EUROPEAN
COMMISSION

Strasbourg, 3.5.2022
COM(2022) 197 final

2022/0140 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the European Health Data Space

(Text with EEA relevance)

{SEC(2022) 196 final} - {SWD(2022) 130 final} - {SWD(2022) 131 final} -
{SWD(2022) 132 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

The European strategy for data[1] proposed the establishment of domain-specific common European data spaces. The European Health Data Space ('EHDS') is the first proposal of such domain-specific common European data spaces. It will address health-specific challenges to electronic health data access and sharing, is one of the priorities of the European Commission in the area of health[2] and will be an integral part of building a European Health Union. EHDS will create a common space where natural persons can easily control their electronic health data. It will also make it possible for researchers, innovators and policy makers to use this electronic health data in a trusted and secure way that preserves privacy.

Today, natural persons have difficulties in exercising their rights over their electronic health data, including accessing and transmitting their electronic health data nationally and cross-borders. This is despite the provisions of Regulation (EU) 2016/679 (here after 'GDPR')[3], where rights of natural persons over their data, including health data, are safeguarded. As shown by the study assessing EU Member States' rules on health data in light of the GDPR[4], the uneven implementation and interpretation of the GDPR by Member States creates considerable legal uncertainties, resulting in barriers to secondary use of electronic health data. Thus, it creates certain situations where natural persons cannot benefit from innovative treatments and policy-makers cannot react effectively to a health crisis, due to barriers impeding access for researchers, innovators, regulators and policy makers to necessary electronic health data. Moreover, due to different standards and limited interoperability, manufacturers of digital health products and providers of digital health services operating in one Member State face barriers and additional costs when entering another one.

In addition, the COVID-19 pandemic has shown even further the importance of electronic health data for the development of policy in response to health emergencies. It has also highlighted the imperative of ensuring timely access to personal electronic health data for health threats preparedness and response, as well as for treatment, but also for research, innovation, patient safety, regulatory purposes, policy-making, statistical purposes or personalised medicine. The European Council has recognised the urgency to make progress towards and to give priority to the EHDS.

The general objective is to ensure that natural persons in the EU have increased control in practise over their electronic health data. It also aims to ensure a legal framework consisting of trusted EU and Member State governance mechanisms and

---

1 European Commission. European Data Strategy (2020). https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

2 As mentioned in the mission-letter-stella-kyriakides_en.pdf (europa.eu).

3 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 European Commission, Assessment of the EU Member States' rules on health data in the light of the GDPR, 2021.

a secure processing environment. This would allow researchers, innovators, policy-makers and regulators at EU and Member State level to access relevant electronic health data to promote better diagnosis, treatment and well-being of natural persons, and lead to better and well- informed policies. It also aims to contribute to a genuine single market for digital health products and services, by harmonising rules, and so boost healthcare system efficiencies.

Article 14 of the Directive 2011/24/EU on the application of patients' rights in cross-border healthcare (here after 'CBHC Directive')[5] was the first reference to eHealth in EU legislation. However, as stated in the impact assessment accompanying this EHDS Regulation, the relevant provisions of CBHC Directive are voluntary in nature. This partly explains why this aspect of the Directive has shown limited effectiveness in supporting natural persons' control over their personal electronic health data at national and cross-border level and very low effectiveness on secondary uses of electronic health data. The COVID-19 pandemic has revealed the urgent need and the high potential for interoperability and harmonisation, building upon existing technical expertise at national level. At the same time, digital health products and services, including telemedicine, have become an intrinsic part of the delivery of healthcare.

The evaluation of the digital aspects of the CBHC Directive addressed the COVID-19 pandemic and Regulation (EU) 2021/953 on the EU Digital COVID Certificate[6]. This time-limited Regulation addresses free movement restrictions imposed due to COVID-19. The evaluation shows that legal provisions supporting harmonisation and a common EU approach to use of electronic health data for specific purposes (as opposed to voluntary actions only), and EU efforts to ensure legal, semantic and technical interoperability[7], can deliver benefits. In particular, they can significantly support the free movement of natural persons and can promote the EU as a global standard setter in the field of digital health.

The EHDS will also promote better exchange and access to different types of electronic health data, including electronic health records, genomics data, patient registries etc. Not only will this support healthcare delivery (services and personnel involved in providing health care or primary use of electronic health data), it will also support health research, innovation, policy-making, regulatory purposes and personalised medicine purposes (secondary use of electronic health data). It will also establish mechanisms for data altruism in the health sector. The EHDS will help to attain the Commission's vision for EU's digital transformation by 2030, the Digital Compass[8] aim of providing 100% of natural persons with access to their medical records and Declaration of Digital Principles[9].

---

5 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).

6 Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic (OJ L 211, 15.6.2021, p. 1–22).

7 European Commission, European Interoperability Framework.

8 European Commission, Europe's digital decade: digital targets for 2030.

9 European Commision, Initiative on Declaration of Digital Principles – the 'European way' for the digital society.

- **Consistency with existing policy provisions in the policy area**

Cross-border exchange of electronic health data is to a certain extent addressed in the CBHC Directive in particular in its Article 14 on the eHealth Network. Established in 2011, it is a voluntary body at European level composed of digital health experts of all Member States with Iceland and Norway. They are working to promote EU-wide interoperability of electronic health data and to develop guidelines, such as semantic and technical standards, datasets and descriptions of infrastructures. The evaluation of the digital aspects of CBHC Directive noted the voluntary nature of this work and the guidelines. This explains why they have had a rather limited impact on supporting natural persons' access to and control over their electronic health data. The EHDS aims to address these issues.

The EHDS builds upon legislation such as the GDPR, the Regulation (EU) 2017/745 on medical devices (Medical Devices Regulation)[10] and the Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices (In Vitro Diagnostics Regulation)[11], the proposed Artificial Intelligence Act[12], the proposed Data Governance Act[13] and the proposed Data Act[14], the Directive 2016/1148 on security of network and information systems (NIS Directive)[15] and the CBHC Directive.

Considering that a substantial amount of electronic data to be accessed in the EHDS are personal health data relating to natural persons in the EU, the proposal is designed in full compliance not only with the GDPR but also with Regulation (EU) 2018/1725 (EU Data Protection Regulation)[16]. The GDPR provides the rights to access, to portability and to accessibility/transmission to a new controller of data. It also designates data related to health as a "special category of data", affording it special protection through the establishment of additional safeguards for its processing. The EHDS supports the implementation of the rights enshrined in the GDPR as applied to electronic health data. This is regardless of the Member State, the type of healthcare provider, the sources of electronic health data or the affiliation of the natural person. The EHDS builds upon the possibilities offered by the GDPR for an EU legislation on the use of personal electronic health data for medical diagnosis, the provision of health care or treatment or the management of health care systems and services. It also permits the use of electronic health data for scientific or

---

10 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1–175).

11 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176–332).

12 Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM/2021/206 final.

13 Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767 final.

14 Proposal for a Regulation on harmonised rules on fair access and use of data (Data Act) COM/2022/068 final.

15 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1–30).

16 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. 39–98).

historical research, official statistical purposes, and public interest in the area of public health, such as protecting against serious cross-border health threats or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. The EHDS envisages further provisions to promote interoperability and enhances the right of the natural persons to data portability in the health sector.

In the context of the European Health Union, the EHDS will support the work of the European Health Emergency Preparedness and Response Authority (HERA)[17], in the Europe's Beating Cancer Plan[18] the EU Mission on Cancer[19], and in the Pharmaceutical Strategy for Europe[20]. The EHDS will create a legal and technical environment that will support the development of innovative medicinal products and vaccines, and of medical devices and in vitro diagnostics. This will help to prevent, detect, and rapidly respond to health emergencies. In addition, the EHDS will help to improve understanding, prevention, early detection, diagnosis, treatment and monitoring of cancer, through the EU cross-border secure access and sharing between healthcare providers of health, including cancer related data of natural persons. Therefore, by providing secure access to a wide range of electronic health data, the EHDS will open new opportunities for diseases prevention and treatment of natural persons.

The EHDS proposal also builds on the requirements that have been imposed on software through the Medical Devices Regulation and the proposed Artificial Intelligence Act. Medical device software already needs to be certified under the Medical Devices Regulation and AI-based medical devices and other AI systems would also need to comply with the requirements of the Artificial Intelligence Act once in force. However, a regulatory gap has been identified when it comes to information systems used in the health domain, also called electronic health record systems ('EHR systems'). The focus is therefore on these EHR systems that are intended to be used to store and share electronic health data of natural persons. Therefore, the EHDS sets essential requirements specifically for EHR systems in order to promote interoperability and data portability of such system, which would allow natural persons to control their electronic health data more effectively. In addition, where manufacturers of medical devices and high-risk AI systems declare interoperability with the EHR systems, they will need to comply with the essential requirements on interoperability under the EHDS Regulation.

When providing a framework for the secondary use of electronic health data, the EHDS **builds upon the proposed Data Governance Act** and the proposed **Data Act**. As horizontal framework, the Data Governance Act only lays down generic conditions for secondary use of public sector data without creating a genuine right to secondary use of such data. The proposed Data Act enhances portability of certain user-generated data, which can include health data, but does not provide rules for all health data. Therefore, the EHDS complements these proposed legislative acts and provides more specific rules for the health sector. These specific rules cover the exchange of electronic health data and may impact on provider of data sharing

17 Health Emergency Preparedness and Response Authority | European Commission (europa.eu).
18 A cancer plan for Europe | European Commission (europa.eu).
19 EU Mission: Cancer | European Commission (europa.eu).
20 A pharmaceutical strategy for Europe (europa.eu).

services, formats that ensure the portability of health data, cooperation rules for data altruism in health and complementarity on access to private data for secondary use.

The NIS Directive set the first **EU-wide rules on cybersecurity**. This Directive is being revised (the 'NIS2 proposal[21]), currently undergoing negotiations with the co-legislators. It aims to raise the EU common level of ambition of the cybersecurity regulatory framework, through a wider scope, clearer rules and stronger supervision tools. The Commission proposal addresses these issues across three pillars: (1) Member State capabilities; (2) risk management; (3) cooperation and information exchange. Operators in the healthcare system remain under the scope. The EHDS is enhancing security and trust in the technical framework designed to facilitate the exchange of electronic health data for both primary and secondary use.

A proposal for a Cyber Resilience Act is also planned for adoption by the Commission in 2022, with the aim to set out horizontal cybersecurity requirements for digital products and ancillary services. The envisaged set of essential cybersecurity requirements to be laid down by the Cyber Resilience Act will be applied to all sectors and categories of digital products whose producers and vendors shall comply with, before placing the products on the market or, as applicable, when putting them into service and also through the entire product lifecycle. These requirements will be of general nature and technology neutral. The security requirements set out in the EHDS, notably as regards the EHR systems, provide more specific requirements in certain areas, such as access control.

The EHDS builds upon the new proposal on the European Digital Identity[22] with the improvements in the domain of electronic identification, including the Digital Identity Wallet. This would allow better mechanisms for the online and offline identification of natural persons and health professionals.

- **Consistency with other Union policies**

This proposal is in line with the EU's overarching objectives. These include building a stronger European Health Union, implementing the European Pillar of Social Rights, improving the functioning of the internal market, promoting synergies with the EU digital internal market agenda, and delivering an ambitious research and innovation agenda. In addition, it will provide an important set of elements contributing to the formation of the European Health Union, by encouraging innovation and research and dealing better with future health crises.

The proposal is consistent with the Commission's priorities to make Europe fit for the digital age and to build a future-proof economy that works for people. It also allows exploring the potential of cross-border regions as pilot tests for innovative solutions to European integration, as suggested in in the Commission report EU Border Regions: Living labs of European integration[23]. It supports the Commission's Recovery Plan, learning lessons from the COVID-19 pandemic and delivers benefits of more easily accessible electronic health data where necessary.

---

21 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final.

22 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final.

23 European Commission, Report on EU border Regions: Living labs of European integration, 2021.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The proposal is based on Articles 16 and 114 of the Treaty on the Functioning of the European Union (TFEU). Such a dual legal basis is possible, if it is established that the measure simultaneously pursues several objectives that are inseparably linked without one being secondary or only indirectly related to the other. That is the case of the present proposal, as explained below. The procedures laid down for each legal basis are compatible with each other.

Firstly, Article 114 TFEU aims at improving the functioning of the internal market through measures for the approximation of national rules. Some Member States have taken legislative action to address the problems described above, by establishing national certification systems for EHR systems, whereas others have not. This can lead to legislative fragmentation in the internal market and different rules and practices across the EU. It could also lead to costs for companies that would have to comply with different regimes.

Article 114 TFEU is the appropriate legal basis since the majority of provisions of this Regulation aim to improve the functioning of the internal market and the free movement of goods and services. In this respect, Article 114(3) TFEU explicitly requires that, in achieving harmonisation, a high level of protection of human health is to be guaranteed taking account in particular of any new development based on scientific facts. This legal basis is therefore also appropriate where an action is related to the domain of public health protection. This is also in full respect of Article 168 which provides that a high level of human protection is to be achieved in all Union policies, while respecting Member State responsibility for the definition of their health policy and for the organisation and delivery of health services and medical care.

The legislative proposal will allow the EU to benefit from the scale of the internal market, since health data-driven products and services are often developed using electronic health data from different Member States and later commercialised across the EU.

The second legal basis for this proposal is Article 16 TFEU. The GDPR provides important safeguards in relation to rights of natural persons over their health data. However, as outlined in Section 1, these rights cannot be implemented in practice because of interoperability reasons and limited harmonisation of requirements and technical standards implemented at national and EU level. Additionally, the scope of the right to portability under the GDPR renders it less effective in the health sector[24]. Therefore, there is a need to put in place additional legally binding provisions and safeguards. It is also necessary to design specific requirements and standards that build on safeguards provided in the field of electronic health data processing to take advantage of the value of health data for the society. Moreover, the proposal aims to expand the use of electronic health data while strengthening the rights arising from Article 16 TFEU. Overall, the EHDS brings to reality the possibility offered by GDPR for an EU law for several purposes. These include medical diagnosis, the provision of health care or treatment or the management of health care systems and

[24] The exclusion of “inferred” data and the limitation to data processed based on consent or contract mean that large amounts of data related to health are outside the scope of the GDPR portability right.

services. It also allows the use of electronic health data for public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health and care and of medicinal products or medical devices. It also serves scientific or historical research and statistical purposes.

- **Subsidiarity**

The current proposal aims to harmonise data flows to support natural persons in benefiting from protection and free movement of electronic health data, especially personal data. The proposal does not aim to regulate how healthcare is provided by Member States.

The evaluation of the digital aspects of the CBHC Directive reviewed the current situation of fragmentation, differences and barriers to access and use of electronic health data. It showed that action by Member States alone is not sufficient and may hamper the rapid development and deployment of digital health products and services including based on artificial intelligence.

The above-mentioned study on the GDPR's implementation in the health sector, notes that the Regulationprovides extensive rights on natural persons' access to and transmission of their data, including health data. Nevertheless, their practical implementation is hampered by low interoperability in the healthcare sector, which has been addressed so far mainly through soft law instruments. Such differences in local, regional and national standards and specifications can also prevent manufacturers of digital health products and providers of digital health service from entering new markets, where they need to adapt to new standards. This legislative proposal is thus designed to complement the rights and safeguards provided in the GDPR, so that its goals can indeed be achieved.

The same study reviewed that the extensive use of facultative specification provisions under the GDPR at national level. This created fragmentation and difficulties for accessing electronic health data, both at national level and between Member States. It had an impact on the possibility of researchers, innovators, policy makers and regulators to carry out their tasks or to carry out research or innovation. Ultimately, it was detrimental to the European economy.

In the impact assessment, the evaluation of Article 14 of the CBHC Directive shows that the approaches taken so far, consisting of low intensity/soft instruments, such as guidelines and recommendations aimed to support interoperability, have not produced the desired results. Natural persons' access to and control of their personal electronic health data is still limited, and there are significant deficiencies in the interoperability of information systems used in the health domain. Moreover, national approaches in addressing the problems have only limited scope and do not fully address the EU-wide issue. Currently, the cross-border exchange of electronic health data is still very limited, which is partly explained by the significant diversity in standards applied to electronic health data in different Member States. In many Member States, there are substantial national, regional and local challenges to interoperability and data portability, hampering continuity of care and efficient healthcare systems. Even if health data are available in electronic format, it does not usually follow the natural person when they use services of a different healthcare provider. The EHDS proposal will address these challenges at EU level, providing mechanisms for improving interoperability solutions used at national, regional and local levels and reinforcing the rights of natural persons.

Therefore, EU-wide action in the content and form indicated is required to promote cross-border flow of electronic health data and to foster a genuine internal market for electronic health data, digital health products and services.

- **Proportionality**

The initiative seeks to put in place measures that are necessary to achieve the main objectives. The proposal creates an enabling framework that does not go beyond what is necessary to achieve the objectives. It addresses existing barriers to foster the realisation of the potential value of electronic health data. It sets a framework that reduces fragmentation and legal uncertainty. The initiative involves and relies on the work of the national authorities and seeks a strong involvement of relevant stakeholders.

The proposed Regulation will give rise to financial and administrative costs, which are to be borne through the allocation of resources at both Member States and EU level. The impact assessment demonstrates that the preferred policy option brings the best benefits at the least cost. The preferred policy option does not exceed what is necessary to achieve the objectives of the Treaties.

- **Choice of the instrument**

The proposal takes the form of a new Regulation. This is considered the most suitable instrument, given the need for a regulatory framework that directly addresses the rights of natural persons and reduces fragmentation in the digital single market. To prevent the fragmentation that resulted from inconsistent use of the relevant clauses in the GDPR (e.g. Article 9(4)), the EHDS uses the options for an EU law offered by the GDPR Regulation concerning the use of health data, for various purposes. In the preparing the proposal, different national legal contexts that built upon the GDPR by providing national legislation were carefully analysed. In order to prevent major disruption, but also inconsistent future developments, the EHDS aims to put forward an initiative that takes into account the main common elements of different frameworks. A Directive was not selected, as it would allow a divergent implementation and a fragmented market that could affect the protection and free movement of personal data in the health sector. The proposal will strengthen the EU's health data economy by increasing legal certainty and guaranteeing a fully uniform and consistent sectoral legal framework. The proposed Regulation also calls for stakeholder involvement to ensure that requirements meet the needs of health professionals, natural persons, academia, industry and other relevant stakeholders.

3. RESULTS OF *EX-POST* EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- ***Ex-post* evaluations/fitness checks of existing legislation**

The CBHC Directive was adopted in 2011 and was transposed in all Member States by 2015. Article 14 of the Directive, establishing the eHealth Network, has been evaluated to better understand the impact it has had on digital health in the EU. The evaluation, which is an Annex to the EHDS impact assessment staff working document, finds that its impact has been rather limited. The evaluation of the eHealth provisions under the Directive concluded that its effectiveness and efficiency has been rather limited and that this was due to the voluntary nature of the eHealth Network actions.

