European Journal of Risk Regulation (2024), **15**, 939–949
doi:10.1017/err.2024.25

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

European Health Data Space – Is the Proposed Certification System Effective against Cyber Threats?

Federica Casarosa

Scuola Superiore di Studi Universitari e di Perfezionamento Sant'Anna, Pisa, Italy
Email: federica.casarosa@santannapisa.it

Abstract

The proposal for a European Health Data Space aims at creating a common space where individuals may control their health data in a trusted and secure way. The objective is not only improving healthcare delivery, but also enhancing the opportunities to use health data for research and innovation. To achieve these results, the proposal implements a mandatory self-certification scheme for European health records systems as well as for wellness devices and applications, setting up essential requirements related to interoperability and security. Although this is the first intervention that sets a horizontal framework that is mandatory for all Member States, the security requirements that are included in the legislative proposal are not sufficiently detailed and comprehensive. Given that cyberthreats are increasing and security incidents affecting health data may potentially have an impact on the lives of patients, it is important that cybersecurity measures are adopted and implemented in the most effective way. The paper will analyse the European Health Data Space proposal pointing to the open issues and doubts that may be emerging and it will compare them with the proposed Cyber Resilience Act, identifying the issues that may be solved thanks to this horizontal regulation and the ones that instead remain open.

Keywords: certification; cybersecurity; European Health Data Space; health data

I. Introduction

The COVID-19 pandemic provided the worst-case scenario, clearly showing the difficulties emerging in achieving meaningful and effective health data sharing to facilitate biomedical research in Europe. However, practitioners and academic communities have already acknowledged this situation as problematic. The pandemic provided a more substantial justification to push forward the EU Commission's plan to create a common European Health Data Space. The initial plan was presented in early 2020 as one of the pillars of the European Data Strategy,[1] along with the Data Governance Act[2] and the recently adopted Data Act.[3] The overall strategy aimed at providing new avenues for

[1] Commission, "A European strategy for data" (Communication) COM(2020) 66 final.

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

[3] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (2023) OJ L2023/2854.

the use of data and developing a common data space where data can be accessed and shared safely and securely.[4]

According to the view of the Commission, the data space would provide a framework where health data would be stored, managed and operationalised to contribute to research developments, overcoming the challenges of limited data interoperability, fragmented rules for access to data for research, and barriers on individuals to exercise access to and control over their health data.[5]

The European Health Data Space Regulation (EHDS) proposal was then presented in May 2022 to set a benchmark for other areas of law and jurisdictions.[6] The EHDS proposal addresses two challenges: on the one hand, the need to expand the use of electronic health data to deliver healthcare to the individual from whom those data were collected, and on the other hand, the need to improve research, innovation, policy making, patient safety, personalised medicine, official statistics or regulatory activities. The first set of purposes are qualified as primary use of health data, while the others are secondary use of data.

Although the number of contributions addressing the risks and issues associated with the secondary use of health data has steadily increased since the first presentation of the EHDS proposal,[7] less attention has been devoted to the analysis of the rules applicable to the primary use of data,[8] and in particular to the cybersecurity requirements defined in the EDHS proposal.[9] This contribution aims to fill this gap by focusing on the rules applicable to electronic health records systems and those applicable to wellness devices and applications that, according to the definition in the EHDS proposal, guarantee interoperability with electronic health records systems.[10] Although relevant, the security requirements envisaged by the legislative proposal are insufficient to safeguard the cybersecurity of electronic health data collected and stored in the Electronic Health

[4] This data-driven approach vis-à-vis health data was already defined in Commission, "Enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society" (Communication) COM(2018) 233 final. See P de Hert and A Kiseleva, "Creating a European Health Data Space: Obstacles in Four Key Legal Areas" (2021) European Pharmaceutical Law Review.

[5] Commission, "Digital health data and services – The European health data space" (Consultation) which ran from 23 December 2020–04 February 2021, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Digital-health-data-and-services-the-European-health-data-space_en> (last accessed 21 March 2024).

