Data & Policy (2020), 2: e3, 1–11
doi:10.1017/dap.2020.2

COMMENTARY

Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union

Giorgia Bincoletto[1,2,*]

[1]Department of Legal Studies, University of Bologna, Bologna, Italy
[2]Department of Legal Studies, University of Luxembourg, Luxembourg City, Luxembourg
*Corresponding author. Email: giorgia.bincoletto2@unibo.it

(Received 23 August 2019; revised 05 December 2019; accepted 12 December 2019)

Keywords: data protection by design; digital health; EHR; EU policy; interoperability

Abstract

This study investigates the data protection concerns arising in the context of the cross-border interoperability of Electronic Health Record (EHR) systems in the European Union. The article first introduces the policies on digital health and examines the related interoperability issues. Second, the work analyses the latest Recommendation of the European Commission on this topic. Then, the study discusses the rules and the obligations settled by the General Data Protection Regulation to be taken into account when developing interoperable EHRs. According to the data protection by design and by default provision, EHR systems should be designed ex ante to guarantee data protection rules.

Policy Significance Statement

In the context of the European Union (EU) policies for the cross-border access to personal health data, it is of paramount importance for policymakers to take into account data protection requirements when defining new rules for the implementation of EHR system interoperability at Member State and EU levels. Data protection concerns and obligations are general conditions which have considerable impact on the future EU strategies for digital healthcare.

Introduction

Digital technologies have deeply transformed the provision of healthcare by enabling new opportunities for medical treatments and ensuring the sharing of data in more effective ways.[1] Within the European Union (EU) policies for the digital single market, the "transformation of health and care" plays a pivotal role. Three priorities have been identified in the "communication on digital transformation of healthcare in the digital single market" adopted by the European Commission (EC) in 2018.[2] Enabling EU citizens to access and share their health data securely across the Member States is the first area of action. Second, the EC calls for improving the data quality for research purposes, disease prevention and for enabling personalized healthcare. In the end, the Commission claims that further action at EU level is crucial for developing digital tools for citizens' empowerment and person-centered care. A public consultation on these three areas has been carried out. Results show that the lack of interoperability between Electronic Health Records (hereinafter EHRs)—that is, the comprehensive medical records of an individual that are

accessible in electronic form[3]—is one of the major barriers to access to health personal data in another Member State.[4]

The Directive on patients' rights in cross-border healthcare (Directive 2011/24) requires that EU citizens have the right to access healthcare in any EU Member State.[5] In 2018, the EC proposed to make some recommendations on how EHR systems could be accessed and shared more easily across Member States.[6] As argued by the Commission, EU standard formats for EHRs will make the access to health data easier for patients, health professionals, and other authorized parties from different records across the EU. On December 22, 2018, the feedback period was closed. The Recommendation was planned for the first quarter of 2019. So, on February 6, 2019, the Commission released the final version of the text.[7]

The cross-border interoperability and the secure access to EHR systems are necessarily bound with data protection issues. The General Data Protection Regulation (GDPR) sets the rules for the processing of personal data.[8] The purpose of the present study is to investigate the connection between the "transformation of health and care" EU policy and the data protection concerns arising in the context of interoperability of EHR systems. In particular, this contribution will identify rules and obligations settled by the GDPR to be taken into account when an EHR interoperability standard format is drafted. Addressing data protection and security in EHR systems demands the definition of clear legal rules. So, the study contributes to the ongoing debate by analyzing the new Recommendation of the European Commission and by examining certain data protection requirements.

To understand and investigate the policy at stake, the EC's Recommendations, Communications and Working documents, and the Council's documentation will be scrutinized. The text of the GDPR is a fundamental source of analysis because it is the general legal framework for data protection in the EU. Moreover, as the debate is still open, online feedback and the academic literature related to the present topic will be considered with an interdisciplinary approach.

Following this Introduction, section "The Interoperability of EHRs" will revolve around the "transformation of health and care" policy and the interoperability issue. Then, in section "The New Recommendation," the last Recommendation of the European Commission is analyzed. The article will focus on the data protection concerns and will investigate the requirements settled by the GDPR to be taken into account in section "The Data Protection Concerns and the Obligations Settled by the GDPR," giving particular attention to the data protection by design (hereinafter: DPbD) and by default obligations.[9] Conclusions are presented in section "Concluding Remarks."