Progress was slow on the use of personal electronic health data for primary purpose in the context of cross-border healthcare. The MyHealth@EU platform was implemented in only 10 Member States and it is currently supporting only two services (electronic prescription and patient summary). The low and slow uptake is partly related to the fact that the Directive, while establishing the right of natural persons to receive a written record of the treatment carried out, does not require this medical record to be provided in electronic form. Natural persons' access to their personal electronic health data remains burdensome, and natural persons have limited control over their own health data and the use of these health data for medical diagnosis and treatment. The eHealth Network recommended that Member States use the Electronic Health Record Exchange Format standards and specifications in their procurements, in order to build interoperability. However, their real uptake of the format was limited, resulting in a fragmented landscape and uneven access to, and portability of, electronic health data.

Most Member States are expected to implement the MyHealth@EU platform by 2025. Only when more Member States will have implemented the MyHealth@EU platform and developed the necessary tools, will their use, development and maintenance become more efficient across the EU. However, advancements in eHealth in recent years call for a more coordinated action at EU level.

Nevertheless, following the outbreak of the COVID-19 pandemic in Europe, the eHealth Network proved to be very effective and efficient in times of a public health crisis and this promoted political convergence.

On secondary use of electronic health data, the eHealth Network activities were very limited and not very effective. The few non-binding documents on big data were not followed up by further specific actions and their implementation in practice remains very limited. At national level, other actors emerged on secondary use of electronic health data than the ones represented in the eHealth Network. Some Member States set up different bodies to deal with the subject and participated in the joint action Towards a European Health Data Space (TEHDaS). However, neither this joint action, nor the numerous funds provided by the Commission, for example under Horizon Europe, to support the secondary use of electronic health data have been sufficiently implemented in coherence with eHealth Network activities.

It was therefore concluded that the current structure of the eHealth Network is no longer appropriate. It only allows soft cooperation on primary use of electronic health data and interoperability, which did not solve in a systematic manner data access and portability problems at national and cross-border level. Moreover, the eHealth Network is not able to address the needs related to secondary use of electronic health data in an effective and efficient manner. The CBHC Directive provides empowerments for implementing acts on the use of electronic health data for primary and secondary use; these empowerments are limited.

The COVID-19 pandemic has highlighted and emphasised the importance of secure and safe access to and availability of public health and healthcare data across Member States borders, and the wide availability of electronic health data for public health in the context of the free movement of people within the EU during the pandemic. Building on a strong regulatory framework, the EU has been very effective in establishing EU-level standards and services to facilitate the free movement of people, such as the EU Digital COVID Certificate. However, overall progress seems to be hindered by the absence of binding or compulsory standards

across the EU and consequently limited interoperability. Addressing this issue would not just benefit natural persons, it would also contribute to achieving the digital internal market and lowering barriers to the free movement of digital healthcare products and services.

- **Stakeholder consultations**

In preparing this EHDS proposal, stakeholders were consulted in various ways. The public consultation collected views from stakeholders on options for establishing the EHDS[25]. Feedback was received from various stakeholder groups. Their views can be found in detail in the annex to the impact assessment staff working document.

A **public consultation** was conducted from May to July 2021. In total, 382 valid responses were received. Respondents expressed support for action at EU level for accelerating research in health (89%), promoting natural persons' control over their own health data (88%) and facilitating the delivery of healthcare across borders (83%). There was great support for promoting access and sharing of health data through a digital infrastructure (72%) or an EU infrastructure (69%). Most respondents are also of the view that natural persons should be able to transmit data collected from mHealth and telemedicine into EHR systems (77%). An EU level certification scheme to promote interoperability attracted 52% support.

In the area of secondary use of health data, most respondents said an EU body could facilitate access to health data for secondary purposes (87%). Mandatory use of technical requirements and standards is supported by 67%.

Stakeholder views were also collected through the study on the 'Assessment of the EU Member States' rules on health data in the light of the GDPR'. During the study, five workshops took place with ministries of health representatives, experts, stakeholder representatives and experts from national data protection offices[26]. A stakeholder survey was also carried out to cross validate and supplement the topics addressed and identified. In total, the online survey received 543 responds. From an online survey, 73% of respondents consider that having health data in a personal data space or patient portal facilitates data transmission between healthcare providers. Furthermore, 87% consider a lack of data portability drives up costs in healthcare, while 84% consider a lack of data portability delays diagnosis and treatment. Some 84% are of the view that additional measures should be taken at EU level to strengthen natural persons' control over their health data. Some 81% consider the use of different GDPR legal basis makes it difficult to share health data. Some 81% of respondents suggest the EU should support secondary use of health data under the same legal base.

A study on the regulatory gaps to cross-border provision of digital health services and products, including artificial intelligence, and the evaluation of the existing framework for cross-border exchange of health data. A study on Health Data, Digital Health and Artificial Intelligence in Healthcare, was carried out between September 2020 and August 2021. This study provides evidence needed to enable informed policy making in the areas of digital health products and services, artificial intelligence, governance on the use of health data and the evaluation of Article 14 of the CBHC Directive. The consultation activities included interviews, focus groups

25 Press corner | European Commission (europa.eu).

26 More details in Nivel for European Commission, p. 20.

and online surveys. Stakeholders support measures in a number of areas, ranging from guidance on digital health services and products quality, interoperability, reimbursement, identification and authentication, and digital literacy and skills. On primary use, stakeholders support mandating national digital health authorities with tasks to support cross-border provision of digital health and access to electronic health data. In addition, they also support expansion of the MyHealth@EU services. There is also support for giving natural persons the right to portability of their electronic health records in an interoperable format. On secondary use, there is support for putting in place a legal and governance framework and structure, building on the establishment of health data access bodies in a number of Member States, with cooperation at EU level through a network or an advisory group. To reduce barriers, there would be support for specifications and standards.

A study on infrastructures and data ecosystem supporting the impact assessment of the EHDS[27], was carried out between April 2021 and December 2021. This study aims to present evidence-based insights that will support the impact assessment of options for a European digital health infrastructure. The study identifies, characterises and assesses options for a digital infrastructure, outlines the cost-effectiveness and provides data on the expected impacts, both for primary and secondary use of electronic health data. Interactive workshops were conducted covering 65 stakeholders who actively engage with health data usage. Their background varies across ministries of health, digital health authorities, national contact points for eHealth, health data research infrastructures, regulatory agencies, health data access bodies, healthcare providers, patients and advocacy groups. In addition, a survey focusing on costs was developed, including questions related to the value, benefits, impact and cost of different options.

Finally, the impact assessment study was carried out between June 2021 and December 2021. It aimed to present evidence-based insights that supported the impact assessment of options for the EHDS. The study sets out and assessed the overall policy options for the EHDS, building upon the evidence gathered in the previous studies. The 'public consultation on overcoming cross-border obstacles[28]' also illustrates that natural persons face related obstacles in the context of cross-border regions. More details of these studies are provided in the Annex in the staff working document.

- **Collection and use of expertise**

  Several studies and contributions supported the work on the EHDS, including:

  - A study on the "Assessment of the EU Member States' rules on health data in the light of the GDPR"[29],
  - A study on the regulatory gaps to cross-border provision of digital health services and products, including artificial intelligence, and the evaluation of the existing framework for cross-border exchange of health data (forthcoming);

27 European Commission (forthcoming study). A study on an infrastructure and data ecosystem supporting the impact assessment of the European Health Data Space, Trasys.

28 European Commission, public consultation on overcoming cross-border obstacles, 2020.

29 European Commission (2020). Assessment of the EU Member States rules on health data in the light of GDPR. (Annexes available here: https://ec.europa.eu/health/system/files/2021-02/ms_rules_health-data_annex_en_0.pdf).

- A study on an infrastructure and data ecosystem supporting the impact assessment of the EHDS (forthcoming);
- Study supporting the Impact assessment of policy options for an EU initiative on a EHDS (forthcoming);
- A study on the electronic health record interoperability in the European Union (MonitorEHR)[30];
- A study on the use of real-world data (RWD) for research, clinical care, regulatory decision making, health technology assessment, and policy making and its executive summary[31];
- A market study on telemedicine[32];
- The European Data Protection Supervisor (EDPS) preliminary opinion on the EHDS[33].

• **Impact assessment**

An impact assessment was carried out for this proposal. On 26 November 2021, the Regulatory Scrutiny Board issued a negative opinion on the first submission. After substantial revision of the impact assessment to address the comments and a resubmission of the impact assessment, on 26 January 2022 the Board delivered a positive opinion without reservations. The opinions of the Board, the recommendations and an explanation of how they have been taken into account are presented in Annex 1 of the staff working document.

The Commission examined different policy options to achieve the general objectives of the proposal. These are to ensure that natural persons have control over their own electronic health data, that they can benefit from a range of health-related products and services and that researchers, innovators, policy-makers and regulators can make the most of available electronic health data.

Three policy options of varying degrees of regulatory intervention and two additional variations of these options were assessed:

– **Option 1: Intervention with low intensity:** It relies on an increased cooperation mechanism and voluntary instruments that would cover digital health products and services and the secondary use of electronic health data. It would be supported by improved governance and digital infrastructure.

– **Option 2 and 2+: Intervention with medium intensity:** It would strengthen the rights of natural persons to control digitally their health data and provide an EU framework for the secondary use of electronic health data. The governance would rely on national bodies for primary and secondary use of electronic health data that would implement the policies nationally and, at EU level, support the development of appropriate requirements. Two digital infrastructures would support cross border sharing and secondary use of electronic health data. Implementation would be supported by a mandatory

30 eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU, Lot 1 - Interoperability of Electronic Health Records in the EU (2020).

31 Study on the use of real-world data (RWD) for research, clinical care, regulatory decision-making, health technology assessment, and policy-making.

32 Market study on telemedicine.

33 Preliminary Opinion 8/2020 on the European Health Data Space.

certification for EHR systems and a voluntary label for wellness applications, thus ensuring transparency for authorities, procurers and users.

– **Option 3 and 3+: Intervention with high intensity:** It would go beyond Option 2 by assigning to an existing or new EU body the definition of EU level requirements and access to cross border electronic health data. It would also extend the coverage of certification.

The preferred option is **Option 2+,** which builds upon **Option 2.** This would ensure a certification of EHR systems, a voluntary label for wellness application and a cascading effect in medical devices that aim to be interoperable with EHR systems. This would ensure the best balance between effectiveness and efficiency in reaching the objectives. **Option 1** would improve the baseline marginally, as it remains voluntary. **Option 3** would also be effective, but would have higher costs, may have a greater impact on SMEs and may be less feasible politically.

The preferred option would ensure that natural persons are able to digitally access and transmit their electronic health data, and enable access to it, irrespective of healthcare provider and data source. MyHealth@EU would become mandatory and natural persons could exchange their personal electronic health data cross-border in a foreign language. Mandatory requirements and certification (for EHR systems and medical devices claiming interoperability with EHR systems) and a voluntary label for wellness applications would ensure transparency for users and procurers and reduce cross-border market barriers for manufacturers.

The mandatory requirements have been maintained, but third-party certification was modified into self-certification coupled with an earlier review clause, allowing for a possible later transition to third-party certification. Given the novelty of the certification, it was decided to opt for a stepwise approach, that would allow less prepared Member States and manufacturers more time to put in place the certification system and build capacity. At the same time, more advanced Member States may require specific checks at national level in the context of procurement, financing and reimbursement of EHR systems. Such a change would reduce the estimated costs for certification for an individual manufacturer of an EHR system from EUR 20,000-50,000 to EUR 12,000-38,000, which could yield a reduction of approximately 30% in overall costs for manufacturers (from EUR 0.3-1.7 billion to EUR 0.2-1.2 billion).

This system seems the most proportionate for manufacturers in terms of administrative burden and potential capacity limitations of notified bodies for third-party certification. However, the actual benefits it produces on Member States, patients and procurers will need to be carefully analysed in the evaluation of the legal framework after five years.

On secondary use of electronic health data, researchers, innovators, policy makers and regulators would be able to have access to quality data for their work in a secure way, with a trusted governance and at lower costs than relying on consent. The common framework for secondary use would reduce the fragmentation and barriers for cross-border accesses. The preferred option requires Member States to set up one or more health data access bodies (with a coordination body), that can provide access to electronic health data to third parties, either as a new organisation or part of an existing organisation, building on the Data Governance Act. Parts of the costs will be offset through fees charged by health data access bodies. The setting up of health data access bodies is expected to lower costs to regulators and policy makers for

accessing electronic health data, thanks to greater transparency of the effectiveness of medicinal products, resulting in a reduction of costs in the regulatory processes and in public procurement in health. Digitalisation can also reduce unnecessary tests and ensure transparency in spending, allowing savings to the health budget. EU funds will provide support for digitalisation.

The goal is to ensure transparency of information concerning datasets to data users, for which a stepwise approach was also adopted. This would mean that the dataset description would be mandatory for all datasets, excluding those held by micro-enterprises, while the self-declared data quality label, would only be mandatory for data holders with publicly funded datasets and voluntary for others. These nuances introduced after the impact assessment do not substantially alter the calculation of the costs for data holders stemming from the impact assessment.

The total economic benefits of this option are expected, over 10 years, to be above EUR 11 billion, above the baseline. This amount would be split almost evenly between benefits originating from measures on primary (EUR 5.6 billion) and secondary uses (EUR 5.4 billion) of health data.

In the area of primary use of health data, patients and healthcare providers will see benefits of approximately EUR 1.4 billion and EUR 4.0 billion stemming from savings in health services through greater update of telemedicine and more efficient exchanges of health data, including across borders.

In the area of secondary use of health data, researchers and innovators in digital health, medical devices and medicinal products would have benefits of over EUR 3.4 billion thanks to a more efficient secondary use of health data. Patients and healthcare would benefit from EUR 0.3 and EUR 0.9 billion in savings thanks to access to more innovative medical products and better decision-marking. The more intensive use of real-world evidence in health policy-making would yield additional savings, estimated at EUR 0.8 billion, for policy-makers and regulators.

The overall costs for the preferred option are estimated at EUR 0.7-2.0 billion above the baseline, over 10 years. The majority of costs would originate from measures on primary (EUR 0.3-1.3 billion) and secondary uses (EUR 0.4-0.7 billion) of health data.

In the area of primary use of health data, manufacturers of EHR systems and products intended to connect to EHR systems would bear most costs. This would amount to approximately EUR 0.2-1.2 billion due to the stepwise introduction of certification for EHR systems, medical devices and high-risk AI systems and voluntary labelling for wellness applications. The rest (less than EUR 0.1 billion) would be on public authorities, at national and EU level, for the completion of the coverage of MyHealth@EU.

In the area of secondary use of health data, public authorities, including regulators and policy-makers at Member State and EU level, would bear the costs (EUR 0.4-0.7 billion) for the rollout of health data access bodies and the necessary digital infrastructure connecting these bodies, research infrastructures and EU bodies, and the promotion of interoperability and data quality.

The preferred option is limited to aspects that Member States cannot achieve satisfactorily on their own, as shown by the evaluation of Article 14 of the CBHC Directive. The preferred option is proportionate, given the medium intensity of the proposal and the expected benefits for natural persons and industry.

The assessment of environmental impacts, in line with the European Climate Law[34], shows that this proposal would result in limited impacts on climate and the environment. While new digital infrastructures and increased volumes of data traffic and storage may increase digital pollution, greater interoperability in health would largely offset such negative impacts by reducing travel-related pollution and energy and paper usage.

- **Regulatory fitness and simplification**

  Not applicable.

- **Fundamental rights**

  Since the use of electronic health data involves the processing of sensitive personal data, some elements of the proposed Regulation fall within the scope of the EU data protection legislation. The provisions of this proposal comply with the EU data protection legislation. They are designed to complement the rights provided by the EU data protection legislation by strengthening the control and access of the natural persons to their electronic health data. The proposal is expected to have a significant positive impact on fundamental rights related to the protection of personal data and free movement. This is because under MyHealth@EU, natural persons will be able to effectively share their personal electronic health data in the language of the country of destination when travelling abroad or take their personal electronic health data with them when moving to another country. Natural persons will have additional possibilities to digitally access and transmit their electronic health data, building upon provisions in the GDPR. Market operators in the health sector (either healthcare providers or providers of digital services and products) will be obliged to share electronic health data with user-selected third parties from the health sector. The proposal will provide the means to enforce these rights (through common standards, specifications and labels) without compromising on the required safety measures to protect natural person rights under the GDPR. It would contribute to the increased protection of health-related personal data and the free movement of such data as enshrined in Article 16 TFEU and in the GDPR.

  Regarding secondary use of electronic health data, e.g. for innovation, research, public policy, patient safety, regulatory purposes or personalised medicine the proposal will follow and comply with the EU data protection legislation on this matter. Strong safeguards and security measures will be implemented to ensure that the fundamental rights of data protection are fully protected, in accordance with Article 8 of the EU Charter of Fundamental Rights. The proposal sets out an EU framework for accessing electronic health data for scientific and historical research purposes and statistical purposes, building upon the possibilities offered in this respect by the GDPR and, for EU institutions and bodies, by the EU Data Protection Regulation. It will include suitable and specific measures required to safeguard fundamental rights and the interests of natural persons in accordance with Articles 9.2 (h), (i) and (j) of the GDPR; and Articles 10.2 (h), (i) and (j) of the EU Data Protection Regulation. Setting up health data access bodies will ensure a predictable and simplified access to electronic health data, and a higher level of transparency, accountability and security in data processing. Coordinating these bodies at EU level

[34] Paragraph 4 of Article 6 of Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law').

and enshrining their activities in a common framework will ensure a level playing field. This will support cross-border analysis of electronic health data for research, innovation, official statistics, policy making and regulatory purposes. The promotion of interoperability of electronic health data and its secondary use will contribute to promoting an EU internal market for electronic health data in line with Article 114 TFEU.

4. BUDGETARY IMPLICATIONS

This proposal sets out a number of obligations for Member State authorities and the Commission and requires specific actions to promote the establishment and functioning of the EHDS. These cover, in particular, the development, deployment and maintenance of infrastructures for primary and secondary uses of electronic health data. The EHDS has strong ties with several other actions of the Union in the areas of health and social care, digitisation, research, innovation and fundamental rights.

In its 2021 and 2022 work programmes, EU4Health already supports the development and establishment of the EHDS with a substantial initial contribution of almost EUR 110 million. This includes the functioning of the existing infrastructure for primary uses of electronic health data (MyHealth@EU) and secondary use of electronic health data (HealthData@EU), the uptake of international standards by Member States, actions on capacity building and other preparatory actions, as well as an infrastructure pilot project for the secondary use of health data, a pilot project for the access of patients to their health data through MyHealth@EU and its scale-up, and the development of the central services for secondary uses of health data.

The fulfilment of the obligations by the Commission and associated support actions under this legal proposal will require EUR 220 million between 2023 and 2027 and will be funded directly from the EU4Health programme (EUR 170 million) and supported further from the Digital Europe Programme (EUR 50 million)[35]. In both cases, the expenditure linked to this proposal will be covered within the programmed amounts of these programmes.

The implementation of actions for natural persons' control of and access to personal electronic health data for the provision of healthcare (Chapter II) will require EUR 110 million. These actions include the operations of the European digital health platform services for MyHealth@EU, Member States audits for the National Contact Points for Digital Health as part of MyHealth@EU, support for the uptake of international standards and support for patients' access to health data through MyHealth@EU.