[6] AEPD, "Approach to Data Spaces from GDPR Perspective" (AEPD 2023) <https://www.aepd.es/documento/approach-to-data-spaces-from-gdpr-perspective.pdf> (last accessed 21 March 2024). M Shabani, "Will the European Health Data Space Change Data Sharing Rules?" (2022) 375 Science 1357.

[7] P Terzis, "Compromises and Asymmetries in the European Health Data Space" (2022) 30 European Journal of Health Law 345; Shabani (n 6); S Slokenberga, "Scientific Research Regime 2.0? Transformations of the Research Regime and the Protection of the Data Subject That the Proposed EHDS Regulation Promises to Bring Along" [2022] Technology and Regulation 135; S Slokenberga, O Tzortzatou and J Reichel (eds), *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe*, vol 43 (Springer International Publishing 2021); de Hert and Kiseleva (n 4); E Biasin, "Synthetic Data: Implications for Healthcare and Data Law" (2023).

[8] Few exceptions are P Terzis and (E)OS Echeverria, "Interoperability and Governance in the European Health Data Space Regulation" (2023) Medical Law International 096853322311656; G Bincoletto, "Data Protection Issues in Cross-Border Interoperability of Electronic Health Record Systems within the European Union" (2020) 2 Data & Policy e3; C Stellmach, MR Muzoora and S Thun, "Digitalization of Health Data: Interoperability of the Proposed European Health Data Space" in P Scott and others (eds), *Studies in Health Technology and Informatics* (IOS Press 2022).

[9] E Biasin and E Kamenjasevic, "Cybersecurity of Medical Devices: Regulatory Challenges in the European Union" in IG Cohen and others (eds), *The Future of Medical Device Regulation* (1st edn, Cambridge University Press 2022).

[10] This contribution will not address the case of devices and application that fall into the definition of medical devices, as they are covered by the rules defined in the 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 (2017) OJ L117/1. For more discussion on this issue please see K Ludvigsen, S Nagaraja and A Daly, "When Is Software a Medical Device? Understanding and Determining the 'Intention' and Requirements for Software as a Medical Device in European Union Law" (2022) 13 European Journal of Risk Regulation 78.

Records systems. This is due to the narrow perspective adopted by the EHDS proposal only towards the confidentiality perspective, disregarding the integrity and availability of networks and data. Moreover, not only no ex-ante assessment of compliance with the essential requirements is envisaged, but in the case of strict interpretation, wellness devices and applications may not be subject to monitoring and corrective obligations in the case of potential risks and incidents that may affect the health and safety of patients. This negative evaluation can still be tempered, but coordination is crucial.

The contribution will initially address the rules applicable to Electronic Health Records systems, Section II, and to wellness devices and applications, Section III, highlighting the main critical issues emerging from the cybersecurity perspective. Section IV will then provide some tentative solutions thanks to the coordination between the EHDS proposal and the co-eve Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act – CRA proposal), showing that the latter may have the opportunity to solve at least part of the mentioned critical issues.[11] Conclusions will follow.

II. The evolution of Electronic Health Records Systems

The Electronic Health Records (EHR) system was put in place in 2008 to enhance the shift of patient documentation from paper to digital format, with the final objective of making the EHR accessible throughout Europe and strengthening the protection of citizens' health.[12] EHR systems have several benefits, including reducing errors, improving patient safety, better communication, and potentially reducing costs.[13] Truthfully, the EHR system has passed through an initial cumbersome process of transcribing the existing medical data until it is collected and managed on paper and entered into an electronic format. This first step required quite an adaptation effort, not only regarding adopting new legal rules and provisions applicable to medical data collection and storage but also an investment in the training and education of all medical practitioners.[14] The second step was setting up a technical and legal framework that would allow the sharing of the gathered medical data by the different actors (ie patients, healthcare providers and health insurance companies) for processing and communication. The EHR is qualified as a comprehensive medical record, or similar documentation, of the past and present physical and mental state of health of an individual in electronic form and provides for ready availability of these data for medical treatment and other closely related purposes.[15] Given the sensitivity of this broad set of information, it must be safeguarded from the data protection perspective.[16]

The European intervention in this area was initially carried out using Recommendations, which set the common principles to be implemented at the national

[11] Commission "Proposal for a Regulation (EU) of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020" <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454> (last accessed 21 March 2024). Pending the publication, the Proposal was approved by the European Parliament on 12 March 2024. The article will refer to the latest version of the document, before the EP approval.

