed the personal electronic health data;

(b) identification of the specific natural person or persons having accessed the personal electronic health data;

(c) the categories of data accessed;

(d) the time and date of access;

(e) the origin or origins of data.

3.3. The harmonised software 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.

3.4. The harmonised software 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 37 shall contain at least the following information, as applicable to the harmonised software components of an EHR system in the relevant EHR system:

1. A detailed description of the EHR system including:

   (a) its intended purpose, and the date and 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 or software 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 or 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 for 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 36 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, in particular the applicable essential requirements.

5. A copy of the information sheet referred to in Article 38.

6. A copy of the EU declaration of conformity.

# ANNEX IV

EU declaration of conformity

The EU declaration of conformity for the harmonised software components of an EHR system 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, its 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 and, if applicable, with any other relevant Union law that provides for the issuing of an EU declaration of conformity, complemented by the result from the testing environment mentioned in Article 40.

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.