Implementing the self-certification scheme for EHR systems (Chapter III) will require over EUR 14 million to develop and maintain a European database for interoperable EHR systems and wellness applications. Additionally, Member States will have to designate market surveillance authorities in charge of implementing the legislative requirements. Their supervisory function for the self-certification of EHR systems could build on existing arrangements, for example regarding market

[35] The contributions from the Digital Europe Programme as of 2023 are indicative, and will be considered in the context of the preparation of the respective Work Programmes. Ultimate allocations will be subject to the prioritisation for funding in the context of the underpinning adoption procedure and agreement of the respective Programme Committee.

surveillance, but would require sufficient expertise and human and financial resources. Actions for the secondary use of electronic health data for research, innovation, policy-making, regulatory decisions, patient safety or personalised medicine (Chapter IV) will require EUR 96 million. This funding will cover the European platform and Member States audits for the connection nodes, as part of infrastructure for secondary uses of electronic health data (HealthData@EU).

Beyond this, the costs for the connection of Member States to the European infrastructures within the EHDS will be partially covered by EU funding programmes that will complement EU4Health. Instruments such as Recovery and Resilience Facility (RRF) and the European Regional Development Fund (ERDF) will be able to support the connection of Member States to the European infrastructures.

The implementation of the objectives and provisions of this Regulation will be complemented by other actions under Digital Europe Programme, Connecting Europe Facility and Horizon Europe. These programmes, among others, aim at *building up and strengthening quality data resources and corresponding exchange mechanisms*[36] (under the Specific Objective Artificial Intelligence) and *developing, promoting and advance scientific excellence*[37], respectively, including in health. Instances of such complementarity include horizontal support for the development and large-scale piloting of a smart middleware platform for common data spaces, where EUR 105 million from Digital Europe Programme have already been allocated in 2021-2022; domain-specific investments to facilitate the secure cross-border access to cancer images and genomics, supported by Digital Europe Programme in 2021-2022 with EUR 38 million; and research and innovation projects and coordination and support actions on health data quality and interoperability are already supported by Horizon Europe (Cluster 1) with EUR 108 million in 2021 and 2022, as well as EUR 59 million from the Research Infrastructures programme. Horizon Europe has also provided in 2021 and 2022 additional support for secondary use of health data dedicated to COVID-19 (EUR 42 million) and cancer (EUR 3 million).

Additionally, where physical connectivity is lacking in the health sector, Connecting Europe Facility will also *contribute to the development of projects of common interest relating to the deployment of and access to safe and secure very high capacity networks, including 5G systems, and to the increased resilience and capacity of digital backbone networks on Union territories*[38]. EUR 130 million are programmed in 2022 and 2023 for the interconnection of cloud infrastructures, including in health.

The Commission's administrative costs are estimated to be of approximately EUR 17 million, including costs for human resources and other administrative expenditure.

---

36 Article 5 of Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240.

37 Article 3, paragraph 2(a), of Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013.

38 Article 3, paragraph 2(c), of Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014.

The legislative financial statement attached to this proposal sets out the budgetary, human and administrative resource implications.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

Due to the dynamic nature of the digital tranformation of health, monitoring the trend in impacts arising from the EHDS will constitute a key part of the action in this domain. To ensure that the selected policy measures actually deliver the intended results and to inform possible future revisions, it is necessary to monitor and evaluate the implementation of this proposal.

Monitoring the specific objectives and the regulatory obligations will be achieved firstly through reporting by digital health authorities and health data access bodies. In addition, there will be monitoring of MyHealth@EU indicators and of the infrastructure for secondary uses of electronic health data.

The implementation of the infrastructures, particularly the implementation of the European platform of the new infrastructure for secondary uses of electronic health data, will be done in coherence with the overall IT governance framework of the European Commission. Therefore, IT development and procurement choices will be subject to pre-approval by the European Commission Information Technology and Cybersecurity Board.

- **Detailed explanation of the specific provisions of the proposal**

Chapter I presents the subject matter and the scope of the regulation, sets out the definitions used throughout the instrument and explains its relationship with other EU instruments.

Chapter II develops the additional rights and mechanisms designed to complement the natural person's rights provided under the GDPR in relation to their electronic health data. In addition, it describes the obligations of various health professionals in relation to electronic health data. Some type of electronic health data are identified as a priority to be integrated in the EHDS in a staged process with a transition period. Member States will have to set up a digital health authority responsible for monitoring these rights and mechanisms and for ensuring that these additional natural person's rights are properly implemented. This Chapter includes provisions related to the interoperability of certain health related datasets. Member States will also have to designate national contact point tasked with enforcing the obligations and requirement of this Chapter. Finally, a common infrastructure MyHealth@EU is designed to provide the infrastructure to facilitate cross-border exchange of electronic health data.

Chapter III focuses on implementing a mandatory self-certification scheme for EHR systems, where such systems must comply with essential requirements related to interoperability and security. This approach is required to ensure that electronic health records are compatible between each system and allow easy transmission of electronic health data between them. This Chapter defines the obligations of each economic operator of EHR systems, the requirements related to the conformity of such EHR systems, as well as the obligations of market surveillance authorities responsible for EHR systems in the context of their market surveillance activities. This Chapter also includes provisions on the voluntary labelling of wellness

applications, interoperable with EHR systems, and establishes an EU database where certified EHR systems and labelled wellness applications will be registered.

Chapter IV facilitates the secondary use of electronic health data, e.g. for research, innovation, policy making, patient safety or regulatory activities. It defines a set of data types that can be used for defined purposes, as well as prohibited purposes (e.g. use of data against persons, commercial advertising, increasing insurance, develop dangerous products). Member States will have to set up a health data access body for secondary use of electronic health data and ensure that electronic data are made available by data holders for data users. This Chapter also contains provisions on the implementation of data altruism in health. The duties and obligations of the health data access body, the data holders and the data users are also set out. In particular, data holders should cooperate with the health data access body to ensure availability of electronic health data for data users. Furthermore, responsabilities are defined for the health data access bodies and data users as joint controllers of the processed electronic health data.

The secondary use of electronic health data may involve costs. This chapter includes general provisions on transparency of fees calculation. On a practical level, requirements are in particular set out on security of the secure processing environment. Such a secure processing environment is required to access and process electronic health data under this Chapter. The conditions and the information needed in the data request form for obtaining access to electronic health data are listed in Section 3. Conditions attached to the issuance of the data permit are also described.

Section 4 of this Chapter mainly contains provisions on setting up and fostering cross-border access to electronic health data, so that a data user in one Member State can have access to electronic health data for secondary use from other Member States, without having to request a data permit from all these Member States. The cross-border infrastructure designed to enable such a process and its operation are also described.

Finally, this Chapter contains provisions related to dataset description and their quality. It would enable data users to ascertain the content and potential quality of the dataset used and allow them to assess wether these datasets were fit for purpose.

Chapter V aims to put forward other measures to promote capacity building by the Member States to accompany the development of the EHDS. These include exchange of information on digital public services, funding, etc. In addition, this Chapter regulates the international access to non-personal data in the EHDS.

Chapter VI creates the 'European Health Data Space Board' ('EHDS Board') that will facilitate the cooperation between digital health authorities and health data access bodies, in particular the relation between primary and secondary use of electronic health data. Dedicated sub-groups such as on primary use of electronic health data and on secondary use of electronic health data may be formed to focus on specific issues or process. The Board will be tasked with promoting the collaboration between digital health authorities and health data access bodies. This Chapter also provides for the composition of the Board and how its functioning is organised.

In addition, this Chapter contains provisions related to the joint controllership groups for EU infrastructure which will be tasked with taking decisions related to the cross-border digital infrastructure necessary, both for primary and secondary use of electronic health data.

Chapter VII allows the Commission to adopt delegated acts on the EHDS. Following the adoption of the proposal, the Commission intends to create an expert group in line with decision C (2016) 3301, in order to advise and assist it in the preparation of delegated acts, as well as on issues related to implementation of the Regulation as regards:

– delivering sustainable economic and social benefits of European digital health systems and 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;

– enhancing the interoperability of electronic health data for healthcare, building on existing European, international or national standards and experience of other data spaces;

– harmonised implementation of the access and sharing of electronic health data for primary use, at national and EU level;

– interoperability of EHR systems and of other products transmitting data to electronic health records, including medical devices, AI systems and wellness applications. Where relevant, the expert group shall cooperate with the Medical Devices Coordination Group and European Artificial Intelligence Board;

– minimum categories of electronic health data for secondary use;

– harmonised implementation of the access to electronic health data for secondary use, at national and EU level;

– data altruism activities in health sector;

– harmonised fees policy for secondary use of electronic health data;

– penalties applied by health data access bodies;

– minimal requirements and technical specifications for HealthData@EU and for secure processing environments;

– requirements and technical specifications for the data quality and utility label;

– minimum datasets;

– technical requirements to support data altruism in the health sector;

– other elements related to primary and secondary use of electronic health data.

The expert group may cooperate with and consult the Medical Devices Coordination Group and the European Artificial Intelligence Board, where relevant.

Chapter VIII contains provisions on cooperation and penalties and sets down final provisions.

2022/0140 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the European Health Data Space

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The aim of this Regulation is to establish the European Health Data Space ('EHDS') in order to improve access to and control by natural persons over their personal electronic health data in the context of healthcare (primary use of electronic health data), as well as for other purposes that would benefit the society such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities (secondary use of electronic health data). In addition, the goal is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of electronic health record systems ('EHR systems') in conformity with Union values.

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

---

1 OJ C , , p. .

2 OJ C , , p. .

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

this was only an emergency solution, showing the need for a structural approach at Member States and Union level.

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

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

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

(6) Chapter III of Regulation (EU) 2016/679 sets out specific provisions concerning the rights of natural persons in relation to the processing of their personal data. EHDS builds upon these rights and further develops some of them. The EHDS should support

---

4 EOSC Portal (eosc-portal.eu).

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

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

the coherent implementation of those rights as applied to electronic health data, regardless of the Member State in which the personal electronic health data are processed, type of healthcare provider, sources of data or Member State of affiliation of the natural person. The rights and rules related to the primary use of personal electronic health data under Chapter II and III of this Regulation concern all categories of those data, irrespective of how they have been collected or who has provided hem, of the legal ground for the processing under Regulation (EU) 2016/679 or the status of the controller as a public or private organisation of the legal ground for their processing.

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

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

(9) At the same time, it should be considered that immediate access to certain types of personal electronic health data may be harmful for the safety of natural persons, unethical or inappropriate. For example, it could be unethical to inform a patient through an electronic channel about a diagnosis with an incurable disease that is likely to lead to their swift passing instead of providing this information in a consultation with the patient first. Therefore, a possibility for limited exceptions in the implementation of this right should be ensured. Such an exception may be imposed by the Member States where this exception constitutes a necessary and proportionate

measure in a democratic society, in line with the requirements of Article 23 of Regulation (EU) 2016/679. Such restrictions should be implemented by delaying the display of the concerned personal electronic health data to the natural person for a limited period. Where health data is only available on paper, if the effort to make data available electronically is disproportionate, there should be no obligation that such health data is converted into electronic format by Member States. Any digital transformation in the healthcare sector should aim to be inclusive and benefit also natural persons with limited ability to access and use digital services. Natural persons should be able to provide an authorisation to the natural persons of their choice, such as to their relatives or other close natural persons, enabling them to access or control access to their personal electronic health data or to use digital health services on their behalf. Such authorisations may also be useful for convenience reasons in other situations. Proxy services should be established by Member States to implement these authorisations, and they should be linked to personal health data access services, such as patient portals on patient-facing mobile applications. The proxy services should also enable guardians to act on behalf of their dependent children; in such situations, authorisations could be automatic. In order to take into account cases in which the display of some personal electronic health data of minors to their guardians could be contrary to the interests or will of the minor, Member States should be able to provide for such limitations and safeguards in national law, as well as the necessary technical implementation. Personal health data access services, such as patient portals or mobile applications, should make use of such authorisations and thus enable authorised natural persons to access personal electronic health data falling within the remit of the authorisation, in order for them to produce the desired effect.

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

(11) Natural persons should be further empowered to exchange and to provide access to personal electronic health data to the health professionals of their choice, going beyond the right to data portability as established in Article 20 of Regulation (EU) 2016/679. This is necessary to tackle objective difficulties and obstacles in the current state of play. Under Regulation (EU) 2016/679, portability is limited only to data processed based on consent or contract, which excludes data processed under other legal bases, such as when the processing is based on law, for example when their processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It only concerns data provided by the data subject to a controller, excluding many inferred or indirect data, such as diagnoses, or tests. Finally, under Regulation (EU) 2016/679, the natural

person has the right to have the personal data transmitted directly from one controller to another only where technically feasible. That Regulation, however, does not impose an obligation to make this direct transmission technically feasible. All these elements limit the data portability and may limit its benefits for provision of high-quality, safe and efficient healthcare services to the natural person.

(12) Natural persons should be able to exercise control over the transmission of personal electronic health data to other healthcare providers. Healthcare providers and other organisations providing EHRs should facilitate the exercise of this right. Stakeholders such as healthcare providers, digital health service providers, manufacturers of EHR systems or medical devices should not limit or block the exercise of the right of portability because of the use of proprietary standards or other measures taken to limit the portability. For these reasons, the framework laid down by this Regulation builds on the right to data portability established in Regulation (EU) 2016/679 by ensuring that natural persons as data subjects can transmit their electronic health data, including inferred data, irrespective of the legal basis for processing the electronic health data. This right should apply to electronic health data processed by public or private controllers, irrespective of the legal basis for processing the data under in accordance with the Regulation (EU) 2016/679. This right should apply to all electronic health data.

(13) Natural persons may not want to allow access to some parts of their personal electronic health data while enabling access to other parts. Such selective sharing of personal electronic health data should be supported. However, such restrictions may have life threatening consequences and, therefore, access to personal electronic health data should be possible to protect vital interests as an emergency override. According to Regulation (EU) 2016/679, vital interests refer to situations in which it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal electronic health data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. More specific legal provisions on the mechanisms of restrictions placed by the natural person on parts of their personal electronic health data should be provided by Member States in national law. Because the unavailability of the restricted personal electronic health data may impact the provision or quality of health services provided to the natural person, he/she should assume responsibility for the fact that the healthcare provider cannot take the data into account when providing health services.

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

(15) Article 9(2), point (h), of Regulation (EU) 2016/679 provides for exceptions where the processing of senstitive data is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health care or treatment or the management of health care systems and services on the basis of Union or Member State law. This Regulation should provide conditions and safeguards for the processing of electronic

health data by healthcare providers and health professionals in line with Article 9(2), point (h), of Regulation (EU) 2016/679 with the purpose of accessing personal electronic health data provided by the natural person or transmitted from other healthcare providers. However, this Regulation should be without prejudice to the national laws concerning the processing of health data, including the legislation establishing categories of health professionals that can process different categories of electronic health data.

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

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

(18) Access and sharing of electronic health data should be enabled for all the data that exist in the EHR of a natural person, when technically feasible. However, some electronic health data may not be structured or coded, and the transmission between healthcare providers may be limited or only possible in formats that do not allow for

translation (when data is shared cross-borders). In order to provide enough time to prepare for implementation, dates of deferred application should be determined to allow for achieving legal, organisational, semantic and technical readiness for the transmission of different categories of electronic health data. When need for the exchange of new categories of electronic health data is identified, related dates of application should be determined in order to allow for the implementation of this exchange.

(19) The level of availability of personal health and genetic data in an electronic format varies between Member States. The EHDS should make it easier for natural persons to have those data available in electronic format. This would also contribute to the achievement of the target of 100% of Union citizens having access to their electronic health records by 2030, as referred to in the Policy Programme "Path to the Digital Decade". In order to make electronic health data accesible and transmissible, such data should be accessed and transmitted in an interoperable common European electronic health record exchange format, at least for certain categories of electronic health data, such as patient summaries, electronic prescriptions and dispensations, medical images and image reports, laboratory results and discharge reports, subject to transition periods. Where personal electronic health data is made available to a healthcare provider or a pharmacy by a natural person, or is transmitted by another data controller in the European electronic health record exchange format, the electronic health data should be read and accepted for the provision of healthcare or for dispensation of a medicinal product, thus supporting the provision of the health care services or the dispensation of the electronic prescription. Commission Recommendation (EU) 2019/243[7] provides the foundations for such a common European electronic health record exchange format. The use of European electronic health record exchange format should become more generalised at EU and national level. While the eHealth Network under Article 14 of Directive 2011/24/EU of the European Parliament and of the Council[8] recommended Member States to use the European electronic health record exchange format in procurements, in order to improve interoperability, uptake was limited in practice, resulting in fragmented landscape and uneven access to and portability of electronic health data.

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

---

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

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

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

(22) Regulation (EU) No 910/2014 of the European Parliament and of the Council[9] lays down the conditions under which Members States perform identification of natural persons in cross-border situations using identification means issued by another Member State, establishing rules for the mutual recognition of such electronic identification means. The EHDS requires a secure access to electronic health data, including in cross-border scenarios where the health professional and the natural person are from different Member States, to avoid cases of unauthorised access. At the same time, the existence of different means of electronic identification should not be a barrier for exercising the rights of natural persons and health professionals. The rollout of interoperable, cross-border identification and authentication mechanisms for natural persons and health professionals across the EHDS requires strengthening cooperation at Union level in the European Health Data Space Board ('EHDS Board').As the rights of the natural persons in relation to the access and transmission of personal electronic health data should be implemented uniformly across the Union, a strong governance and coordination is necessary at both Union and Member State level. Member States should establish relevant digital health authorities for the planning and implementation of standards for electronic health data access, transmission and enforcement of rights of natural persons and health professionals. In addition, governance elements are needed in Member States to facilitate the participation of national actors in the cooperation at Union level, channelling expertise and advising the design of solutions necessary to achieve the goals of the EHDS. Digital health authorities exist in most of the Member States and they deal with EHRs, interoperability, security or standardisation. Digital health authorities should be established in all Member States, as separate organisations or as part of the currently existing authorities.

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

[9] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

entities handling reimbursement schemes, health technology assessment bodies, medicinal products regulatory authorities and agencies, medical devices authorities, procurers and cybersecurity or e-ID authorities.

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

(25) In the context of MyHealth@EU, a central platform should provide a common infrastructure for the Member States to ensure connectivity and interoperability in an efficient and secure way. In order to guarantee compliance with data protection rules and to provide a risk management framework for the transmission of personal electronic health data, the Commission should, by means of implementing acts, allocate specific responsibilities among the Member States, as joint controllers, and prescribe its own obligations, as processor.

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

(27) In order to ensure respect for the rights of natural persons and health professionals, EHR systems marketed in the internal market of the Union should be able to store and transmit, in a secure way, high quality electronic health data. This is a key principle of

the EHDS to ensure the secure and free movement of electronic health data across the Union. To that end, a mandatory self-certification scheme for EHR systems processing one or more priority categories of electronic health data should be established to overcome market fragmentation while ensuring a proportionate approach. Through this self-certification, EHR systems should prove compliance with essential requirements on interoperability and security, set at Union level. In relation to security, essential requirements should cover elements specific to EHR systems, as more general security properties should be supported by other mechanisms such as cybersecurity schemes under Regulation (EU) 2019/881 of the European Parliament and of the Council[10].