[12] P Kierkegaard, "Electronic Health Record: Wiring Europe's Healthcare" (2011) 27 Computer Law & Security Review 503.

[13] S Hoffman, "EHR Data Security," *Electronic Health Records and Medical Big Data: Law and Policy* (1st edn, Cambridge University Press 2016) 16–20.

[14] For the initial (negative) evaluation of the EHR system adopted in US by doctors and medical experts, see ibid. 32–33.

[15] See point 3 (d) of the Recommendation on cross-border interoperability of EHR systems.

[16] Art 29 Working Party also highlighted this issue in the first appraisal of the EHR system. See Art 29 Working Party "Working Document on the processing of personal data relating to health in electronic health records (EHR)" (WP 131, 2007).

level.[17] The last recommendation issued by the Commission was then devoted to identifying a standard exchange format[18] and aimed at facilitating the cross-border exchange of EHR by indirectly supporting the introduction of interoperable EHR at the national level. Although a system of voluntary cooperation among Member States exists, thanks to the eHealth network and the eHealth Digital Service Infrastructure,[19] the information systems used at the national level for recording, retrieving and managing health records were deemed incompatible due to varying formats and technical standards. The lack of interoperable standards was considered one of the significant barriers to accessing health personal data.[20] The 2019 Recommendation was another effort to solve this problem, providing a set of principles governing the access and exchange of EHRs, baseline technical specifications and a coordinated process to elaborate the format further. Among the principles, data security is also included to safeguard data transmission across different national infrastructures. In particular, to protect the integrity and confidentiality of personal data, EHR systems should incorporate security measures, such as auditing and archiving of access and backup mechanisms.[21]

The baseline for the European EHR exchange format described in the Recommendation is then developed in the EHDS proposal, where Article 6 allocates explicitly the power to the Commission "to lay down the technical specifications for the priority categories of personal electronic health data [. . .], setting out the European electronic health record exchange format."[22] Then, according to Article 14 of the EHDS Proposal, the EHR systems intended for the primary use of electronic health data should comply with a mandatory certification scheme based on the set of requirements identified in Article 17 of the EDHS Proposal and subsequently specified in the Annexes.

The essential requirements listed in Annex II of the EHDS proposal are the baseline for the manufacturers of EHR systems. Among them, a specific section is dedicated to (cyber) security issues. The security perspective adopted in the EHDS proposal follows the principles defined in Recommendation 2019 on the standard exchange format for EHR. The security requirements mainly focus on preventing unauthorised access to electronic health data, requiring the adoption of reliable mechanisms for identification and authentication of health professionals, allowing different access rights depending on the specific role and supported by digital signature.[23] Interestingly, the EHR system should enable patients (ie data subjects) to restrict access to electronic health data, except for

[17] For an overview of the applicable national legislation, see Anna Essen et al., "Patient Access to Electronic Health Records: Differences across Ten Countries" (2018) 7 Health Policy Technology 44, 45.

[18] Commission, "European Electronic Health Record exchange format" (Recommendation) COM(2019) 800 final.

[19] Respectively <https://health.ec.europa.eu/ehealth-digital-health-and-care/eu-cooperation/ehealth-network_en> (last accessed 21 March 2024), and <https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en> (last accessed 21 March 2024).

[20] See Commission, "State of Health Preparedness Report" (Communication) COM(2022) 669 final, 8.

[21] See Bincoletto (n 8).

[22] Art 6 EHDS Proposal clarifies that the format includes three main elements: the datasets containing electronic health data and defining structures, the coding systems and values to be used in datasets containing electronic health data, and the technical specifications for the exchange of electronic health data. Art 6 should be read in the light of the Recital 72 EHDS proposal, which explicitly refers to the European Interoperability Framework and promotes its use to ensure legal, organisational, semantic and technical interoperability. See also W Li and P Quinn, "The European Health Data Space: An Expanded Right to Data Portability?" (2024) 52 Computer Law & Security Review 105913.