The interoperability of EHRs

EU policies on health and care stress the importance of the use and implementation of e-health systems, such as EHRs, for more targeted, personalized, effective, and efficient healthcare and for reducing errors and length of hospitalization.[10] In the "transformation of health and care" policy, the access to healthcare and the sharing of health data are priorities of the EU agenda. Significant investments are made by EU and by Member States and costs continue to rise[11] (Arak and Wójcik, 2017). Many projects, initiatives, and studies were launched in the last years (Van Langenhove et al., 2013).

Given the impact of the digital technologies in healthcare, the EU Council called upon the Member States to conceive initiatives and strategies aimed at enabling interoperability of digital technologies across the EU.[12] However, the state of play highlighted many times by the EU institutions shows the urgent need to make progress on standardization and interoperability of e-health systems in order to foster the greater use of the digital tools.[1] Interoperability of these technologies is also necessary to enable the free flow of patients, products, and services in the EU market.[13]

From a general point of view, the term interoperability means "the ability of a system or a product to work with other systems or products without special effort on the part of the customer" (IEEE SA, 2016). Interoperability implies not only that information can be exchanged between many systems or services, but also the receiving system is able to use the information to perform new actions (Arak and Wójcik, 2017). It has been argued that the concept of interoperability has remarkably evolved due to the

advancements of digital technologies in healthcare (Blobel, 2018). Any definition encompasses a variety of layers: technical, semantic, organizational, and legal interoperability should be distinguished. First, technical interoperability allows the exchange of data from System A to System B neutralizing the distance; while, semantic interoperability ensures that System A and System B understand the data in the same way without ambiguity (Soceanu, 2016). Moreover, the organizational interoperability ensures that separated business processes are aligned.[14] Finally, legal interoperability concerns how to ensure that organizations operating under different legal frameworks are able to work together avoiding barriers on the data processing.[14]

In the context of the European Interoperability Framework (EIF) for public services, considerable efforts have been made by the EC in the healthcare domain.[15] According to the first Recommendation on this topic, EHRs are "comprehensive medical records or similar documentation of the past and present physical and mental state of health of an individual" available in electronic form for medical treatment and closely related purposes.[16] So, the interoperability of these systems allows the exchange and the use of the collected data between neighboring and non-neighboring Member States.[16] Healthcare interoperability covers, for examples, prescriptions for medications or investigations, examination reports, and clinic appointments, which are usually collected in different digital records, but they could be interoperable as well (Soceanu, 2016). The EC recommended the interoperability of EHRs at technical, semantic, organizational, and legal levels, adding a political layer (i.e., leveraging investments and adapting policies).[16] However, the Member States have different approaches on regulating EHRs. As regards legal interoperability, in 2014, only six Member States had established legal provisions setting a framework for the cross-border exchange (Milieu and Time.lex, 2014). Less than half of the Member States implemented specific technical rules and standards. Thus, the large majority of the countries did not have legal provisions relating to the different layers of interoperability. A binding legal requirement in the EHR systems implementation was neither available for the national nor for the EU frameworks. In 2017, during an online public consultation of the EC, high importance was assigned to support interoperability with harmonized standards. The results highlighted the need of open exchange formats, common data aggregations, and robust EU standards for health data quality, reliability, privacy, and cybersecurity.[4] Moreover, the participants agreed on the necessity to have a future EU legislation on these issues.

However, interoperability of EHRs does not implies uniformity of technologies and rules do not have to impose it (Milieu and Time.lex, 2014). Nevertheless, the presence of different data repositories and various data formats negatively effects the cross-border access to health data and increases the costs to provide care.[6] Moreover, as the mainly used tools are mostly based on closed proprietary solutions, the market has not yet deliver interoperable and open EHR solutions.[1] As a reply, and in order to avoid proprietary solutions creating vendor lock-in, the EU Council invited the Member States and the Commission to promote the use of international and open standards and underlined the need to create common data structures, coding systems, and terminologies to improve interoperability.[17]

Therefore, it has been argued that some factors should be put in place to achieve interoperability: (a) a thorough understanding of the operational environment; (b) the identification of inter-relationships and needs of stakeholders; (c) the presence of recommendations for redesigning services and processes; (d) supporting policies for the implementation; (e) incentives; and (f) availability of adequate resources (i.e., finances and time) (Kouroubalia and Katehakis, 2019). Interoperability needs to be achieved on different layers and a significant step forward is the EC's Recommendation that will be analyzed in the next section.