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

(29) Software or module(s) of software which falls within the definition of a medical device or high-risk artificial intelligence (AI) system should be certified in accordance with Regulation (EU) 2017/745 of the European Parliament and of the Council[11] and Regulation […] of the European Parliament and of the Council [AI Act COM/2021/206 final], as applicable. The essential requirements on interoperability of this Regulation should only apply to the extent that the manufacturer of a medical device or high-risk AI system, which is providing electronic health data to be processed as part of the EHR system, claims interoperability with such EHR system. In such case, the provisions on common specifications for EHR systems should be applicable to those medical devices and high-risk AI systems.

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

(31) In order to guarantee effective exercise by patients of their rights under this Regulation, where healthcare providers develop and use an EHR system ‘in house’ to carry out internal activities without placing it on the market in return of payment or remuneration, they should also comply with this Regulation. In that context, such healthcare providers should comply with all requirements applicable to the manufacturers.

---

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

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

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

(33) Compliance with essential requirements on interoperability and security should be demonstrated by the manufacturers of EHR systems through the implementation of common specifications. To that end, implementing powers should be conferred on the Commission to determine such common specifications regarding datasets, coding systems, technical specifications, including standards, specifications and profiles for data exchange, as well as requirements and principles related to security, confidentiality, integrity, patient safety and protection of personal data as well as specifications and requirements related to identification management and the use of electronic identification. Digital health authorities should contribute to the development of such common specifications.

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

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

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

streamline and facilitate the flow of information. For medical devices and AI systems, the registration should be maintained under the existing databases established respectively under Regulations (EU) 2017/745 and […] [AI act COM/2021/206 final], but the compliance with interoperability requirements should be indicated when claimed by manufacturers, to provide information to procurers.

(37) For the secondary use of the clinical data for research, innovation, policy making, regulatory purposes, patient safety or the treatment of other natural persons, the possibilities offered by Regulation (EU) 2016/679 for a Union law should be used as a basis and rules and mechanisms and providing suitable and specific measures to safeguard the rights and freedoms of the natural persons. This Regulation provides the legal basis in accordance with Articles 9(2) (g), (h), (i) and (j) of Regulation (EU) 2016/679 for the secondary use of health data, establishing the safeguards for processing, in terms of lawful purposes, trusted governance for providing access to health data (through health data access bodies) and processing in a secure environment, as well as modalities for data processing, set out in the data permit. At the same time, the data applicant should demonstrate a legal basis pursuant to Article 6 of Regulation (EU) 2016/679, based on which they could request access to data pursuant to this Regulation and should fulfil the conditions set out in Chapter IV. More specifically: for processing of electronic health data held by the data holder pursuant to this Regulation, this Regulation creates the legal obligation in the sense of Article 6(1) point (c) of Regulation (EU) 2016/679 for disclosing the data by the data holder to health data access bodies, while the legal basis for the purpose of the initial processing (e.g. delivery of care) is unaffected. This Regulation also meets the conditions for such processing pursuant to Articles 9(2) (h),(i),(j) of the Regulation (EU) 2016/679. This Regulation assigns tasks in the public interest to the health data access bodies (running the secure processing environment, processing data before they are used, etc.) in the sense of Article 6(1)(e) of Regulation (EU) 2016/679 to the health data access bodies, and meets the requirements of Article 9(2)(h),(i),(j) of the Regulation (EU) 2016/679. Therefore, in this case, this Regulation provides the legal basis under Article 6 and meets the requirements of Article 9 of that Regulation on the conditions under which electronic health data can be processed. In the case where the user has access to electronic health data (for secondary use of data for one of the purposes defined in this Regulation), the data user should demonstrate its legal basis pursuant to Articles 6(1), points (e) or (f), of Regulation (EU) 2016/679 and explain the specific legal basis on which it relies as part of the application for access to electronic health data pursuant to this Regulation: on the basis of the applicable legislation, where the legal basis under Regulation (EU) 2016/679 is Article 6(1), point (e), or on Article 6(1), point (f), of Regulation (EU) 2016/679. If the user relies upon a legal basis offered by Article 6(1), point (e), it should make reference to another EU or national law, different from this Regulation, mandating the user to process personal health data for the compliance of its tasks. If the lawful ground for processing by the user is Article 6(1), point (f), of Regulation (EU) 2016/679, in this case it is this Regulation that provides the safeguards. In this context, the data permits issued by the health data access bodies are an administrative decision defining the conditions for the access to the data.

(38) In the context of the EHDS, the electronic health data already exists and is being collected by healthcare providers, professional associations, public institutions, regulators, researchers, insurers etc. in the course of their activities. Some categories of data are collected primarily for the provisions of healthcare (e.g. electronic health records, genetic data, claims data, etc.), others are collected also for other purposes

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

(39) The categories of electronic health data that can be processed for secondary use should be broad and flexible enough to accommodate the evolving needs of data users, while remaining limited to data related to health or known to influence health. It can also include relevant data from the health system (electronic health records, claims data, disease registries, genomic data etc.), as well as data with an impact on health (for example consumption of different substances, homelessness, health insurance, minimum income, professional status, behaviour, including environmental factors (for example, pollution, radiation, use of certain chemical substances). They can also include person-generated data, such as data from medical devices, wellness applications or other wearables and digital health applications. The data user who benefits from access to datasets provided under this Regulation could enrich the data with various corrections, annotations and other improvements, for instance by supplementing missing or incomplete data, thus improving the accuracy, completeness or quality of data in the dataset. To support the improvement of the original database and further use of the enriched dataset, the dataset with such improvements and a description of the changes should be made available free of charge to the original data holder. The data holder should make available the new dataset, unless it provides a justified notification against it to the health data access body, for instance in cases of low quality of the enrichment. Secondary use of non-personal electronic data should also be ensured. In particular, pathogen genomic data hold significant value for human health, as proven during the COVID-19 pandemic. Timely access to and sharing of such data has proven to be essential for the rapid development of detection tools, medical countermeasures and responses to public health threats. The greatest benefit from pathogen genomics effort will be achieved when public health and research processes share datasets and work mutually to inform and improve each other.

(40) The data holders can be public, non for profit or private health or care providers, public, non for profit and private organisations, associations or other entities, public and private entities that carry out research with regards to the health sector that process the categories of health and health related data mentioned above. In order to avoid a disproportionate burden on small entities, micro-enterprises are excluded from the obligation to make their data available for secondary use in the framework of EHDS. The public or private entities often receive public funding, from national or Union funds to collect and process electronic health data for research, statistics (official or not) or other similar purposes, including in area where the collection of such data is fragmented of difficult, such as rare diseases, cancer etc. Such data, collected and processed by data holders with the support of Union or national public funding, should

be made available by data holders to health data access bodies, in order to maximise the impact of the public investment and support research, innovation, patient safety or policy making benefitting the society. In some Member States, private entities, including private healthcare providers and professional associations, play a pivotal role in the health sector. The health data held by such providers should also be made available for secondary use. At the same time, data benefiting from specific legal protection such as intellectual property from medical device companies or pharmaceutical companies often enjoy copyright protection or similar types of protection. However, public authorities and regulators should have access to such data, for instance in the event of pandemics, to verify defective devices and protect human health. In times of severe public health concerns (for example, PIP breast implants fraud) it appeared very difficult for public authorities to get access to such data to understand the causes and knowledge of manufacturer concerning the defects of some devices. The COVID-19 pandemic also revealed the difficulty for policy makers to have access to health data and other data related to health. Such data should be made available for public and regulatory activities, supporting public bodies to carry out their legal mandate, while complying with, where relevant and possible, the protection enjoyed by commercial data. Specific rules in relation to the secondary use of health data should be provided. Data altruism activities may be carried out by different entities, in the context of Regulation […] [Data Governance Act COM/2020/767 final] and taking into account the specificities of the health sector.

(41) The secondary use of health data under EHDS should enable the public, private, not for profit entities, as well as individual researchers to have access to health data for research, innovation, policy making, educational activities, patient safety, regulatory activities or personalised medicine, in line with the purposes set out in this Regulation. Access to data for secondary use should contribute to the general interest of the society. Activities for which access in the context of this Regulation is lawful may include using the electronic health data for tasks carried out by public bodies, such as exercise of public duty, including public health surveillance, planning and reporting duties, health policy making, ensuring patient safety, quality of care, and the sustainability of health care systems. Public bodies and Union institutions, bodies, offices and agencies may require to have regular access to electronic health data for an extended period of time, including in order to fulfil their mandate, which is provided by this Regulation. Public sector bodies may carry out such research activities by using third parties, including sub-contractors, as long as the public sector body remain at all time the supervisor of these activities. The provision of the data should also support activities related to scientific research (including private research), development and innovation, producing goods and services for the health or care sectors, such as innovation activities or training of AI algorithms that could protect the health or care of natural persons. In some cases, the information of some natural persons (such as genomic information of natural persons with a certain disease) could support the diagnosis or treatment of other natural persons. There is a need for public bodies to go beyond the emergency scope of Chapter V of Regulation […] [Data Act COM/2022/68 final]. However, the public sector bodies may request the support of health data access bodies for processing or linking data. This Regulation provides a channel for public sector bodies to obtain access to information that they require for fulfilling their tasks assigned to them by law, but does not extend the mandate of such public sector bodies. Any attempt to use the data for any measures detrimental to the natural person, to increase insurance premiums, to advertise products or treatments, or develop harmful products should be prohibited.

(42) The establishment of one or more health data access bodies, supporting access to electronic health data in Member States, is an essential component for promoting the secondary use of health-related data. Member States should therefore establish one or more health data access body, for instance to reflect their constitutional, organisational and administrative structure. However, one of these health data access bodies should be designated as a coordinator in case there are more than one data access body. Where a Member State establishes several bodies, it should lay down rules at national level to ensure the coordinated participation of those bodies in the EHDS Board. That Member State should in particular designate one health data access body to function as a single contact point for the effective participation of those bodies, and ensure swift and smooth cooperation with other health data access bodies, the EHDS Board and the Commission. Health data access bodies may vary in terms of organisation and size (spanning from a dedicated full-fledged organization to a unit or department in an existing organization) but should have the same functions, responsibilities and capabilities. Health data access bodies should not be influenced in their decisions on access to electronic data for secondary use. However, their independence should not mean that the health data access body cannot be subject to control or monitoring mechanisms regarding its financial expenditure or to judicial review. Each health data access body should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of its tasks, including those related to cooperation with other health data access bodies throughout the Union. Each health data access body should have a separate, public annual budget, which may be part of the overall state or national budget. In order to enable better access to health data and complementing Article 7(3) of Regulation […] of the European Parliament and of the Council [Data Governance Act COM/2020/767 final], Member States should entrust health data access bodies with powers to take decisions on access to and secondary use of health data. This could consist in allocating new tasks to the competent bodies designated by Member States under Article 7(1) of Regulation […] [Data Governance Act COM/2020/767 final] or in designating existing or new sectoral bodies responsible for such tasks in relation to access to health data.

(43) The health data access bodies should monitor the application of Chapter IV of this Regulation and contribute to its consistent application throughout the Union. For that purpose, the health data access bodies should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation. The health data access bodies should also cooperate with stakeholders, including patient organisations. Since the secondary use of health data involves the processing of personal data concerning health, the relevant provisions of Regulation (EU) 2016/679 apply and the supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 should be tasked with enforcing these rules. Moreover, given that health data are sensitive data and in a duty of loyal cooperation, the health data access bodies should inform the data protection authorities of any issues related to the data processing for secondary use, including penalties. In addition to the tasks necessary to ensure effective secondary use of health data, the health data access body should strive to expand the availability of additional health datasets, support the development of AI in health and promote the development of common standards. They should apply tested techniques that ensure electronic health data is processed in a manner that preserves the privacy of the information contained in the data for which secondary use is allowed, including techniques for pseudonymisation, anonymisation, generalisation, suppression and randomisation of personal data. Health data access bodies can prepare datasets to the

data user requirement linked to the issued data permit. This includes rules for anonymization of microdata sets.

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

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

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

(47) Health data access bodies and single data holders should be allowed to charge fees based on the provisions of Regulation […] [Data Governance Act COM/2020/767 final] in relation to their tasks. Such fees may take into account the situation and interest of SMEs, individual researchers or public bodies. Data holders should be allowed to also charge fees for making data available. Such fees should reflect the costs for providing such services. Private data holders may also charge fees for the collection of data. In order to ensure a harmonised approach concerning fee policies and structure, the Commission may adopt implementing acts. Provisions in Article 10 of the Regulation [Data Act COM/2022/68 final] should apply for fees charged under this Regulation.

(48) In order to strengthen the enforcement of the rules on the secondary use of electronic health data, appropriate measures that can lead to penalties or temporary or definitive exclusions from the EHDS framework of the data users or data holders that do not comply with their obligations. The health data access body should be empowered to verify compliance and give data users and holders the opportunity to reply to any findings and to remedy any infringement. The imposition of penalties should be subject to appropriate procedural safeguards in accordance with the general principles of law of the relevant Member State, including effective judicial protection and due process.

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

(50) In order to ensure that all health data access bodies issue permits in a similar way, it is necessary to establish a standard common process for the issuance of data permits, with similar requests in different Member States. The applicant should provide health data access bodies with several information elements that would help the body evaluate the request and decide if the applicant may receive a data permit for secondary use of data, also ensuring coherence between different health data access bodies. Such information include: the legal basis under Regulation (EU) 2016/679 to request access to data (exercise of a task in the public interest assigned by law or legitimate interest), purposes for which the data would be used, description of the needed data and possible data sources, a description of the tools needed to process the data, as well as characteristics of the secure environment that are needed. Where data is requested in pseudonymised format, the data applicant should explain why this is necessary and why anonymous data would not suffice. An ethical assessment may be requested based on national law. The health data access bodies and, where relevant data holders, should assist data users in the selection of the suitable datasets or data sources for the intended purpose of secondary use. Where the applicant needs anonymised statistical data, it should submit a data request application, requiring the health data access body to provide directly the result. In order to ensure a harmonised approach between health data access bodies, the Commission should support the harmonisation of data application, as well as data request.

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

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

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

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

(55) For the processing of electronic health data in the scope of a granted permit, the health data access bodies and the data users should be joint controllers in the sense of Article 26 of Regulation (EU) 2016/679, meaning that the obligations of joint controllers under that Regulation will apply. To support health data access bodies and data users, the Commission should, by means of an implementing act, provide a template for the joint controller arrangements health data access bodies and data users will have to enter into. In order to achieve an inclusive and sustainable framework for multi-country secondary use of electronic health data, a cross-border infrastructure should be established. HealthData@EU should accelerate the secondary use of electronic health data while increasing legal certainty, respecting the privacy of natural persons and being interoperable. Due to the sensitivity of health data, principles such as "privacy by design" and "bring questions to data instead of moving data" should be respected whenever possible. Authorised participants in HealthData@EU could be health data access bodies, research infrastructures established as an European Research Infrastructure Consortium ('ERIC') under Council Regulation (EC) No 723/2009[12] or similar structures established under another Union legislation, as well as other types of entities, including infrastructures under the European Strategy Forum on Research Infrastructures (ESFRI), infrastructures federated under the European Open Science Cloud (EOSC). Other authorised participants should obtain the approval of the joint controllership group for joining HealthData@EU. On the other hand, HealthData@EU should enable the secondary use of different categories of electronic health data, including linking of the health data with data from other data spaces such as environment, agriculture, social etc. The Commission could provide a number of services within HealthData@EU, including supporting the exchange of information amongst health data access bodies and authorised participants for the handling of cross-border access requests, maintaining catalogues of electronic health data available through the infrastructure, network discoverability and metadata queries, connectivity and compliance services. The Commission may also set up a secure environment, allowing data from different national infrastructures to be transmitted and analysed, at the request of the controllers. The Commission digital strategy promote the linking of the various common European data spaces. For the health sector, interoperability with the sectors such as the environmental, social, agricultural sectors may be relevant for additional insights on health determinants. For the sake of IT efficiency, rationalisation and interoperability of data exchanges, existing systems for data sharing should be reused as much as possible, like those being built for the exchange of evidences under the once only technical system of Regulation (EU) 2018/1724 of the European Parliament and of the Council[13].

(56) In case of cross-border registries or databases, such as the registries of European Reference Networks for Rare Diseases, which receive data from different healthcare providers in several Member States, the health data access body where the coordinator of the registry is located should be responsible for providing access to data.

(57) The authorisation process to gain access to personal health data in different Member States can be repetitive and cumbersome for data users. Whenever possible, synergies

---

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

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

should be established to reduce the burden and barriers for data users. One way to achieve this aim is to adhere to the "single application" principle whereby, with one application, the data user obtain authorisation from multiple health data access bodies in different Member States.

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

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

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

(61) Cooperation and work is ongoing between different professional organisations, the Commission and other institutions to set up minimum data fields and other characteristics of different datasets (registries for instance). This work is more advanced in areas such as cancer, rare diseases, and statistics and shall be taken into account when defining new standards. However, many datasets are not harmonised, raising comparability issues and making cross-border research difficult. Therefore,

more detailed rules should be set out in implementing acts to ensure a harmonised provision, coding and registration of electronic health data. Member States should work towards delivering sustainable economic and social benefits of European electronic health systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of healthcare and ensuring access to safe and high-quality healthcare.

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

(63) The use of funds should also contribute to attaining the objectives of the EHDS. Public procurers, national competent authorities in the Member States, including digital health authorities and health data access bodies, as well as the Commission should make references to applicable technical specifications, standards and profiles on interoperability, security and data quality, as well as other requirements developed under this Regulation when defining the conditions for public procurement, calls for proposals and allocation of Union funds, including structural and cohesion funds.

(64) Certain categories of electronic health data can remain particularly sensitive even when they are in anonymised format and thus non-personal, as already specifically foreseen in the Data Governance Act. Even in situations of the use of state of the art anonymization techniques, there remains a residual risk that the capacity to re-identify could be or become available, beyond the means reasonably likely to be used. Such residual risk is present in relation to rare diseases (a life-threatening or chronically debilitating condition affecting not more than five in 10 thousand persons in the Union), where the limited numbers of case reduce the possibility to fully aggregate the published data in order to preserve the privacy of natural persons while also maintaining an appropriate level of granularity in order to remain meaningful. It can affect different types of health data depending on the level of granularity and description of the characteristics of data subjects, the number of people affected or and for instance in cases of data included in electronic health records, disease registries, biobanks, person generated data etc. where the identification characteristics are broader and where, in combination with other information (e.g. in very small geographical areas) or through the technological evolution of methods which had not been available at the moment of anonymisation, can lead to the re-identification of the data subjects using means that are beyond those reasonably likely to be used. The realisation of such risk of re-identification of natural persons would present a major concern and is likely to put the acceptance of the policy and rules on secondary use provided for in this Regulation at risk. Furthermore, aggregation techniques are less tested for non-personal data containing for example trade secrets, as in the reporting on clinical trials, and enforcement of breaches of trade secrets outside the Union is more difficult in the absence of a sufficient international protection standard. Therefore, for these types of health data, there remains a risk for re-identification after the anonymisation or aggregation, which could not be reasonably mitigated initially. This falls within the criteria indicated in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final]. These types of health data would thus fall within the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final] for transfer to third countries. The protective measures, proportional to the risk of re-identification, would need to take into account the

specificities of different data categories or of different anonymization or aggregation techniques and will be detailed in the context of the Delegated Act under the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final].