[23] Note that according to point 3.4 Annex II EHDS, the logging information that should be recorded are the following: "(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."

emergencies. These measures align with the security-by-design perspective envisaged in the General Data Protection Regulation, which requires that any data processing activity be adequately secured against unauthorised access or unlawful processing, accidental loss, disclosure, destruction or damage, and identity theft or fraud.[24]

Although relevant, these essential requirements are insufficient to safeguard the cybersecurity of electronic health data collected and stored in the EHR systems. For instance, these measures cannot provide any solution in case of denial-of-service attacks, malware attacks, or social engineering threats.[25] For example, in case of a denial-of-service attack, users of an EHR system may not be able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure. Such an attack, then, may affect the possibility of the patient or the healthcare provider (a doctor or a hospital) to provide the needed service, ranging from slowness in patient admission to risks to patient safety due to unavailability of IT services in emergencies. The abovementioned cases are all threats listed in the recent ENISA Health threat landscape as the most relevant threats after ransomware attacks and data threats.[26] Such concerns were also confirmed by the evaluations of the Italian Data Protection Authority as regards the vis-à-vis the draft decree adapting the national EHR system.[27] Remarkably, the Italian DPA affirmed that the legislation, to be acceptable from the data protection perspective, should (1) ensure minimum levels of security, (2) identify criteria for encryption and for the separation of data capable of revealing health status and sexual life from other personal data, (3) indicate the entity responsible for carrying out authorisation activities, management of privileges, and profiling of authorised subjects, (4) envisage technical measures to be adopted concerning sensible data subject. Moreover, the Italian DPA suggested that legislation should require manufacturers (a) to apply the principles of privacy by default/design in the design and development phases of EHR, (b) to adopt policies and procedures aimed at ensuring that the development of EHR takes place in compliance with secure coding guidelines conforming to best practices and there is constant monitoring, identification and replacement of third-party libraries presenting vulnerabilities that malicious attacks may exploit, (c) to adopt and maintain procedures to test, verify and regularly evaluate the effectiveness of technical and organisational measures to ensure the security of processing (including risks of homonymy resulting from software bugs, transcoding errors, or metadata association with documents, in the interactions between the various components of the systems with particular attention to integration tests of components and services).

Considering the risks identified by ENISA and the Italian DPA, the cybersecurity baseline of the EDHS proposal is insufficient. The EDHS proposal is focused only on the confidentiality perspective, bearing less if no attention to the other two dimensions associated with cybersecurity, namely availability and integrity.[28]

[24] Bincoletto (n 8).

[25] Social engineering encompasses a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services, see ENISA, "Health Threat Landscape" Report/Study 14 <https://www.enisa.europa.eu/publications/health-threat-landscape> (last accessed 21 March 2024).

[26] See ibid.

[27] See Italian Data Protection Authority, "Opinion on the Ministry of Health draft decree, to be adopted together with the Minister delegate for technological innovation and digital transition, in consultation with the Minister of Economy and Finance, on the Electronic Health Record (EHR)" (Opinion n. 256, 2023) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9900433> (last accessed 21 March 2024).

[28] See ENISA, "Security and Resilience in eHealth Infrastructures and Services" (2015) Report/Study 21 <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services> (last accessed 21 March 2024).

An additional element to consider is that the proposal envisages the need for further specifications of the requirements set in Annex II, and it leaves the task of defining "Common specifications" to the Commission under Article 23 of the EHDS Proposal. However, as affirmed elsewhere,[29] the process for drafting Common specifications is neither transparent nor inclusive of the relevant stakeholders. Additionally, the EHDS proposal does not envisage the possibility of referring to standards, European or international, which may provide coherent, updated and comprehensive requirements.[30]

The security requirements are then subject to a certification process based on the self-assessment of the EHR system manufacturer. The latter will ensure that the product complies with all the obligations in Article 17 of the EHDS Proposal. The market surveillance authorities then oversee the process set up at the national level.[31] The authorities shall be able to exercise their powers of investigation and enforcement,[32] requiring the EHR system manufacturer to take preventive or corrective measures in case of risks or incidents. Although the self-assessment procedure is a way of enhancing the autonomy and responsibility of the manufacturer in complying with the essential requirements, such procedure has a degree of risk as regards the reliability of the evaluation. Given the potential impact of a misevaluation of cybersecurity compliance, it may be more reasonable to have a third-party assessment that could verify the compliance in advance.