The New Recommendation

The Recommendation released in February 2019 follows all the EU efforts to overcome the interoperability issues and aims at the creation of European EHR format defining the principles that the system should comply with for the cross-border interoperability.[7] Moreover, the documentation establishes wide-ranging technical specifications for the access to the EHR and the interoperability, and promotes best

practices to ensure privacy and integrity of health data. Technical specifications are indicated as baseline for a future development and a governance process involving all the relevant stakeholders is recommended.

In the text, the EC specifies that Member States should use the tools provided by the European e-Health Digital Services Infrastructure and take appropriate measures to support the use of interoperable EHR systems at policy and legal levels. EU citizens should be able to access and securely share their electronic health data across borders to choose to whom they provide access and the level of detail of the shared health information.[7] So, the framework includes: (a) the principles that should govern the access and the exchange of EHRs across borders; (b) a set of common technical specifications in certain health information domains (i.e., the baseline for the exchange format); and (c) a process to take forward the further elaboration of the format.[7]

The principles are set out in the Annex of the Recommendation.[18] They are listed as follows: (a) "citizen centric by design," that is the implementation of DPbD and data protection by default at the development stage of the EHR; (b) "comprehensiveness and machine-readability," that is EHRs should be as comprehensive as possible and the data should be provided in machine-readable format to enhance the reuse; (c) "data protection and confidentiality," that is full compliance with confidentiality rules and data protection legislation from design stage onward; (d) "consent or other lawful basis," that is the presence of a legal ground of the data processing; (e) "auditability," that is the implementation of auditing and logging techniques; (f) "security," that is the implementation of appropriate technical and organizational measures to secure the EHR systems from any risk; (g) "identification and authentication," that is the use of strong and secure access mechanisms; (h) "continuity of service," that is the necessary continuity and availability of the EHRs exchange service. Furthermore, the baseline for the European EHR Exchange Format includes some interoperability specifications for representing and exchanging health data (appointing the standards). In the future the Commission's Exchange Format will be developed through a joint coordination process that takes into account the latest technological and methodological innovations.

Evaluating the Recommendation, some challenges could be underlined. First, it could conceivably be hypothesized that it will be necessary to remove the residual barriers existing at Member States level and to create efficient mechanism to sustain the cooperation. Indeed, the EC will monitor the implementation of the specifications, but the steps to achieve technical progress remain upon the Member States and, concretely, upon the market of EHRs. Looking at the concrete benefits of the detailed Recommendation, it may be the case that EU legislation will better harmonize the standards than the present soft-law approach. Nevertheless, high importance is assigned to privacy and data protection concerns. As section "The Data Protection Concerns and the Obligations Settled by the GDPR" will investigate, data security and privacy are significant challenges for the interoperability of EHR systems.

The Data Protection Concerns and the Obligations Settled by the GDPR

Some recent surveys highlighted that privacy problems are considered as deterrent from adopting e-health systems by legal practitioners (Lupiáñez-Villanueva et al., 2018). As mentioned above, the cross-border interoperability of EHRs is inevitably bound with data protection issues because of the processing of personal data. The security and privacy risks increase when systems are more interconnected as in this context because of the huge amount of data and processing, the different actors involved and the nature of the collected information. This section identifies the key data security and privacy concerns in the presented framework and the obligations settled by the GDPR to be taken into account when the interoperability standard format is drafted. The presentation of the issues is divided in four parts. The section "*Issues at legal interoperability layer*" analyses the concerns at the legal interoperability layer while the section "*Issues at organizational layer*" focuses on the organizational level. The data protection issues related to the technical layer are presented in the section "*Issues at technical layer.*" Then, the section "*GDPR obligations in the cross-border interoperability context*" summarizes the GDPR obligations related to interoperability embracing all levels.