(65) In order to promote the consistent application of this Regulation, a European Health Data Space Board (EHDS Board) should be set up. The Commission should participate in its activities and chair it. It should contribute to the consistent application of this Regulation throughout the Union, including by helping Member State to coordinate the use of electronic health data for healthcare, certification, but also concerning the secondary use of electronic health data. Given that, at national level, digital health authorities dealing with the primary use of electronic health data may be different to the health data access bodies dealing with the secondary use of electronic health data, the functions are different and there is a need for distinct cooperation in each of these areas, the EHDS Board should be able to set up subgroups dealing with these two functions, as well as other subgroups, as needed. For an efficient working method, the digital health authorities and health data access bodies should create networks and links at national level with different other bodies and authorities, but also at Union level. Such bodies could comprise data protection authorities, cybersecurity, eID and standardisation bodies, as well as bodies and expert groups under Regulations […], […], […] and […] [Data Governance Act, Data Act, AI Act and Cybersecurity Act].

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

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

(68) In order to ensure that EHDS fulfils its objectives, the power to adopt acts in accordance with Article 290 Treaty on the Functioning of the European Union should be delegated to the Commission in respect of different provisions of primary and secondary use of electronic health data. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better

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

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

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

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

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

(73) The evaluation of the digital aspects of Directive 2011/24/EU shows limited effectiveness of eHealth Network, but also strong potential for EU work in this area, as shown by the work during pandemic. Therefore, the article 14 of the Directive will be repealed and replaced by the current Regulation and the Directive will be amended accordingly.

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

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

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

---

14 OJ L 123, 12.5.2016, p. 1.

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

16 European Commission, European Interoperability Framework.

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 rules, common standards and practices, infrastructures and a governance framework for the primary and secondary use of electronic health data.

2. This Regulation:

   (a) strengthens the rights of natural persons in relation to the availability and control of their electronic health data;

   (b) lays down rules for the placing on the market, making available on the market or putting into service of electronic health records systems ('EHR systems') in the Union;

   (c) lays down rules and mechanisms supporting the secondary use of electronic health data;

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

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

3. This Regulation applies to:

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

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

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

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

4. This Regulation shall be without prejudice to other Union legal acts regarding access to, sharing of or secondary use of electronic health data, or requirements related to the processing of data in relation to electronic health data, in particular Regulations (EU) 2016/679, (EU) 2018/1725, […] [Data Governance Act COM/2020/767 final] and […] [Data Act COM/2022/68 final].

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

6. This Regulation shall not affect the rights and obligations laid down in Union or national law concerning data processing for the purposes of reporting, complying with information requests or demonstrating or verifying compliance with legal obligations.

Article 2

Definitions

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

   (a) the definitions in Regulation (EU) 2016/679;

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

   (c) the definitions of 'data', 'access', 'data altruism', 'public sector body' and 'secure processing environment', pursuant to Article 2 (1), (8), (10), (11) and (14) of [Data Governance Act COM/2020/767 final];

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

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

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

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

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

   (b) 'non-personal electronic health data' means data concerning health and genetic data in electronic format that falls outside the definition of personal data provided in Article 4(1) of Regulation (EU) 2016/679;

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

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

(e) ‘secondary use of electronic health data’ means the processing of electronic health data for purposes set out in Chapter IV of this Regulation. The data used may include personal electronic health data initially collected in the context of primary use, but also electronic health data collected for the purpose of the secondary use;

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

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

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

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

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

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

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

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

(n) ‘EHR system’ (electronic health record system) means any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records;

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

(p) ‘CE marking of conformity’ means a marking by which the manufacturer indicates that the EHR system is in conformity with the applicable

requirements set out in this Regulation and other applicable Union legislation providing for its affixing;

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

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

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

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

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

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

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

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

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

(y) ‘data holder’ means any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data;

(z) ‘data user’ means a natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use;

(aa) ‘data permit’ means an administrative decision issued to a data user by a health data access body or data holder to process the electronic health data specified in the data permit for the secondary use purposes specified in the data permit based on conditions laid down in this Regulation;

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

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

(ad) ‘data quality’ means the degree to which characteristics of electronic health data are suitable for secondary use;

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

Chapter II

Primary use of electronic health data

SECTION 1

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

Article 3

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

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

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

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

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

5. Member States shall:

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

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

The proxy services shall provide authorisations free of charge, electronically or on paper. They shall enable guardians or other representatives to be authorised, either automatically or upon request, to access electronic health data of the natural persons whose affairs they administer. Member States may provide that authorisations do not apply whenever necessary for reasons related to the protection of the natural person, and in particular based on patient safety and ethics. The proxy services shall be interoperable among Member States.

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

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

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

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

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

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

9. Notwithstanding Article 6(1), point (d), of Regulation (EU) 2016/679, natural persons shall have the right to restrict access of health professionals to all or part of their electronic health data. Member States shall establish the rules and specific safeguards regarding such restriction mechanisms.

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

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

this Regulation shall, where relevant, cooperate in the enforcement of this Regulation, within the remit of their respective competences.

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

Article 4

Access by health professionals to personal electronic health data

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

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

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

2. In line with the data minimisation principle provided for in Regulation (EU) 2016/679, Member States may establish rules providing for the categories of personal electronic health data required by different health professions. Such rules shall not be based on the source of electronic health data.

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

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

Article 5

Priority categories of personal electronic health data for primary use

1. Where data is processed in electronic format, Member States shall implement access to and exchange of personal electronic health data for primary use fully or partially falling under the following categories:

   (a) patient summaries;

   (b) electronic prescriptions;

   (c) electronic dispensations;

(d) medical images and image reports;

(e) laboratory results;

(f) discharge reports.

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

Access to and exchange of electronic health data for primary use may be enabled for other categories of personal electronic health data available in the EHR of natural persons.

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

(a) the category is relevant for health services provided to natural persons;

(b) according to the most recent information, the category is used in a significant number of EHR systems used in Member States;

(c) international standards exist for the category that have been examined for the possibility of their application in the Union.

Article 6

European electronic health record exchange format

1. The Commission shall, by means of implementing acts, lay down the technical specifications for the priority categories of personal electronic health data referred to in Article 5, setting out the European electronic health record exchange format. The format shall include the following elements:

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

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

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

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

3. Member States shall ensure that the priority categories of personal electronic health data referred to in Article 5 are issued in the format referred to in paragraph 1 and such data shall be read and accepted by the data recipient.

Article 7

Registration of personal electronic health data

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

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

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

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

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

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

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

Article 8

Telemedicine in the context of cross-border healthcare

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

Article 9

Identification management

1. Where a natural person uses telemedicine services or personal health data access services referred to in Article 3(5), point (a), that natural person shall have the right to identify electronically using any electronic identification means which is recognised pursuant to Article 6 of Regulation (EU) No 910/2014.

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

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

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

Article 10

Digital health authority

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) measures taken to implement this Regulation;

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 11

Right to lodge a complaint with a digital health authority

1. Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the digital health authority. Where the complaint concerns the rights of natural persons pursuant to Article 3 of this Regulation, the digital health authority shall inform the supervisory authorities under Regulation (EU) 2016/679.

2. The digital health authority with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken.

3. Digital health authorities shall cooperate to handle and resolve complaints, including by exchanging all relevant information by electronic means, without undue delay.

SECTION 2

CROSS-BORDER INFRASTRUCTURE FOR PRIMARY USE OF ELECTRONIC HEALTH DATA

Article 12

MyHealth@EU

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

2. Each Member State shall designate one national contact point for digital health to ensure the connection to all other national contact points for digital health and to the

central platform for digital health. Where a designated national contact point is an entity consisting of multiple organisations responsible for implementing different services, the Member State shall communicate to the Commission a description of the separation of tasks between the organisations. The national contact point for digital health shall be considered an authorised participant in the infrastructure. Each Member State shall communicate the identity of its national contact point to the Commission by [*the date of application of this Regulation*]. Such contact point may be established within the digital health authority established by Article 10 of this Regulation. Member States shall communicate to the Commission any subsequent modification of the identity of those contact points. The Commission and the Member States shall make this information publicly available.

3. Each national contact point for digital health shall enable the exchange of the personal electronic health data referred to in Article 5 with all other national contact points. The exchange shall be based on the European electronic health record exchange format.

4. The Commission shall, by means of implementing acts, adopt the necessary measures for the technical development of MyHealth@EU, detailed rules concerning the security, confidentiality and protection of electronic health data and the conditions and compliance checks necessary to join and remain connected to MyHealth@EU and conditions for temporary or definitive exclusion from MyHealth@EU. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

5. Member States shall ensure connection of all healthcare providers to their national contact points for digital health and shall ensure that those connected are enabled to perform two-way exchange of electronic health data with the national contact point for digital health.

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

7. The national contact points for digital health shall act as joint controllers of the 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, allocate responsibilities among controllers and as regards the processor referred to in paragraph 7 of this Article, in accordance with Chapter IV of Regulation (EU) 2016/679. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

9. The approval for individual authorised participants to join MyHealth@EU for different services, or to disconnect a participant shall be issued by the Joint Controllership group, based on the results of the compliance checks.

Article 13

Supplementary cross-border digital health services and infrastructures

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

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

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

   The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the procedure referred to in Article 68. The connection of the national contact point of the third country or of the system established at an international level to the central platform for digital health, as well as the decision to be disconnected shall be subject to a decision of the joint controllership group for MyHealth@EU referred to in Article 66.

   The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available.

CHAPTER III

EHR systems and wellness applications

SECTION 1

GENERAL PROVISIONS FOR EHR SYSTEMS

Article 14

Interplay with legislation governing medical devices and AI systems

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

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

3. Manufacturers of medical devices as defined in Article 2(1) of Regulation (EU) 2017/745 that claim interoperability of those medical devices with EHR systems shall prove compliance with the essential requirements on interoperability laid down in Section 2 of Annex II of this Regulation. Article 23 of this Chapter shall be applicable to those medical devices.

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

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

Article 15

Placing on the market and putting into service

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

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

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

Article 16

Claims

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

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

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

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

SECTION 2

OBLIGATIONS OF ECONOMIC OPERATORS WITH REGARD TO EHR SYSTEMS

Article 17

Obligations of manufacturers of EHR systems

1. Manufacturers of EHR systems shall:

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

(b) draw up the technical documentation of their EHR systems in accordance with Article 24;

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

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

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

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

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

(h) inform the distributors of their EHR systems and, where applicable, the authorised representative and importers of any corrective action, recall or withdrawal;

(i) inform the market surveillance authorities of the Member States in which they made their EHR systems available or put them into service of the non-conformity and of any corrective action taken;

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

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

2. Manufacturers of EHR systems shall ensure that procedures are in place to ensure that the design, development and deployment of an EHR system continues to comply with the essential requirements laid down in Annex II and the common specifications referred to in Article 23. Changes in EHR system design or characteristics shall be adequately taken into account and reflected in the technical documentation.

3. Manufacturers of EHR systems shall keep the technical documentation and the EU declaration of conformity for 10 years after the last EHR system covered by the EU declaration of conformity has been placed on the market.

Article 18

Authorised representatives

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

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

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

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

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

Article 19

Obligations of importers

1. Importers shall place on the Union market only EHR systems which are in conformity with the essential requirements laid down in Annex II.

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

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

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

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

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

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

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

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

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

Article 20

Obligations of distributors

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

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

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

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

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

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

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

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, on any action taken to bring their EHR systems in conformity with the essential requirements laid down in Annex II.

Article 21

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

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

Article 22

Identification of economic operators

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

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

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

SECTION 3

CONFORMITY OF THE EHR SYSTEM

Article 23

Common specifications

1. The Commission shall, by means of implementing acts, adopt common specifications in respect of the essential requirements set out in Annex II, including a time limit for implementing those common specifications. Where relevant, the common specifications shall take into account the specificities of medical devices and high risk AI systems referred to in paragraphs 3 and 4 of Article 14.

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

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

   (a) scope;

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

   (c) version;

   (d) validity period;

   (e) normative part;

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

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

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

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

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

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

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

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

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

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

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

Article 24

Technical documentation

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

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

3. The technical documentation shall be drawn up in one of the official languages of the Union. Following a reasoned request from the market surveillance authority of a

Member State, the manufacturer shall provide a translation of the relevant parts of the technical documentation into the official language of that Member State.

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

Article 25

Information sheet accompanying the EHR system

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

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

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

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

   (c) its intended purpose;

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

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

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

Article 26

EU declaration of conformity

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

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

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

4. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the conformity of the EHR system.

Article 27

CE marking

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

2. The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) 765/2008 of the European Parliament and of the Council[20].

SECTION 4

MARKET SURVEILLANCE OF EHR SYSTEMS

Article 28

Market surveillance authorities

1. Regulation (EU) 2019/1020 shall apply to EHR systems covered by Chapter III of this Regulation.

2. Member States shall designate the market surveillance authority or authorities responsible for the implementation of this Chapter. They shall entrust their market surveillance authorities with the powers, resources, equipment and knowledge necessary for the proper performance of their tasks pursuant to this Regulation. Member States shall communicate the identity of the market surveillance authorities to the Commission which shall publish a list of those authorities.

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

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

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

6. For medical devices or high-risk AI systems referred to in Article 14 (3) and (4), the responsible authorities for market surveillance shall be those referred to in Article 93 of Regulation (EU) 2017/745 or Article 59 of Regulation […] [AI act COM/2021/206 final], as applicable.

---

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

Article 29

Handling of risks posed by EHR systems and of serious incidents

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

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

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

4. Manufacturers of EHR systems placed on the market shall report any serious incident involving an EHR system to the market surveillance authorities of the Member States where such serious incident occurred and the corrective actions taken or envisaged by the manufacturer.

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

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

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

Article 30

Handling of non-compliance

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

   (a) the EHR system is not in conformity with essential requirements laid down in Annex II;

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

(c) the EU declaration of conformity has not been drawn up or has not been drawn up correctly;

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

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

SECTION 5

OTHER PROVISIONS ON INTEROPERABILITY

Article 31

Voluntary labelling of wellness applications

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

2. The label shall indicate the following information:

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

(b) reference to common specifications to demonstrate compliance;

(c) validity period of the label.

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

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

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

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

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

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

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

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

Article 32

Registration of EHR systems and wellness applications

1. The Commission shall establish and maintain a publicly available database with information on EHR systems for which an EU declaration of conformity has been issued pursuant to Article 26 and wellness applications for which a label has been issued pursuant to Article 31.
2. Before placing on the market or putting into service an EHR system referred to in Article 14 or a wellness application referred to in Article 31, the manufacturer of such EHR system or wellness application or, where applicable, its authorised representative shall register the required data into the EU database referred to in paragraph 1.
3. Medical devices or high-risk AI systems referred to in paragraphs 3 and 4 of Article 14 of this Regulation shall be registered in the database established pursuant to Regulations (EU) 2017/745 or […] [AI Act COM/2021/206 final], as applicable.
4. The Commission is empowered to adopt delegated acts in accordance with Article 67 to determine the list of required data to be registered by the manufacturers of EHR systems and wellness applications pursuant to paragraph 2.

CHAPTER IV

Secondary use of electronic health data

SECTION 1

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

Article 33

Minimum categories of electronic data for secondary use

1. Data holders shall make the following categories of electronic data available for secondary use in accordance with the provisions of this Chapter:
   (a) EHRs;
   (b) data impacting on health, including social, environmental behavioural determinants of health;
   (c) relevant pathogen genomic data, impacting on human health;
   (d) health-related administrative data, including claims and reimbursement data;
   (e) human genetic, genomic and proteomic data;
   (f) person generated electronic health data, including medical devices, wellness applications or other digital health applications;

(g) identification data related to health professionals involved in the treatment of a natural person;

(h) population wide health data registries (public health registries);

(i) electronic health data from medical registries for specific diseases;

(j) electronic health data from clinical trials;

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

(l) research cohorts, questionnaires and surveys related to health;

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

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

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

2. The requirement in the first subparagraph shall not apply to data holders that qualify as micro enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC[21].

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

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

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

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

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

8. Health data access bodies may provide access to additional categories of electronic health data that they have been entrusted with pursuant to national law or based on

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

voluntary cooperation with the relevant data holders at national level, in particular to electronic health data held by private entities in the health sector.

Article 34

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

1. Health data access bodies shall only provide access to electronic health data referred to in Article 33 where the intended purpose of processing pursued by the applicant complies with:

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

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

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

   (d) education or teaching activities in health or care sectors;

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

   (f) development and innovation activities for products or services contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;

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

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

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

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

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

Article 35

Prohibited secondary use of electronic health data

Seeking access to and processing electronic health data obtained via a data permit issued pursuant to Article 46 for the following purposes shall be prohibited:

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

(b) taking decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract or to modify their contributions and insurance premiums;

(c) advertising or marketing activities towards health professionals, organisations in health or natural persons;

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

(e) developing products or services that may harm individuals and societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco products, or goods or services which are designed or modified in such a way that they contravene public order or morality.

SECTION 2

GOVERNANCE AND MECHANISMS FOR THE SECONDARY USE OF ELECTRONIC HEALTH DATA

Article 36

Health data access bodies

1. Member States shall designate one or more health data access bodies responsible for granting access to electronic health data for secondary use. 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. Where a Member State designates several health data access bodies, it shall designate one health data access body to act as coordinator, with responsibility for coordinating requests with the other health data access bodies.

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

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

4. Member States shall communicate to the Commission the identity of the health data access bodies designated pursuant to paragraph 1 by the date of application of this Regulation. They shall also communicate to the Commission any subsequent

modification of the identity of those bodies. The Commission and the Member States shall make this information publicly available.

Article 37

Tasks of health data access bodies

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(q) make public, through electronic means:

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

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

(iii) penalties applied pursuant to Article 43;

(iv) results communicated by data users pursuant to Article 46(11);

(r) fulfil obligations towards natural persons pursuant to Article 38;

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

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

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

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

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

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

(d) cooperate with other national competent bodies, including the national competent bodies supervising data altruism organisations under Regulation […] [Data Governance Act COM/2020/767 final], the competent authorities under Regulation […] [Data Act COM/2022/68 final] and the national

competent authorities for Regulations (EU) 2017/745 and Regulation […] [AI Act COM/2021/206 final] .