III. Wellness devices and applications

The EHDS Proposal also extends its scope of application to the so-called wellness devices and applications (wellness D&A). The latter is defined as "any appliance or software intended by the manufacturer to be used by a natural person to process electronic health data for purposes other than healthcare, such as well-being and pursuing healthy lifestyles."[33] According to recital 35 of the proposal, wellness D&A become relevant as they can collect several types of data that can become health data if they are processed to identify specific health conditions or if they are processed together with other data concerning health. For instance, the data collected by a wellness D&A regarding an individual's physical activity may become health data if they relate to the medical prescriptions of a doctor regarding strategies to reduce the level of cholesterol.[34] As is underlined by an evaluation of the proposal by the EDPB and EDPS,[35] it is clear that the

[29] F Casarosa, "Cybersecurity Certification of Artificial Intelligence: A Missed Opportunity to Coordinate between the Artificial Intelligence Act and the Cybersecurity Act" (2022) 3 International Cybersecurity Law Review 115.

[30] It is interesting that the EHDS Proposal does not mention the International Patient Summary developed by the European Committee for Standardization (CEN Technical Specification for the implementation guideline for European use of the International Patient Summary, CEN/TS 17288:2020) nor the ISO 23903 standard dedicated to interoperability and integration reference architecture. ISO/TC 215 Health informatics (2021) ISO 23903:2021, <https://www.iso.org/obp/ui/> (last accessed 21 March 2024).

[31] See Art 28 EHDS Proposal.

[32] See Art 31(7) EHDS Proposal. It must be noted that Art 28 EHDS Proposal clarifies that the market surveillance authorities will be subject to the rules defined in Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products (2019) OJ L 169/1, thus allocating both the investigative and enforcement powers as regards the product's compliance.

[33] Art 2(2)(o) EHDS proposal.

[34] As is underlined by an evaluation of the proposal by the EDPB and EDPS, it is clear that the quality requirements and characteristics of the health-related data generated by wellness applications are lower than those generated by medical devices. See EDPB-EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, p. 12, <https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf> (last accessed 21 March 2024).

[35] EDPB-EDPS (n 34).

quality requirements and characteristics of the health-related data generated by wellness applications are lower than those generated by those qualified as medical devices.[36]

The purpose of including such wellness D&A within the scope of the EHDS proposal is to enhance their interoperability with the existing EHR system and allow the possibility of collecting and using the data produced by such devices and applications for healthcare purposes. However, given that not all wellness D&A gather data that may be relevant for healthcare purposes, the EHDS proposal does not impose a mandatory certification system. Instead, it leaves the manufacturers to decide whether to start the certification process. This will depend on the manufacturers' interest in including their devices and applications in the infrastructure for the primary use of electronic health data.[37]

According to Article 31 of the EHDS Proposal, the wellness D&A that claims interoperability with the EHR systems should comply with the essential requirements laid down in Annex II, namely the abovementioned mechanisms to ensure the safe and secure processing of data and the prevention of unauthorised access; the identification and authentication mechanisms (including role-based control); the log records; the tools to allow natural persons to restrict access to personal data; the digital signature mechanisms; and the control over data retention periods.[38] As mentioned above, these requirements are insufficient to safeguard security. Moreover, in this case, the certification system is based on a self-assessment conformity test, which is left entirely to the manufacturer of the wellness device, following the same rules that apply to EHR systems.[39] The market surveillance authorities then oversee the system with investigation and enforcement powers. However, no ex-ante third-party assessment is envisaged in the certification process.