Issues at legal interoperability layer

Legal interoperability needs coherence that avoids barriers between legislation.[14] The GDPR lays down the conditions that are directly applicable across the EU for the lawful processing of personal data. The regulation requires personal data to be protected so that all the principles are ensured: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.[19] Moreover, it provides many data subject's rights.[20] In the EHR systems, the collected data are mostly sensitive.[21] A higher level of protection to this information should be guaranteed because of the potential discrimination and misuse (Romanou, 2018) and the high risks (ENISA, 2017).

EHR systems are managed by national healthcare institutions and public administrations. Specifications for the data processing are provided at Member State level with possible disparities of statutory approaches (Milieu and Time.lex, 2014). As a result, the concerns for the legal layer are linked to the fragmentation of the existing national legislation. In order to ensure a consistent and higher level of data protection, Member States should establish clear interoperability policies. National law could determine more precisely conditions for the processing in the EHR.[22] However, legal interoperability could be eased by ensuring an aligned interpretation of the GDPR provisions and homogeneous applications of data protection principles in all Member States.

Issues at organizational layer

As explained above, organizational interoperability refers to policies and procedures that should be coordinated. Within the cross-border interoperability context, the patient's data is first processed in a Member State, then it is exchanged and used in another Member State for a new treatment or a medical consulting. Therefore, there will be two or more data controllers and processors. It may be argued that they are joint controllers. According to Article 26 of the GDPR, joint controllers both determine the purposes and means of the processing. This is not the case of the interoperability context, where operators are independent in the most common scenarios.[23] The different actors should comply with the data protection rules separately, but in the same way.

All the controllers should be responsible and demonstrate compliance (i.e., accountability principle). Documents on the cross-borders processing could be shared among the stakeholders. As the data processing is grounded on a risk-based approach and the level of privacy risks in this context is high, a Data Protection Impact Assessment (DPIA) must be carried out.[24]

Furthermore, it is interesting to notice that the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) have recently released a Joint Opinion on the processing of patients' data and on the role of the EC within the eHealth Digital Service Infrastructure (eHDSI).[25] The use of this infrastructure is recommended by the EC[7] and is necessary for the cross-border exchange. The Joint Opinion is the result of a consultation request pursuant to Article 42 (2) of the Regulation 2018/1725. This Regulation applies when the processing is carried out by EU institutions, bodies, offices, and agencies.[26] The EC is involved in the eHDSI processing as EU Institution. Thus, the GDPR applies to Member States and to the other actors (e.g., healthcare providers), while the Regulation 2018/1725 applies to the EC. Whenever the interoperability between EHR systems is enhanced with the eHDSI, the security of the transmission of personal health data is maintained by the private network developed by the EC. Therefore, the EDPB and the EDPS pointed out that the involvement of the EC entails the development of technical measures. The EC does not determine the purposes and means of the processing. However, from an organizational point of view, the opinion explains that the EC is the processor of the eHDSI processing operation.[27]

In addition to the issues related to the allocation of responsibilities, the presence of the legal basis for the cross-border exchange should be discussed. The "patient profile" in the EHR system is created in one national state, and then it is exchanged. So, the further processing abroad should be lawful and the legal ground should be present as in the first processing. In this matter, the GDPR lists the basis for processing of personal health data.[28] The cross-border exchange, access, and use of the EHR should be possible only if the legal ground of the first Member State is still lawful or another ground applies in the concrete case. It should be noted that the consent is only one of the possible legal grounds.[29] However, as collected data are

related to the health status of the data subject, if the legal basis is the consent, a prior explicit, informed and freely given consent is necessary for the exchange of health data in any EHR system.[30]

Moreover, personal data shall be processed in a transparent manner. The information should be provided to the patient by the data controllers in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.[31] So, in the next Member State, the information could be provided in the mother language of the subject, or any other well-known language.