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

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

Article 38

Obligations of health data access bodies towards natural persons

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

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

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

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

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

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

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

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

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

Article 39

Reporting by health data access bodies

1. Each health data access body shall publish an annual activity report which shall contain at least the following:

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

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

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

(d) information on audits carried out on data users to ensure compliance of the processing with this Regulation,

(e) information on audits on compliance of secure processing environments with the defined standards, specifications and requirements*;*

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

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

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

(i) revenues from data permits and data requests;

(j) satisfaction from applicants requesting access to data;

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

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

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

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

2. The report shall be transmitted to the Commission.

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

Article 40

Data altruism in health

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

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

Article 41

Duties of data holders

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

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

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

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

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

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

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

Article 42

Fees

1. Health data access bodies and single data holders may charge fees for making electronic health data available for secondary use. Any fees shall include and be derived from the costs related to conducting the procedure for requests, including for assessing a data application or a data request, granting, refusing or amending a data permit pursuant to Articles 45 and 46 or providing an answer to a data request pursuant to Article 47, in accordance with Article 6 of Regulation […] [Data Governance Act COM/2020/767 final]

2. Where the data in question are not held by the data access body or a public sector body, the fees may also include compensation for part of the costs for collecting the electronic health data specifically under this Regulation in addition to the fees that may be charged pursuant to paragraph 1. The part of the fees linked to the data holder's costs shall be paid to the data holder.

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

4. Any fees charged to data users pursuant to this Article by the health data access bodies or data holders shall be transparent and proportionate to the cost of collecting

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

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

6. The Commission may, by means of implementing acts, lay down principles and rules for the fee policies and fee structures. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

Article 43

Penalties by health data access bodies

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

2. When requesting from data users and data holders the information that is necessary to verify compliance with this Chapter, the health data access bodies shall be proportionate to the performance of the compliance verification task.

3. Where health data access bodies find that a data user or data holder does not comply with the requirements of this Chapter, they shall immediately notify the data user or data holder of those findings and shall give it the opportunity to state its views within 2 months.

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

5. Where data holders withhold the electronic health data from health data access bodies with the manifest intention of obstructing the use of electronic health data, or do not respect the deadlines set out in Article 41, the health data access body shall have the power to fine the data holder with fines for each day of delay, which shall be transparent and proportionate. The amount of the fines shall be established by the health data access body. In case of repeated breaches by the data holder of the obligation of loyal cooperation with the health data access body, that body can exclude the data holder from participation in the EHDS for a period of up to 5 years. Where a data holder has been excluded from the participation in the EHDS pursuant to this Article, following manifest intention of obstructing the secondary use of

electronic health data, it shall not have the right to provide access to health data in accordance with Article 49.

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

7. Any penalties and measures imposed pursuant to paragraph 4 shall be made available to other health data access bodies.

8. The Commission may, by means of implementing act, set out the architecture of an IT tool aimed to support and make transparent to other health data access bodies the activities referred to in this Article, especially penalties and exclusions. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

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

10. The Commission may issues guidelines on penalties to be applied by the health data access bodies.

SECTION 3

DATA PERMIT FOR THE SECONDARY USE OF ELECTRONIC HEALTH DATA

Article 44

Data minimisation and purpose limitation

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

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

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

Article 45

Data access applications

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

2. The data access application shall include:

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

(b) a description of the requested electronic health data, their format and data sources, where possible, including geographical coverage where data is requested from several Member States;

(c) an indication whether electronic health data should be made available in an anonymised format;

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

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

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

(g) an estimation of the period during which the electronic health data is needed for processing;

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

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

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

(a) a description of how the processing would comply with Article 6(1) of Regulation (EU) 2016/679;

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

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

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

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

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

Article 46

Data permit

1. Health data access bodies shall assess if the application fulfils one of the purposes listed in Article 34(1) of this Regulation, if the requested data is necessary for the purpose listed in the application and if the requirements in this Chapter are fulfilled by the applicant. If that is the case, the health data access body shall issue a data permit.

2. Health data access bodies shall refuse all applications including one or more purposes listed in Article 35 or where requirements in this Chapter are not met.

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

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

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

6. The data permit shall set out the general conditions applicable to the data user, in particular:

   (a) types and format of electronic health data accessed, covered by the data permit, including their sources;

   (b) purpose for which data are made available;

   (c) duration of the data permit;

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

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

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

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

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

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

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

11. Data users shall make public the results or output of the secondary use of electronic health data, including information relevant for the provision of healthcare, no later than 18 months after the completion of the electronic health data processing or after having received the answer to the data request referred to in Article 47. Those results or output shall only contain anonymised data. The data user shall inform the health data access bodies from which a data permit was obtained and support them to make the information public on health data access bodies' websites. Whenever the data users have used electronic health data in accordance with this Chapter, they shall acknowledge the electronic health data sources and the fact that electronic health data has been obtained in the context of the EHDS.

12. Data users shall inform the health data access body of any clinically significant findings that may influence the health status of the natural persons whose data are included in the dataset.

13. The Commission may, by means of implementing act, develop a logo for acknowledging the contribution of the EHDS. That implementing act shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

14. The liability of health data access bodies as joint controller is limited to the scope of the issued data permit until the completion of the processing activity.

Article 47

Data request

1. Any natural or legal person may submit a data request for the purposes referred to in Article 34. A health data access body shall only provide an answer to a data request in an anonymised statistical format and the data user shall have no access to the electronic health data used to provide this answer.

2. A data request shall include the elements mentioned in paragraphs 2 (a) and (b) of Article 45 and if needed may also include:

(a) a description of the result expected from the health data access body;

(b) a description of the statistic's content.

3. Where an applicant has requested a result in an anonymised form, including statistical format, based on a data request, the health data access body shall assess, within 2 months and, where possible, provide the result to the data user within 2 months.

Article 48

Making data available for public sector bodies and Union institutions, bodies, offices and agencies without a data permit

By derogation from Article 46 of this Regulation, a data permit shall not be required to access the electronic health data under this Article. When carrying out those tasks under Article 37 (1), points (b) and (c), the health data access body shall inform public sector bodies and the Union institutions, offices, agencies and bodies, about the availability of data within 2 months of the data access application, in accordance with Article 9 of Regulation […] [Data Governance Act COM/2020/767 final]. By way of derogation from that Regulation […] [Data Governance Act COM/2020/767 final], the health data access body may extend the period by 2 additional months where necessary, taking into account the complexity of the request. The health data access body shall make available the electronic health data to the data user within 2 months after receiving them from the data holders, unless it specifies that it will provide the data within a longer specified timeframe.

Article 49

Access to electronic health data from a single data holder

1. Where an applicant requests access to electronic health data only from a single data holder in a single Member State, by way of derogation from Article 45(1), that applicant may file a data access application or a data request directly to the data holder. The data access application shall comply with the requirements set out in Article 45 and the data request shall comply with requirements in Article 47. Multi-country requests and requests requiring a combination of datasets from several data holders shall be adressed to health data access bodies.

2. In such case, the data holder may issue a data permit in accordance with Article 46 or provide an answer to a data request in accordance with Article 47. The data holder shall then provide access to the electronic health data in a secure processing environment in compliance with Article 50 and may charge fees in accordance with Article 42.

3. By way of derogation from Article 51, the single data provider and the data user shall be deemed joint controllers.

4. Within 3 months the data holder shall inform the relevant health data access body by electronic means of all data access applications filed and all the data permits issued and the data requests fulfilled under this Article in order to enable the health data access body to fulfil its obligations under Article 37(1) and Article 39.

Article 50

Secure processing environment

1. The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures:

   (a) restrict access to the secure processing environment to authorised persons listed in the respective data permit;

   (b) minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;

   (c) limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;

   (d) ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

   (e) keep identifiable logs of access to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;

   (f) ensure compliance and monitor the security measures referred to in this Article to mitigate potential security threats.

2. The health data access bodies shall ensure that electronic health data can be uploaded by data holders and can be accessed by the data user in a secure processing environment. The data users shall only be able to download non-personal electronic health data from the secure processing environment.

3. The health data access bodies shall ensure regular audits of the secure processing environments.

4. The Commission shall, by means of implementing acts, provide for the technical, information security and interoperability requirements for the secure processing environments. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

Article 51

Joint controllers

1. The health data access bodies and the data users, including Union institutions, bodies, offices and agencies, shall be deemed joint controllers of electronic health data processed in accordance with data permit.

2. The Commission shall, by means of implementing acts, establish a template for the joint controllers' arrangement. Those implementing acts shall be adopted in accordance with the advisory procedure set out in Article 68(2).

SECTION 4

CROSS-BORDER ACCESS TO ELECTRONIC HEALTH DATA FOR SECONDARY USE

Article 52

Cross-border infrastructure for secondary use of electronic health data (HealthData@EU)

1. Each Member State shall designate a national contact point for secondary use of electronic health data, responsible for making electronic health data available for secondary use in a cross-border context and shall communicate their names and contact details to the Commission. The national contact point may be the coordinator health data access body pursuant to Article 36. The Commission and the Member States shall make this information publicly available.

2. The national contact points referred to in paragraph 1 shall be authorised participants in the cross-border infrastructure for secondary use of electronic health data (HealthData@EU). The national contact points shall facilitate the cross-border access to electronic health data for secondary use for different authorised participants in the infrastructure and shall cooperate closely with each other and with the Commission.

3. Union institutions, bodies, offices and agencies involved in research, health policy or analysis, shall be authorised participants of HealthData@EU.

4. Health-related research infrastructures or similar structures whose functioning is based on Union law and which support the use of electronic health data for research, policy making, statistical, patient safety or regulatory purposes shall be authorised participants of HealthData@EU.

5. Third countries or international organisations may become authorised participants where they comply with the rules of Chapter IV of this Regulation and provide access to data users located in the Union, on equivalent terms and conditions, to the electronic health data available to their health data access bodies. The Commission may adopt implementing acts establishing that a national contact point of a third country or a system established at an international level is compliant with requirements of HealthData@EU for the purposes of secondary use of health data, is compliant with the Chapter IV of this Regulation and provides access to data users located in the Union to the electronic health data it has access to on equivalent terms and conditions. The compliance with these legal, organisational, technical and security requirements, including with the standards for secure processing environments pursuant to Article 50 shall be checked under the control of the Commission. These implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68 (2). The Commission shall make the list of implementing acts adopted pursuant to this paragraph publicly available.

6. Each authorised participant shall acquire the required technical capability to connect to and participate in HealthData@EU. Each participant shall comply with the requirements and technical specifications needed to operate the cross-border infrastructure and to allow the authorised participants to connect to each other within it.

7. The Commission is empowered to adopt delegated acts in accordance with Article 67 in order to amend this Article to add or remove categories of authorised participants

in HealthData@EU, taking into account the opinion of the joint controllership group pursuant to Article 66 of this Regulation.

8. The Member States and the Commission shall set up HealthData@EU to support and facilitate the cross-border access to electronic health data for secondary use, connecting the national contact points for secondary use of electronic health data of all Member States and authorised participants in that infrastructure.

9. The Commission shall develop, deploy and operate a core platform for HealthData@EU by providing information technology services needed to facilitate the connection between health data access bodies as part of the cross-border infrastructure for the secondary use of electronic health data. The Commission shall only process electronic health data on behalf of the joint controllers as a processor.

10. Where requested by two or more health data access bodies, the Commission may provide a secure processing environment for data from more than one Member State compliant with the requirements of Article 50. Where two or more health data access bodies put electronic health data in the secure processing environment managed by the Commission, they shall be joint controllers and the Commission shall be processor.

11. The authorised participants shall act as joint controllers of the processing operations in which they are involved carried out in HealthData@EU and the Commission shall act as a processor.

12. Member States and the Commission shall seek to ensure interoperability of HealthData@EU with other relevant common European data spaces as referred to in Regulations […] [Data Governance Act COM/2020/767 final] and […] [Data Act COM/2022/68 final].

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

(a) requirements, technical specifications, the IT architecture of HealthData@EU, conditions and compliance checks for authorised participants to join and remain connected to HealthData@EU and conditions for temporary or definitive exclusion from HealthData@EU;

(b) the minimum criteria that need to be met by the authorised participants in the infrastructure;

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

(d) the responsibilities of the joint controllers and processor(s) for the secure environment managed by the Commission;

(e) common specifications for the interoperability and architecture concerning HealthData@EU with other common European data spaces.

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

14. The approval for individual authorised participant to join HealthData@EU or to disconnect a participant from the infrastructure shall be issued by the Joint Controllership group, based on the results of the compliance checks.

Article 53

Access to cross-border sources of electronic health data for secondary use

1. In the case of cross-border registries and databases, the health data access body in which the data holder is registered shall be competent to decide on data access applications to provide access to electronic health data. Where the registry has joint controllers, the health data access body that shall provide access to electronic health data shall be the body in the Member State where one of the joint controllers is established.

2. Where registries or databases from a number of Member States organise themselves into a single network of registries or databases at Union level, the associated registries may designate one of their members as a coordinator to ensure the provision of data from the registries' network for secondary use. The health data access body of the Member State in which the coordinator of the network is located shall be competent to decide on the data access applications to provide access to electronic health data for the network of registries or databases.

3. The Commission may, by means of implementing acts, adopt the necessary rules for facilitating the handling of data access applications for HealthData@EU, including a common application form, a common data permit template, standard forms for common electronic health data access contractual arrangements, and common procedures for handling cross-border requests, pursuant to Articles 45, 46, 47 and 48. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

Article 54

Mutual recognition

1. When handling an access application for cross-border access to electronic health data for secondary use, health data access bodies and relevant authorised participants shall remain responsible for taking decisions to grant or refuse access to electronic health data within their remit in accordance with the requirements for access laid down in this Chapter.

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

SECTION 5

HEALTH DATA QUALITY AND UTILITY FOR SECONDARY USE

Article 55

Dataset description

1. The health data access bodies shall inform the data users about the available datasets and their characteristics through a metadata catalogue. Each dataset shall include information concerning the source, the scope, the main characteristics, nature of electronic health data and conditions for making electronic health data available.

2. The Commission shall, by means of implementing acts, set out the minimum information elements data holders are to provide for datasets and their

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

Article 56

Data quality and utility label

1. Datasets made available through health data access bodies may have a Union data quality and utility label provided by the data holders.

2. Datasets with electronic health data collected and processed with the support of Union or national public funding shall have a data quality and utility label, in accordance with the principles set out in paragraph 3.

3. The data quality and utility label shall comply with the following elements:

   (a) for data documentation: meta-data, support documentation, data model, data dictionary, standards used, provenance;

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

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

   (d) coverage: representation of multi-disciplinary electronic health data, representativity of population sampled, average timeframe in which a natural person appears in a dataset;

   (e) information on access and provision: time between the collection of the electronic health data and their addition to the dataset, time to provide electronic health data following electronic health data access application approval;

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

4. The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the list of principles for data quality and utility label. Such delegated acts may also amend the list set out under paragraph 3 by adding, modifying or removing requirements for data quality and utility label.

5. The Commission shall, by means of implementing acts, set out the visual characteristics and technical specifications of the data quality and utility label, based on the elements referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2). Those implementing acts shall take into account the requirements in Article 10 of Regulation […] [AI Act COM/2021/206 final] and any adopted common specifications or harmonised standards supporting those requirements.

Article 57

EU Datasets Catalogue

1. The Commission shall establish an EU Datasets Catalogue connecting the national catalogues of datasets established by the health data access bodies and other authorised participants in HealthData@EU.

2. The EU Datasets Catalogue and the national datasets catalogues shall be made publicly available.

Article 58

Minimum dataset specifications

The Commission may, by means of implementing acts, determine the minimum specifications for cross-border datasets for secondary use of electronic health data, taking into account existing Union infrastructures, standards, guidelines and recommendations. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).

Chapter V

Additional actions

Article 59

Capacity building

The Commission shall support sharing of best practices and expertise, aimed to build the capacity of Member States to strengthen digital health systems for primary and secondary use of electronic health data. To support capacity building, the Commission shall draw up benchmarking guidelines for the primary and secondary use of electronic health data.

Article 60

Additional requirements for public procurement and Union funding

1. Public procurers, national competent authorities, including digital health authorities and health data access bodies, and the Commission shall make reference to the applicable technical specifications, standards and profiles as referred to in Articles 6, 23, 50, 56, as relevant, as points of orientation for public procurements and when formulating their tender documents or calls for proposals, as well as when defining the conditions for Union funding regarding this Regulation, including enabling conditions for the structural and cohesion funds.

2. The ex-ante conditionality for Union funding shall take into account the requirements developed in the framework of Chapters II, III and IV.

Article 61

Third country transfer of non-personal electronic data

1. Non-personal electronic data made available by health data access bodies, that are based on a natural person's electronic data falling within one of the categories of Article 33 [(a), (e), (f), (i), (j), (k), (m)] shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final], provided that their transfer to third countries presents a risk of re-identification through means going beyond those likely reasonably to be used, in view of the limited number of natural persons involved in that data, the fact that they are geographically scattered or the technological developments expected in the near future.

2. The protective measures for the categories of data mentioned in paragraph 1 shall depend on the nature of the data and anonymization techniques and shall be detailed in the Delegated Act under the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final].

Article 62

International access and transfer of non-personal electronic health data

1. The digital health authorities, health data access bodies, the authorised participants in the cross-border infrastructures provided for in Articles 12 and 52 and data users shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal electronic health data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3 of this Article.

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

3. In the absence of an international agreement as referred to in paragraph 2 of this Article, where a digital health authority, a health data access body, data users is the addressee of a decision or judgment of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where:

   (a) the third-country system requires the reasons and proportionality of such a decision or judgment to be set out and requires such a decision or judgment to be specific in character, for instance by establishing a sufficient link to certain suspected persons or infringements;

   (b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and

   (c) the competent third-country court or tribunal issuing the decision or judgment or reviewing the decision of an administrative authority is empowered under the law of that third country to take duly into account the relevant legal interests of the provider of the data protected under Union law or the national law of the relevant Member State

4. If the conditions laid down in paragraph 2 or 3 are met, digital health authority, a health data access body or a data altruism body shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation of the request.

5. The digital health authorities, health data access bodies, data users shall inform the data holder about the existence of a request of a third-country administrative

authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.

Article 63

International access and transfer of personal electronic health data

In the context of international access and transfer of personal electronic health data, Member States may maintain or introduce further conditions, including limitations, in accordance with and under the conditions of article 9(4) of the Regulation (EU) 2016/679.

Chapter VI

European governance and coordination

Article 64

European Health Data Space Board (EHDS Board)

1. A European Health Data Space Board (EHDS Board) is hereby established to facilitate cooperation and the exchange of information among Member States. The EHDS Board shall be composed of the high level representatives of digital health authorities and health data access bodies of all the Member States. Other national authorities, including market surveillance authorities referred to in Article 28, European Data Protection Board and European Data Protection Supervisor may be invited to the meetings, where the issues discussed are of relevance for them. The Board may also invite experts and observers to attend its meetings, and may cooperate with other external experts as appropriate. Other Union institutions, bodies, offices and agencies, research infrastructures and other similar structures shall have an observer role.
2. Depending on the functions related to the use of electronic health data, the EHDS Board may work in subgroups, where digital health authorities or health data access bodies for a certain area shall be represented. The subgroups may have joint meetings, as required.
3. The composition, organisation, functioning and cooperation of the sub-groups shall be set out in the rules of procedure put forward by the Commission.
4. Stakeholders and relevant third parties, including patients' representatives, shall be invited to attend meetings of the EHDS Board and to participate in its work, depending on the topics discussed and their degree of sensitivity.
5. The EHDS Board shall cooperate with other relevant bodies, entities and experts, such as the European Data Innovation Board referred to in Article 26 of Regulation […] [Data Governance Act COM/2020/767 final], competent bodies set up under Article 7 of Regulation […] [Data Act COM/2022/68 final], supervisory bodies set up under Article 17 of Regulation […] [eID Regulation], European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679 and cybersecurity bodies.
6. The Commission shall chair the meetings of the EHDS Board.
7. The EHDS Board shall be assisted by a secretariat provided by the Commission.