It is important to note that Article 31 (7) of the EHDS only mentions that the market surveillance authorities will check compliance with the essential requirements provided in Annex II. No mention of the extension of obligations related to handling risks and serious incidents, defined in Article 29 of the EHDS, is included. Will the manufacturer of wellness D&A have to inform the market surveillance authority about a serious incident that affects the device? Serious incidents are defined as any malfunction or deterioration in the characteristics or performance that directly or indirectly leads, might have led or might lead to the death of a natural person or serious damage to a natural person's health; a serious disruption of the management and operation of critical infrastructure in the health sector.[40] In this case, if applicable, the manufacturer of wellness D&A would be required to notify no later than 15 days after becoming aware or immediately after they have established a causal link between the application and the event (or the reasonable likelihood of such link).[41] If interpreted strictly, Art. 31 of the EHDS does not extend any obligation applicable to the EHR or wellness D&A apart from the need to ensure interoperability between the two; however, it would be an incomplete and, potentially, an inefficient system of control if, after having imposed the obligation to comply with the same standards of security, the wellness D&A will not have any subsequent monitoring and correction obligations in case of risks, or even incidents, affecting the health and safety of patients.

[36] It is important to note that the definition of "personal health data" provided by the EHDS proposal is inconsistent with the one provided in Art 4(15) GDPR and may lead to doubts on the accuracy and reliability of data. See the detailed analysis in Richard Rak, *Internet of Healthcare (Law): Privacy and Data Protection Aspects in an Internet of Everything*, (Doctoral Thesis, 2023) <http://amsdottorato.unibo.it/10715/1/RichardRudolfRak_DoctoralThesis_final.pdf> (last accessed 21 March 2023).

[37] See Terzis and Santamaria Echeverria (n 8).

[38] See Annex II, point 3 EDHS Proposal.

[39] See Art 26 EHDS Proposal.

[40] Art 2 (2) (q) EHDS Proposal.

[41] Art 29 (4) EHDS Proposal.

From the cybersecurity perspective, the current framework applicable to EHR and wellness D&A does not guarantee a sufficient level of protection: (1) essential requirements dedicated to security are focused only on the confidentiality perspective, disregarding the issues of integrity and availability of networks and data; (2) the monitoring activity of market authorities can only be exercised after the products are put on the market, with no ex-ante assessment of the compliance with the essential requirements; (3) in case of a strict interpretation of Article 31 of the EHDS, wellness D&A may not be subject to monitoring and corrective obligations in case of potential risks and incidents that may affect the health and safety of patients. This negative evaluation can still be tempered, thanks to the interplay between the EHDS proposal and another legislative document explicitly addressing the cybersecurity dimension, namely the Proposal for a Cyber Resilience Act. Thanks to the coordination between the two documents, some of the issues emerging in the EHDS proposal may be solved, while others remain open.

IV. The gap-filling role of the Cyber Resilience Act

EHR systems and wellness D&A must comply with the requirements in the proposed Cyber Resilience Act (CRA Proposal) regarding cybersecurity, defining pre-market and post-market obligations. This Regulation was first proposed in 2022 to address the risks and challenges of cybersecurity, which were already identified in the EU's Cybersecurity Strategy for the Digital Decade presented in 2020.[42] The intervention was justified by the increasing awareness that malicious attacks can exploit vulnerabilities of any product connected online, eventually leading to negative consequences that spread across devices regardless of country borders.

The CRA aims to lay down horizontal rules for any "product with digital elements" available on the European market. Article 3(1) CRA Proposal defines the latter as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately."[43] In the case of software, the CRA specifies that it qualifies as remote processing, ie "any data processing at a distance for which the software is designed and developed by the manufacturer [...], and the absence of which would prevent the product [...] from performing one of its functions."[44] Although the scope of application does not cover the products with digital elements that fall in the definition of medical devices, both EHR systems and wellness D&A can squarely fall in the definition of products with digital elements.

EHR systems and wellness D&A, thus, must comply with the requirements set out in the CRA Proposal regarding cybersecurity, defining both pre-market and post-market obligations. Before they are put on the market, all products with digital elements must be designed, developed and manufactured in such a way as to ensure an appropriate level of cybersecurity.[45] Products must be delivered without known exploitable vulnerabilities and deployed in a secure default configuration. The basic requirements are set in Annex II and include, on the one hand, the security aspects and, on the other hand, the vulnerability handling aspects. Under the first category, the list consists of security by default measures, confidentiality protection, integrity and availability of the data and the networks, data minimisation measures, resilience measures (particularly against DoS attacks), safeguards

[42] Commission "The EU's Cybersecurity Strategy for the Digital Decade" JOIN(2020) 18 final.

[43] Art 3(1) CRA Proposal.

[44] Art 3(2) CRA Proposal. Note that the CRA proposal does not cover the case of Software as a service, as it may fall in the definition of cloud computing service providers already included in the category of essential operators, pursuant Art 3 NIS 2 Directive.

[45] Art 10 (1) and Annex I Part 1 CRA proposal.

against network effects, records on internal activity, and data portability. Additionally, products shall ensure protection from unauthorised access by appropriate control mechanisms and protect the confidentiality considering methods such as encryption.

Differently from the EHDS proposal, Article 18 (2) CRA Proposal acknowledges two possible standardisation techniques: on the one hand, to request by the Commission to the European Standardisation organisations to draft harmonised standards, and on the other, the adoption of common specifications, such as in EHDS proposal. However, this second option is only a fallback situation if the first one is not accepted. The first option is more reliable and transparent, as the process envisaged for adopting European Standards is based on consensus, openness, transparency, national commitment and technical coherence principles. Moreover, it also includes the possibility to involve stakeholders and experts from industry, associations, public administrations, academia and societal organisations.[46]

The technical documentation that manufacturers should prepare before the products are put on the market should contain an assessment of cybersecurity risks and describe the means used by the manufacturer to meet the essential cybersecurity requirements and mitigate the risks.[47]

To receive the declaration of conformity, manufacturers should follow conformity assessment procedures,[48] proving that their products comply with the abovementioned requirements. Depending on the class of risk of the product, the type of conformity assessment may vary, ranging from an internal control procedure to a conformity assessment based on full quality assurance. Internal control conformity assessment is only available for those products with digital elements that do not perform any of the functions listed in Article 6 (2). In particular, Article 6 (2)(b) of the CRA Proposal provides as one of the criteria the fact that "the product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or the health and safety of a large number of individuals through direct manipulation, such as a central system function, including network management, configuration control, virtualisation, processing of personal data." Although wellness D&A will not fall under this category, EHR systems may fall under this category and be subject to the third-party conformity assessment procedure.

After this process, manufacturers may receive a declaration of conformity following the template in Annex IV and will be able to obtain the CE marking. The product is then subject to post-market surveillance controls by specifically defined authorities, which can take all appropriate corrective actions to bring it into compliance, withdraw it from the market, or recall it within a reasonable period.[49]

It is important to note that in the case of becoming aware of exploited vulnerabilities or incidents having an impact on the security of the product with digital elements, the manufacturer is obliged to notify the event within 24 hours to the national Computer Security Response Team (CSIRT),[50] providing the most relevant information about the event, as well as the corrective and mitigating measures taken.[51] The information about the incident should also reach the product user to request the latter's collaboration in the

[46] CEN/CENLEC, "What is a standard?" <https://www.cencenelec.eu/european-standardization/european-standards/> (last accessed 21 March 2024).

[47] Art 23 and Annex V CRA Proposal.

[48] Art 10 (7) and Art 24 CRA proposal.

[49] Art 43(1) CRA Proposal.

[50] The CSIRT is the body designated according to the Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) (2022) OJ L 333/80.

[51] Art 11 (1) and (2) CRA Proposal.

deployment of corrective measures; however, in this case, no specific timeline is set up.[52] According to Article 11 (2dd) of the CRA Proposal, ENISA has the role of setting up (and maintaining) a single reporting platform to collect notifications regarding vulnerability cases and incidents.

It must be highlighted that the interplay between the CRA and the EHDS proposals was already envisaged by the legislator, as in its Article 24 (4), the CRA proposal acknowledges that manufacturers of EHR systems and wellness applications and devices must comply with both acts. Therefore, the Article affirms there is no need to duplicate the technical documentation as the one drafted by the manufacturer will suffice to meet the obligations defined in the two acts.[53] However, this coordination is only limited to the supply of technical information, but it does not extend to any other element in the procedure. Therefore, the conformity assessment will follow the rules defined in the relevant legislative act and will be carried out independently.