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

Article 65

Tasks of the EHDS Board

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

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

   (b) to issue written contributions and to exchange best practices on matters related to the coordination of the implementation at Member State level of this Regulation and of the delegated and implementing acts adopted pursuant to it, in particular as regards:

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

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

      (iii) other aspects of the primary use of electronic health data.

   (c) to facilitate cooperation between digital health authorities through capacity-building, establishing the structure for annual activity reporting, peer-review of annual activity reports and exchange of information;

   (d) to share information concerning risks posed by EHR systems and serious incidents as well as their handling;

   (e) to facilitate the exchange of views on the primary use of electronic health data with the relevant stakeholders, including representatives of patients, health professionals, researchers, regulators and policy makers in the health sector.

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

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

   (b) to issue written contributions and to exchange best practices on matters related to the coordination of the implementation at Member State level of this Regulation and of the delegated and implementing acts adopted pursuant to it, in particular as regards:

      (xi) implementation of rules for access to electronic health data;

      (xii) technical specifications or existing standards regarding the requirements set out in Chapter IV;

      (xiii) incentives policy for promoting data quality and interoperability improvement;

      (xiv) policies concerning fees to be charged by the health data access bodies and data holders;

(xv) the establishment and application of penalties;

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

(c) to facilitate cooperation between health data access bodies through capacity-building, establishing the structure for annual activity reporting, peer-review of annual activity reports and exchange of information;

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

(e) to contribute to the work of the European Data Innovation Board to be established in accordance with Article 29 of the Regulation […] [Data Governance Act COM/2020/767 final];

(f) to facilitate the exchange of views on the secondary use of electronic health data with the relevant stakeholders, including representatives of patients, health professionals, researchers, regulators and policy makers in the health sector.

Article 66

Joint controllership groups for Union infrastructures

1. The Commission shall establish two groups dealing with joint controllership for the cross-border infrastructures provided for in Articles 12 and 52. The groups shall be composed of the representatives of the national contact points and other authorised participants in those infrastructures.

2. The composition, organisation, functioning and cooperation of the sub-groups shall be set out in the rules of procedure adopted by those groups.

3. Stakeholders and relevant third parties, including patients' representatives, may be invited to attend meetings of the groups and to participate in their work.

4. The groups shall elect chairs for their meetings.

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

6. The groups shall take decisions concerning the development and operation of the cross-border infrastructures pursuant to Chapters II and IV, on changes of infrastructure, adding additional infrastructures or services, or ensuring interoperability with other infrastructures, digital systems or data spaces. The group shall also take decisions to accept individual authorised participants to join the infrastructures or to disconnect them.

CHAPTER VII

Delegation and Committee

Article 67

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 5(2), 10(3), 25(3), 32(4), 33(7), 37(4), 39(3), 41(7), 45(7), 46(8), 52(7), 56(4) shall be conferred on the

Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The power to adopt delegated acts referred to in Articles 5(2), 10(3), 25(3), 32(4), 33(7), 37(4), 39(3), 41(7), 45(7), 46(8), 52(7), 56(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 5(2), 10(3), 25(3), 32(4), 33(7), 37(4), 39(3), 41(7), 45(7), 46(8), 52(7), 56(4) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of 3 months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 3 months at the initiative of the European Parliament or of the Council.

Article 68

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

Chapter VIII

Miscellaneous

Article 69

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by date of application of this Regulation and shall notify the Commission without delay of any subsequent amendment affecting them.

Article 70

Evaluation and review

1. After 5 years from the entry into force of this Regulation, the Commission shall carry out a targeted evaluation of this Regulation especially with regards to Chapter III, and submit a report on its main findings to the European Parliament and to the Council, the European Economic and Social Committee and the Committee of the Regions, accompanied, where appropriate, by a proposal for its amendment. The evaluation shall include an assessment of the self-certification of EHR systems and reflect on the need to introduce a conformity assessment procedure performed by notified bodies.

2. After 7 years from the entry into force of this Regulation, the Commission shall carry out an overall evaluation of this Regulation, and submit a report on its main findings to the European Parliament and to the Council, the European Economic and Social Committee and the Committee of the Regions, accompanied, where appropriate, by a proposal for its amendment.

3. Member States shall provide the Commission with the information necessary for the preparation of that report.

Article 71

Amendment to Directive 2011/24/EU

Article 14 of Directive 2011/24/EU is deleted.

Chapter IX

Deferred application and final provisions

Article 72

Entry into force and application

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

It shall apply from 12 months after its entry into force.

However, Articles 3, 4, 5, 6, 7, 12, 14, 23 and 31 shall apply as follows:

(a) from 1 year after date of entry into application to categories of personal electronic health data referred to in Article 5(1), points (a), (b) and (c), and to EHR systems intended by the manufacturer to process such categories of data.;

(b) from 3 years after date of entry into application to categories of personal electronic health data referred to in Article 5(1), points (d), (e) and (f), and to EHR systems intended by the manufacturer to process such categories of data;

(c) from the date established in delegated acts pursuant to Article 5(2) for other categories of personal electronic health data.

Chapter III shall apply to EHR systems put into service in the Union pursuant to Article 15(2) from 3 years after date of entry into application.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5. Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

3.2.2. Estimated output funded with operational appropriations

3.2.3. Summary of estimated impact on administrative appropriations

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Regulation of the European Parliament and of the Council on the European Health Data Space

1.2. Policy area(s) concerned

Heading 1: Single Market, innovation and digital

Heading 2: Cohesion, Resilience and Values

1.3. The proposal/initiative relates to:

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[1]

☐ **the extension of an existing action**

✔ **a merger or redirection of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

The general objective of the intervention is to establish the rules governing the European Health Data Space to ensure natural persons' access and control over their own health data, to improve the functioning of the single market for the development and use of innovative health products and services based on health data, and to ensure that researchers, innovators, policy-makers and regulators can make the most of the available health data for their work, while preserving trust and security.

1.4.2. Specific objective(s)

Specific objective No 1

To empower natural persons through increased digital access to and control of their health data and support their free movement;

Specific objective No 2

To set requirements specific to electronic health record (EHR) systems and obligations in order to ensure that EHR systems placed on the market and used are interoperable, secure and respect the rights of natural persons regarding their health data;

Specific objective No 3

To ensure a consistent and efficient framework for the secondary use of natural persons' health data for research, innovation, policy-making, official statistics, patient safety or regulatory activities.

[1] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

Specific objective No 1

Natural persons should benefit from easier access to and control over their own health data, including across borders.

Specific objective No 2

Suppliers and manufacturers of EHR systems should benefit from a minimal but clear set of requirements on interoperability and security for such systems, reducing barriers to supply such systems across the single market.

Specific objective No 3

Natural persons should benefit from a wealth of innovative health products and services that are provided and developed based on health data primary and secondary use, while preserving trust and security.

Health data users, namely researchers, innovators, policy-makers and regulators, should benefit from a more efficient secondary use of health data.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Specific objective No 1

a) Number of healthcare providers of different types connected to MyHealth@EU calculated a) in absolute terms, b) as share of all healthcare providers and c) as share of natural persons that can use the services provided in MyHealth@EU;

b) volume of personal electronic health data of different categories shared across borders through MyHealth@EU;

c) percentage of natural persons having access to their electronic health records;

d) level of natural persons satisfaction with MyHealth@EU services;

These will be collected by annual reporting from digital health authorities.

Specific objective No 2

e) Number of certified EHR systems and labelled wellness applications enrolled in the EU database;

f) Number of non-compliance cases with the mandatory requirements;

These will be collected by annual reporting from digital health authorities.

Specific objective No 3

g) Number of datasets published in the European data catalogue;

h) Number of data access requests, disaggregated in national and multi-country requests, processed, accepted or rejected by health data access bodies.

These will be collected by annual reporting from health data access bodies.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The Regulation will be fully applicable four years after its entry into force, once the deferred application has expired. Provisions regarding the rights of natural persons (Chapter II), certification of EHR systems (Chapter III), secondary use of health data (Chapter IV) and governance (Chapter V) should be in place before then. In particular, Member States shall have appointed existing authorities and/or established new authorities performing the tasks set out in the legislation earlier, so that the European Health Data Space Board (EHDS Board) is set up and able to assist them earlier. The infrastructure for primary and secondary uses of health data should also be operational earlier to enable the onboarding of all Member States before this Regulation becomes fully applicable.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at European level (ex-ante)

As the evaluation of Article 14 of the Directive 2011/24/EU on cross-border healthcare shows, the approaches taken so far, consisting of low intensity/soft instruments, such as guidelines and recommendations aimed to support interoperability, have not produced the desired results. National approaches in addressing the problems have only limited scope and do not fully address the EU-wide issue: the cross-border exchange of health data is currently still very limited, which is partly explained by the significant diversity in standards applied to health data in different Member States. In many Member States, there are substantial national, regional and local challenges to interoperability and data portability, hampering continuity of care and efficient healthcare systems. Even if health data is available in electronic format, it does not commonly follow the natural person when they use services of a different healthcare provider.

Expected generated Union added value (ex-post)

Action at European level through this Regulation will increase the effectiveness of measures taken to address these challenges. Setting out common rights for natural persons when accessing and controlling the use of their health data and setting common rules and obligations for interoperability and security of EHR systems will reduce the costs for the flow of health data across the EU. A common legal basis for secondary use of health data will also yield efficiency gains for data users in the area of health. The establishment of a common governance framework covering primary and secondary uses of health data will facilitate coordination.

1.5.3. Lessons learned from similar experiences in the past

The evaluation of the Cross Border Healthcare Directive's provisions related to digital health concluded that, given the voluntary nature of the eHealth Network actions, effectiveness and efficiency in increasing cross-border health data exchanges have been rather limited. Progress is slow in the implementation of MyHealth@EU. While the eHealth Network recommended Member States to use the standards,

profiles and specifications from Electronic Health Record Exchange Format in procurements, in order to build interoperable systems, their uptake has been limited, resulting in fragmented landscape and uneven access to and portability of health data. For this reason, there is a need laying down specific rules, rights and obligations regarding the access and control of natural persons over their own health data and regarding the cross-border exchange of such data for primary and secondary uses, with a governance structure ensuring coordination of specific responsible bodies at Union level.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The European Health Data Space has strong ties with several other actions of the Union in the areas of health and social care, digitisation, research, innovation and fundamental rights.

This Regulation defines the rules, rights and obligations for the functioning of the European Health Data Space, as well as the rollout of the necessary infrastructures, certification/labelling schemes and governance frameworks. These measures are complementary to the horizontal provisions in the Data Governance Act, Data Act and the General Data Protection Regulation.

The fulfilment of the obligations by the Commission and associated support actions under this legal proposal will require EUR 220 million between 2023 and 2027. The majority of the costs of this Regulation (EUR 170 million) are foreseen to be funded from the EU4Health programme as per Article 4, point (f) of the EU4Health Regulation[2]. The foreseen actions contribute also to achieving the specific objectives in Article 4, paragraphs a), b) and h). Digital Europe Programme will support patients' access to their health data through MyHealth@EU with additional EUR 50 million. In both cases, the expenditure linked to this proposal will be covered within the programmed amounts of these programmes.

In its 2021 and 2022 work programmes, EU4Health already supports the development and establishment of the European Health Data Space with a substantial initial contribution of almost EUR 110 million. This includes the functioning of the existing infrastructure for primary uses of health data (MyHealth@EU), the uptake of international standards by Member States, actions on capacity building and other preparatory actions, as well as an infrastructure pilot project for the secondary use of health data, a pilot project for the access of patients to their health data through MyHealth@EU and its scale-up, and the development of the central services for secondary uses of health data.

In addition to the EUR 330 million under EU4Health and Digital Europe Programme just described, other actions under Digital Europe Programme, Connecting Europe Facility and Horizon Europe will complement and facilitate the implementation of the European Health Data Space. Moreover, the Commission can support – upon demand – Member States in achieving the objectives of this proposal through the provision of direct technical support from the Technical Support Instrument. These programmes, among others, aim at *building up and strengthening quality data*

[2] Regulation (EU) 2021/522 of the European Parliament and of the Council of 24 March 2021 establishing a Programme for the Union's action in the field of health ('EU4Health Programme') for the period 2021-2027, and repealing Regulation (EU) No 282/2014

resources and corresponding exchange mechanisms[3] and *developing, promoting and advance scientific excellence*[4], respectively, including in health. Instances of such complementarity include horizontal support for the development and large-scale piloting of a smart middleware platform for common data spaces, where EUR 105 million from Digital Europe Programme have already been allocated in 2021-2022; domain-specific investments to facilitate the secure, cross-border access to cancer images and genomics, supported by Digital Europe Programme in 2021-2022 with EUR 38 million; and research and innovation projects and coordination and support actions on health data quality and interoperability are already supported by Horizon Europe (Cluster 1) with EUR 108 million in 2021 and 2022, as well as EUR 59 million from the Research Infrastructures programme. Horizon Europe has also provided in 2021 and 2022 additional support for secondary use of health data dedicated to COVID-19 (EUR 42 million) and cancer (EUR 3 million).

Additionally, where physical connectivity is lacking in the health sector, Connecting Europe Facility will *contribute to the development of projects of common interest relating to the deployment of and access to safe and secure very high capacity networks, including 5G systems, and to the increased resilience and capacity of digital backbone networks on Union territories*[5]. EUR 130 million are programmed in 2022 and 2023 for the interconnection of cloud infrastructures, including in health.

Beyond this, the costs for the connection of Member States to the European infrastructures within the European Health Data Space will be partially covered by EU funding programmes that will complement EU4Health. Instruments such as Recovery and Resilience Facility (RRF) and the European Regional Development Fund (ERDF) will be able to support the connection of Member States to the European infrastructures.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The fulfilment of the obligations by the Commission and associated support actions under this legal proposal will be directly funded from the EU4Health programme and supported further from the Digital Europe Programme.

Redeployed actions under Digital Europe Programme and Horizon Europe regarding health and digital health will also be able to complement the implementation actions supporting this Regulation under EU4Health.

[3] Article 5 of Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240

[4] Article 3, paragraph 2(a), of Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013.

[5] Article 3, paragraph 2(c), of Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014.

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

✔ **unlimited duration**

– Implementation with a start-up period from January 2023,

– followed by full-scale operation.

1.7. Management mode(s) planned[6]

✔ **Direct management** by the Commission

– ✔ by its departments, including by its staff in the Union delegations;

– ✔ by the executive agencies

☐ **Shared management** with the Member States

☐

Indirect management by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

[6] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Regulation will be reviewed and evaluated seven years from the entry into force of the regulation. A targeted evaluation of the self-certification of EHR systems and reflect on the need to introduce a conformity assessment procedure performed by notified bodies shall be carried out five years from the entry into force of the regulation. The Commission will report on the findings of the evaluation to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.

The proposal includes the expansion and rollout of the cross-border digital infrastructures for primary and secondary uses of health data, which will facilitate monitoring of several indicators.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

The Regulation establishes a new policy with regard to the protection of electronic health data, harmonised rules for electronic health record (EHR) systems and rules and governance for the reuse of health data. These new rules require a common coordination mechanism for the cross-border application of the obligations under this Regulation in the form of a new advisory group coordinating the activities of national authorities.

The actions foreseen under this Regulation will be implemented through direct management, using the implementation modes offered by the Financial Regulation, mainly being grants and procurement. Direct management allows to establish grant agreements and contracts with beneficiaries and contractors directly engaged in activities that serve Union policies. The Commission will ensure direct monitoring over the outcome of the actions financed. The payment modalities of the actions funded will be adapted to the risks pertaining to the financial transactions.

In order to ensure the effectiveness, efficiency and economy of the Commission controls, the control strategy will be oriented towards a balance of ex-ante and ex-post checks and focus on three key stages of grant/contract implementation, in accordance with the Financial Regulation:

a) Selection of proposals/tenders that fit the policy objectives of the Regulation.

b) Operational, monitoring and ex-ante controls that cover project implementation, public procurement, pre-financing, interim and final payments, management of guarantees.

Ex-post controls at the beneficiaries/contractors' sites will also be carried out on a sample of transactions. The selection of these transactions will combine a risk assessment and a random selection.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The implementation of this Regulation focuses on the attribution of public procurement contracts and grants for specific activities and organisations.

The public procurement contracts will mainly be concluded in for the provision of European platforms for digital infrastructures and associated services, and technical assitance for the governance framework.

Grants will mainly be awarded for support the connection of Member States to the European infrastructure, to support interoperability projects and carrying out joint actions. The period of execution of the subsidised projects and activities varies from one to three years mostly.

The main risks are the following:

a) Risk of not fully achievening the objectives of the Regulation due to insufficient uptake or quality/delays in the implementation of the selected projects or contracts.

b) Risk of inefficient or non-economic use of funds awarded, both for grants (complexity of funding rules) and for procurement (limited number of economic providers with the required specialist knowledge entailing insufficient possibilities to compare price offers in some sectors).

c) Reputational risk for the Commission, if fraud or criminal activities are discovered; only partial assurance can be drawn from the third parties' internal control systems due to the rather large number of heterogeneous contractors and beneficiaries, each operating their own control system.

The Commission put in place internal procedures that aim at covering the risks identified above. The internal procedures are in full compliance with the Financial Regulation and include anti-fraud measures and cost-benefit considerations. Within this framework, the Commission continues to explore possibilities to enhance the management and to realise efficiency gains. Main features of the control framework are the following:

1) Controls before and during the implementation of the projects:

a) An appropriate project management system will be put in place focusing on the contributions of projects and contracts to the policy objectives, ensuring a systematic involvement of all actors, establishing a regular project management reporting complemented by on-site-visits on a case by case basis, including risk reports to senior management, as well as maintaining appropriate budgetary flexibility.

b) Model grant agreements and service contracts used are developed within the Commission. They provide for a number of control provisions such as audit certificates, financial guarantees, on-site audits as well as inspections by OLAF. The rules governing the eligibility of costs are being simplified, for example, by using unit costs, lump sums, contributions not linked to costs and other possibilities offered by the Financial Regulation. This will reduce the cost of controls and put the focus on checks and controls in high risk areas.

c) All staff sign up to the code of good administrative behaviour. Staff who are involved in the selection procedure or in the management of the grant

agreements/contracts (also) sign a declaration of absence of a conflict of interest. Staff is regularly trained and uses networks to exchange best practices.

d) Technical implementation of a project is checked at regular intervals at the desk on the basis of technical progress reports of the contractors and beneficiaries; in addition contractors'/beneficiaries' meetings and on-site-visits are foreseen on a case by case basis.

2) Controls at the end of the project:

Ex-post audits are performed on a sample of transactions to verify on-the-spot the eligibility of cost claims. The aim of these controls is to prevent, detect and correct material errors related to the legality and regularity of financial transactions. With a view to achieving a high control impact, the selection of beneficiaries to be audited foresees to combine a risk based selection with a random sampling, and to pay attention to operational aspects whenever possible during the on-site audit.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

The yearly costs of the suggested level of controls under the third Health programme 2014-2020 represented approximately 4% to 7% of the yearly budget of the operational expenditure. This is justified by the diversity of transactions to be controlled. Indeed, in the area of health, direct management involves the attribution of numerous contracts and grants for actions of very small to very large sizes, and the payment of numerous operating grants to non-governmental organisations. The risk related to these activities concerns the capacity of (especially) smaller organisations to effectively control expenditure.

The Commission considers that the average costs of controls is likely to be the same for the actions proposed under this Regulation.

Under the third Health Programme 2014-2020, on a 5-year basis, the error rate for the on-the-spot audits of grants under direct management was 1.8% while for procurement contracts it was below 1%. This level of error is considered acceptable, as it is under the materiality level of 2%.

The proposed actions will not affect the way the appropriations are currently managed. The existing control system proved to be able to prevent and/or to detect errors and/or irregularities, and in case of errors or irregularities, to correct them. It will be adapted to include the new actions and to ensure that residual error rates (after correction) remain below the threshold of 2%.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

As for its activities in direct management, the Commission shall take appropriate measures ensuring that the financial interests of the European Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportional and deterrent penalties. To this effect, the Commission adopted an anti-fraud strategy, latest update of April 2019 (COM(2019)196), covering notably the following preventive, detective and corrective measures:

The Commission or its representatives and the Court of Auditors shall have the power of audit, on the basis of documents and on-the-spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds. OLAF shall be authorised to carry out on-the-spot checks and inspections on economic operators concerned directly or indirectly by such funding.

The Commission also implements a series of measures such as:

a) decisions, agreements and contracts resulting from the implementation of the Regulation will expressly entitle the Commission, including OLAF, and the Court of Auditors to conduct audits, on-the-spot checks and inspections and to recover amounts unduly paid and, where appropriate, impose administrative sanctions;

b) during the evaluation phase of a call for proposals/tender, the applicants and tenderers are checked against the published exclusion criteria based on declarations and the Early Detection and Exclusion System (EDES);

c) the rules governing the eligibility of costs will be simplified in accordance with the provisions of the Financial Regulation;

d) regular training on issues related to fraud and irregularities is given to all staff involved in contract management as well as to auditors and controllers who verify the beneficiaries' declarations on the spot.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[1]	from EFTA countries[2]	from candidate countries[3]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
1	02 04 03 - Digital Europe Programme - Artificial Intelligence	Diff.	YES	YES	YES	NO
2b	06 06 01 - EU4Health Programme	Diff.	YES	YES	YES	NO
7	20 02 06 Administrative expenditure	Non-diff.	NO	NO	NO	NO

1 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
2 EFTA: European Free Trade Association.
3 Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ✔ The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

Heading of multiannual financial framework	1	Single Market, innovation and digital

DG CNECT			Year **2022**[1]	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**Subsequent years (yearly)**	**TOTAL 2023-2027**
• Operational appropriations										
02 04 03 - Digital Europe Programme - Artificial Intelligence	Commitments	(1a)			10.000	20.000		20.000		**50.000**
	Payments	(2a)			5.000	15.000	10.000	10.000	10.000[2]	**50.000**
Appropriations of an administrative nature financed from the envelope of specific programmes[3]										
Budget line		(3)								
TOTAL	Commitments	=1a+1b+1c +3			10.000	20.000		20.000		**50.000**

[1] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

[2] This amount stems from the commitment in 2027 and is not a recurrent payment. It is included in the computation for the total for 2023-2027.

[3] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

appropriations for DG CNECT	Payments	=2a+2b+2c +3			5.000	15.000	10.000	10.000	10.000	**50.000**
The contributions from the Digital Europe Programme as of 2023 are indicative, and will be considered in the context of the preparation of the respective Work Programmes. Ultimate allocations will be subject to the prioritisation for funding in the context of the underpinning adoption procedure and agreement of the respective Programme Committee.										

• TOTAL operational appropriations	Commitments	(4)			10.000	20.000		20.000		**50.000**
	Payments	(5)			5.000	15.000	10.000	10.000	10.000	**50.000**
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADING 1 of the multiannual financial framework	Commitments	=4+ 6			10.000	20.000		20.000		**50.000**
	Payments	=5+ 6			5.000	15.000	10.000	10.000	10.000	**50.000**

Heading of multiannual financial framework	2b	Cohesion, resilience and values

DG SANTE			Year **2022** [4]	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**Subsequent years (yearly)**	**TOTAL 2023-2027**
• Operational appropriations										
06 06 01 - EU4Health Programme	Commitments	(1a)		26.000	25.000	34.000	35.000	50.000	15.000	**170.000**
	Payments	(2a)		13.000	25.500	29.500	34.500	67.500	15.000	**170.000**
Appropriations of an administrative nature financed from the envelope of specific programmes[5]										
Budget line		(3)								
TOTAL appropriations for DG SANTE	Commitments	=1a+1b+1c +3		26.000	25.000	34.000	35.000	50.000	15.000	**170.000**
	Payments	=2a+2b+2c +3		13.000	25.500	29.500	34.500	67.500	15.000	**170.000**

• TOTAL operational appropriations	Commitments	(4)		26.000	25.000	34.000	35.000	50.000	15.000	**170.000**
	Payments	(5)		13.000	25.500	29.500	34.500	67.500	15.000	**170.000**

[4] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

[5] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)								
TOTAL appropriations under HEADING 2b of the multiannual financial framework	Commitments	=4+ 6		26.000	25.000	34.000	35.000	50.000	15.000	**170.000**
	Payments	=5+ 6		13.000	25.500	29.500	34.500	67.500	15.000	**170.000**

Heading of multiannual financial framework	7	Administrative expenditure

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**Subsequent years (yearly)**	**TOTAL 2023-2027**
DG SANTE									
• Human resources			3.289	3.289	3.289	3.289	3.289	3.289	**16.445**
• Other administrative expenditure			0.150	0.150	0.250	0.250	0.250	0.250	**1.050**
TOTAL DG SANTE	Appropriations		3.439	3.439	3.539	3.539	3.539	3.539	**17.495**

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)		3.439	3.439	3.539	3.539	3.539	3.539	**17.495**

EUR million (to three decimal places)

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**Subsequent years (yearly)**	**TOTAL 2023-2027**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments		29.439	38.439	57.539	38.539	73.539	18.539	**237.495**
	Payments		16.439	33.939	48.039	48.039	91.039	18.539	**237.495**

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**Subsequent years (yearly)**		**TOTAL 2023-2027**	
	OUTPUTS																	
	Type[1]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	**Total No**	**Total cost**
SPECIFIC OBJECTIVE 1																		
Development and maintenance of the European core platform for MyHealth@EU and support for Member States						16.400		18.000		28.000		10.000		38.000		8.000		**110.400**
Subtotal for specific objective 1						**16.400**		**18.000**		**28.000**		**10.000**		**38.000**		**8.000**		**110.400**
SPECIFIC OBJECTIVE 2																		
Database for EHR systems and wellness applications						3.100		3.000		3.000		3.000		2.000		2.000		**14.100**
Subtotal for specific objective No 2						**3.100**		**3.000**		**3.000**		**3.000**		**2.000**		**2.000**		**14.100**
SPECIFIC OBJECTIVE 3																		
Development and maintenance of the European core platform for HealthData@EU and						6.500		14.000		23.000		22.000		30.000		5.000		**95.500**

[1] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

support for Member States																
Subtotal for specific objective 3				**6.500**		**14.000**		**23.000**		**22.000**		**30.000**		**5.000**		**95.500**
TOTALS				**26.000**		**35.000**		**54.000**		**35.000**		**70.000**		**15.000**		**220.000**

3.2.3. Summary of estimated impact on administrative appropriations

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ✔ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027 and subsequent years**	**TOTAL**
HEADING 7 of the multiannual financial framework							
Human resources		3.289	3.289	3.289	3.289	3.289	**16.445**
Other administrative expenditure		0.150	0.150	0.250	0.250	0.250	**1.050**
Subtotal HEADING 7 of the multiannual financial framework		3.439	3.439	3.539	3.539	3.539	**17.495**

	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027 and subsequent years**	**TOTAL**
Outside HEADING 7[1] of the multiannual financial framework							
Human resources							
Other expenditure of an administrative nature							
Subtotal outside HEADING 7 of the multiannual financial framework							

	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027 and subsequent years**	**TOTAL**
TOTAL		**3.439**	**3.439**	**3.539**	**3.539**	**3.539**	**17.495**

[1] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

3.2.3.1. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources.

– ✔ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027 and subsequent years**
• Establishment plan posts (officials and temporary staff)							
20 01 02 01 (Headquarters and Commission's Representation Offices)			16	16	16	16	16
20 01 02 03 (Delegations)							
01 01 01 01 (Indirect research)							
01 01 01 11 (Direct research)							
Other budget lines (specify)							
20 02 01 (AC, END, INT from the 'global envelope')			9	9	9	9	9
20 02 03 (AC, AL, END, INT and JPD in the delegations)							
XX 01 xx **yy zz** [1]	- at Headquarters						
	- in Delegations						
01 01 01 02 (AC, END, INT - Indirect research)							
01 01 01 12 (AC, END, INT - Direct research)							
Other budget lines (specify)							
TOTAL			**25**	**25**	**25**	**25**	**25**

06 is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	12 AD FTE (10 in policy unit and 2 in IT unit of DG SANTE) and 4 AST FTE (3 in the policy Unit and 1 in the IT Unit of DG SANTE) will be required to perform the tasks related to the development and functioning of the EHDS, namely for the: a) management of cross-border digital infrastructure MyHealth@EU; b) management of cross-border digital infrastructure for secondary uses; c) standardisation of electronic health records and health data exchanges; d) data quality of electronic health records and health data exchanges; e) access to health data for secondary uses; f) complaints, infringements, and compliance checks; g) logistic support for governance framework (physical and online meetings); h) horizontal tasks on communication, stakeholder management and inter-institutional relations; i) internal coordination; j) management of activities.

[1] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

	6.5 AD FTE and 4 AST FTE will be covered with staff currently working on digital health and health data exchanges, under Article 14 of Directive 2011/24/EU and in the preparations for the EHDS Regulation. The remaining 5.5 AD FTE will be covered with internal redeployment from DG SANTE.
External staff	For the performance of the tasks enumerated above, AD and AST personnel will be supported by 5 AC and 4 END at DG SANTE. 4 AC FTE and 3 END FTE will be covered with staff currently working on digital health and health data exchanges, under Article 14 of Directive 2011/24/EU and in the preparations for the EHDS Regulation. The remaining 1 AC FTE and 1 END FTE will be covered with internal redeployment from DG SANTE.

3.2.4. Compatibility with the current multiannual financial framework

The proposal/initiative:

– ✔ can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

Appropriations will be redeployed within the financial envelope allocated to the EU4Health programme and to the Digital Europe Programme in the MFF 2021-2027.

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

– ☐ requires a revision of the MFF.

3.2.5. Third-party contributions

The proposal/initiative:

– ✔ does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **N**[1]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[1] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

3.3. Estimated impact on revenue

– ✔ The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

  – ☐ on own resources

  – ☐ on other revenue

  – please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[2]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[2] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

EUROPEAN
COMMISSION

Strasbourg, 3.5.2022
COM(2022) 197 final

ANNEXES 1 to 4

ANNEXES

to the

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the European Health Data Space

{SEC(2022) 196 final} - {SWD(2022) 130 final} - {SWD(2022) 131 final} -
{SWD(2022) 132 final}

ANNEX I

MAIN CHARACTERISTICS OF ELECTRONIC HEALTH DATA CATEGORIES

Electronic health data category	Main characteristics of electronic health data included under the category
1. Patient summary	Electronic health data that includes important clinical facts related to an identified person and that is essential for the provision of safe and efficient healthcare to that person. The following information is part of a patient summary: 1. Personal details 2. Contact information 3. Information on insurance 4. Allergies 5. Medical alerts 6. Vaccination/prophylaxis information, possibly in the form of a vaccination card 7. Current, resolved, closed or inactive problems 8. Textual information related to medical history 9. Medical devices and implants 10. Procedures 11. Functional status 12. Current and relevant past medicines 13. Social history observations related to health 14. Pregnancy history 15. Patient provided data 16. Observation results pertaining to the health condition 17. Plan of care 18. Information on a rare disease such as details about the impact or characteristics of the disease
2. Electronic prescription	Electronic health data constituting a prescription for a medicinal product as defined in Article 3(k) of Directive 2011/24/EU.
3. Electronic dispensation	Information on the supply of a medicinal product to a natural person by a pharmacy based on an electronic prescription.
4. Medical image and image report	Electronic health data related to the use of or produced by technologies that are used to view the human body in order to prevent, diagnose, monitor, or treat medical conditions.
5. Laboratory result	Electronic health data representing results of studies performed notably through in vitro diagnostics such as clinical biochemistry, haematology, transfusion medicine, microbiology, immunology, and others, and including, where relevant, reports supporting the interpretation of the results.
6. Discharge report	Electronic health data related to a healthcare encounter or episode of care and including essential information about admission, treatment and discharge of a natural person.

ANNEX II

ESSENTIAL REQUIREMENTS FOR EHR SYSTEMS AND PRODUCTS CLAIMING INTEROPERABILITY WITH EHR SYSTEMS

The essential requirements laid down in this Annex shall apply *mutatis mutandis* to products claiming interoperability with EHR systems.

1. General requirements

1.1. An electronic health record system (EHR system) shall achieve the performance intended by its manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, it is suitable for its intended purpose and its use does not put at risk patient safety.

1.2. An EHR system shall be designed and developed in such a way that it can be supplied and installed, taking into account the instructions and information provided by the manufacturer, without adversely affecting its characteristics and performance during its intended use.

1.3. An EHR system shall be designed and developed in such a way that its interoperability, safety and security features uphold the rights of natural persons, in line with the intended purpose of the EHR system, as set out in Chapter II of this Regulation.

1.4. 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.

2. Requirements for interoperability

2.1. An EHR system shall allow personal electronic health data to be shared between health professionals or other entities from the health system, and between health professionals and patient or health professional portals in a commonly used electronic interoperable format, which includes, inter-alia, dataset content, data structures, formats, vocabularies, taxonomies, exchange formats, standards, specifications, profiles for exchange and code lists, thus enabling system to system communication.

2.2. An EHR system shall be interoperable and compatible with the European infrastructures set out in this Regulation for the cross-border sharing of electronic health data.

2.3. An EHR system that includes a functionality for entering structured personal electronic health data shall enable the entry of data structured in a structured way that supports the data sharing in a structured, commonly used and machine-readable format, enabling system to system communication.

2.4. An EHR system shall not include features that prohibit, restrict or place undue burden on authorised access, personal electronic health data sharing, or use of personal electronic health data for permitted purposes.

2.5. An EHR system shall not include features that prohibit, restrict or place undue burden on authorised exporting of personal electronic health data for the reasons of replacing the EHR system by another product.

3. Requirements for security

3.1. An EHR system shall be designed and developed in such a way that it ensures safe and secure processing of electronic health data, and that it prevents unauthorised access to such data.

3.2. An EHR system designed to be used by health professionals shall provide reliable mechanisms for the identification and authentication of health professionals, including checks on professional rights and qualifications.

3.3. An EHR system designed to be used by health professionals shall support the use of information on professional rights and qualifications as part of the access control mechanisms, such as role-based access control.

3.4. An EHR system designed to enable access by health professionals or other individuals to personal electronic health data shall provide sufficient logging mechanisms that record, at least the following information on every access event or group of events:

(a) identification of the health professional or other individual having accessed electronic health data;

(b) identification of the individual;

(c) categories of data accessed;

(d) time and date of access;

(e) origin(s) of data.

3.5. An EHR system shall include tools and mechanism to allow natural persons to restrict health professionals' access to their personal electronic health data. It shall also include mechanisms that allow access to personal electronic health data in emergency situations, and ensure that access is strictly logged.

3.6. An EHR system shall include tools or mechanisms to review and analyse the log data, or it shall support the connection and use of external software for the same purposes.

3.7. An EHR system designed to be used by health professionals shall support digital signatures or similar non-repudiation mechanisms.

3.8. An EHR system designed for the storage of electronic health data shall support different retention periods and access rights that take into account the origins and categories of electronic health data.

3.9. An EHR system designed to be used by natural persons shall enable their identification using any recognised electronic identification means as defined in Regulation (EU) No 910/2014, regardless of the Member State that has issued it. If the service supports other electronic identification means, they shall be of assurance levels 'substantial' or 'high'.

ANNEX III

TECHNICAL DOCUMENTATION

The technical documentation referred to in Article 24 shall contain at least the following information, as applicable to the relevant EHR system:

1. A detailed description of the EHR system including:
   (a) its intended purpose, the date and the version of the EHR system;
   (b) the categories of electronic health data that the EHR system has been designed to process;
   (c) how the EHR system interacts or can be used to interact with hardware or software that is not part of the EHR system itself;
   (d) the versions of relevant software or firmware and any requirement related to version update;
   (e) the description of all forms in which the EHR system is placed on the market or put into service;
   (f) the description of hardware on which the EHR system is intended to run;
   (g) a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing, including where appropriate, labelled pictorial representations (e.g. diagrams and drawings), clearly indicating key parts/components and including sufficient explanation to understand the drawings and diagrams;
   (h) the technical specifications, such as features, dimensions and performance attributes, of the EHR system and any variants/configurations and accessories that would typically appear in the product specification made available to the user, for example in brochures, catalogues and similar publications, including a detailed description of the data structures, storage and input/output of data;
   (i) a description of any change made to the system throughout its lifecycle;
   (j) the instructions of use for the user and, where applicable, installation instructions.
2. A detailed description of the system in place to evaluate the EHR system performance, where applicable.
3. The references to any common specification used in accordance with Article 23 and in relation to which conformity is declared.
4. The results and critical analyses of all verifications and validation tests undertaken to demonstrate conformity of the EHR system with the requirements laid down in Chapter III of this Regulation, in particular the applicable essential requirements;
5. A copy of the information sheet referred to in Article 25.
6. A copy of the EU declaration of conformity.

ANNEX IV

EU DECLARATION OF CONFORMITY

The EU declaration of conformity shall contain all of the following information:

1. The name of the EHR system, version and any additional unambiguous reference allowing identification of the EHR system.
2. Name and address of the manufacturer or, where applicable, their authorised representative.
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the manufacturer.
4. A statement that the EHR system in question is in conformity with the provisions laid down in Chapter III of this Regulation and, if applicable, with any other relevant EU legislation that provides for the issuing of an EU declaration of conformity.
5. References to any relevant harmonized 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.