As a result of this analysis, it is possible to affirm that the CRA Proposal may solve some of the problems highlighted in the EHDS regarding cybersecurity issues. First, the CRA Proposal is more detailed and precise regarding the security requirements, the essential requirements to be adopted, and the vulnerability handling measures. EHR and wellness D&A also fall into the definition of products with digital elements so that such provisions will be applicable and complement the fewer present in the EHDS proposal, strengthening the level of protection. Additionally, it envisages the possibility of adopting European standards that are transparent and based on the participation of relevant stakeholders and experts. Second, the CRA proposal identifies a well-defined procedure in the case of security incidents or vulnerability exploitation, which will again apply to EHR systems and wellness D&A. However, it must be noted that the interplay between the two proposals may solve the risk of under efficient monitoring and control over wellness D&A. Still, it may duplicate the obligations for EHR system manufacturers. According to Article 28 of the EHDS Proposal, the manufacturer must notify two different authorities with different timelines and documentation required if the security incidents also qualify as serious ones.

One of the issues the CRA Proposal does not solve is the ex-ante control of the compliance with the security requirements. Although, in principle, the EHR systems may fall in the category of products with digital elements that are subject to third-party assessment, according to Article 6 (2) (b) of the CRA Proposal, the same Act relieves the manufacturers from this obligation, as Article 24 (4) provides that the conformity assessment will follow the rule defined in the EHDS, namely the self-assessment procedure.

V. Conclusion

According to ENISA, the healthcare sector is one of the prime victims of cyber attackers, and this was even exacerbated by the COVID-19 pandemic when patient data were subject to several ransomware attacks.[54] Securing patient data becomes crucial when looking at the long-term strategy of the EU to set up a European Health data Space that will allow healthcare providers and wellness applications to share health data that will be accessed across the EU. The envisaged data space will be based on the health data collected in the EHR systems and the (interoperable) wellness D&A. Each includes several components allowing health records to be created, stored and retrieved. All the rules and procedures, processing and storage devices, and communication and support facilities must ensure that the data are protected from cyber-attacks that may hamper data confidentiality, availability and integrity.

[52] Art 11 (4) CRA Proposal.
[53] Art 23 (3) CRA Proposal.
[54] ENISA (n 25) 3.

Cybersecurity measures should then be adopted, following the design and development of both EHR systems and (interoperable) wellness D&A. The current EHDS proposal has the merit of addressing security, including requirements for EHR systems and wellness D&A. However, the current text of the EHDS proposal does not guarantee a sufficient level of protection in terms of security: the essential security requirements are focused only on the confidentiality perspective, disregarding the issues of integrity and availability of networks and data; the monitoring activity of market authorities can only be exercised after the products are put on the market, with no ex-ante assessment of the compliance with the essential requirements; and in case of a strict interpretation of Article 31, wellness D&A may not be subject to monitoring and corrective obligations in case of potential risks and incidents that may affect the health and safety of patients.

Analysed in an isolated manner, the current text of the EHDS proposal is insufficient to safeguard the security of the health data collected by EHR systems and wellness devices. However, this negative evaluation can be tempered when a more comprehensive perspective is adopted, and the coordination between the EHDS proposal and the CRA proposal is considered. This coordination effort is crucial to ensure that the detailed cybersecurity and vulnerability handling requirements defined in the CRA proposal will be applicable and, most importantly, complement the fewer ones included in the EHDS proposal. Still, the interplay between these two legislative proposals may increase complexity as in the case of security incidents that are also serious incidents, the manufacturer will have to notify two different authorities with different timelines and documentation required.

Both Acts are still in the legislative process, but some changes are still feasible. It will be crucial that the European legislator considers the interplay between the two Acts and evaluates if any modification in one of the two affects, negatively or positively, the overall level of cybersecurity for the envisaged European health data space.

Competing interests. The author has no conflicts of interest to declare.

Cite this article: F Casarosa (2024). "European Health Data Space – Is the Proposed Certification System Effective against Cyber Threats?" *European Journal of Risk Regulation* **15**, 939–949. https://doi.org/10.1017/err.2024.25