Another fundamental concern that emerges in the organizational context is the possible circumvention of the purpose limitation principle. No different use and cross-border exchange is allowed if the patient data are collected for a specific healthcare purpose in the EHR. The secondary use of personal data for research purposes is allowed only in accordance with Article 89 of the GDPR. As a result, the further processing should be restricted to the limits of the main purpose or should be compatible with that one. Nevertheless, the first purpose could foresee the possibility of the interoperability for medical treatments and then the new controller will determine its own purpose, thus finding the legal ground if the new purpose is deemed incompatible and providing the information as prescribed by Article 13 (3) GDPR. In any case, a patient should have the opportunity to opt-out the sharing of data.[2]

Issues at technical layer

So far, this section has focused on legal and organizational layers. The following data protection issues are related to technical aspects of the EHR systems. According to the data minimization principle, the data in the EHR should be limited to what is necessary for the healthcare purpose and be adequate and relevant. Pseudonymization techniques could achieve this goal (Abedjan et al., 2019). This statement is still applicable for the interoperability scenario because the cross-border exchange of information should take place in accordance with the principles set out in the Annex of the EC and in the GDPR that includes data minimization. During the cross-border access and use, personal data collected and stored in the EHR systems should be limited to what is significant for the healthcare purpose and for the comprehensiveness of the records. Moreover, during the cross-border exchange, the patient's data should be accurate and kept up to date in all the interoperable EHR systems. These systems should be operative for no longer than what is necessary. The time limitation to the storage could be agreed among stakeholders. The archiving duration of EHRs is strictly related to the relevance of the collected data and so, it depends on the circumstances.

One aspect in this context relates to the access of data in the EHR. On the one hand, there is the right to access of the data subject,[32] and on the other hand, health professionals have the access in another Member State. As regards the first situation, the patient has the right to access and to know who accessed the EHR, the rights to rectification, to erasure, and to data portability. These rights are respectively established in Articles 15, 16, 17, and 20 of the GDPR and they safeguard any data subject involved in personal data processing. Granting these rights means that the EHR interoperable systems should have the technical functions to execute the patient's requests. Providing patients access and improving their control over EHR systems is one of the goals of interoperability. When a patient directly controls a digital healthcare record (i.e., the subject manages information on the record), the system is defined Personal Health Record (PHR) (Flaumenhaft and Ben-Assuli, 2018). The PHR could be synchronized with the EHR on patient request (Saripalle et al., 2019). However, as regards interoperable EHRs, the processing is carried out by healthcare providers. So, the exercise of the data protection rights and the expression of the consent are ordinary manifestations of the patient control.

Furthermore, the mechanism for the identification, authentication, and access of healthcare professionals to interoperable EHRs should be considered as a priority in the development of the systems. Enabling access to the patient history and providing the possibility to integrate new information abroad when consulting a specialist on receiving emergency treatment have positive impact on patient healthcare. So, the access and exchange of EHRs should be secure and implemented in full compliance with the GDPR through access control strategies and policies, secure communication channels, and high security standards to prevent any unauthorized access.[18]

Integrity and confidentiality are other fundamental data protection issues for interoperable EHRs. Personal data should be protected from data breaches and security incidents (e.g., losses, damages, etc.). According to Article 32 of the GDPR, systems should be properly secure with measures to ensure a security level appropriate to the concrete risks.[33] The protection against unauthorized access or unlawful processing, accidental loss, disclosure, destruction or damage, and identity theft or fraud, should be granted in each EHR system (Conley and Pocs, 2018). Auditing and archiving of the access and back-up mechanisms are common security measures for interoperable EHR systems.[18] However, harmonized standards for their implementation are required.[34]

According to Article 25 of the GDPR, EHR technologies should integrate DPbD and by default technical and organizational measures. The data protection by design obligation plays a major role in the development of EHRs (Conley and Pocs, 2018). The systems and standard formats should be designed to effectively implement the various data protection principles, to guarantee the compliance with the law, and to protect the rights of data subjects.[35] To apply DPbD requirement, a solution might be using an open and extendable architecture with privacy-by-design modeling and embedded risk analysis tools in order to provide systematic protection for storage and interoperable exchange of health data (Abedjan et al., 2019).

GDPR obligations in the cross-border interoperability context

By analyzing the GDPR within the interoperability context, a number of obligations can be identified and summarized as follows: (a) the implementation of appropriate data protection safeguards (Article 24); (b) the implementation of the DPbD and by default technical and organizational measures (Article 25); (c) the maintenance of the records of the processing (Article 30); (d) the cooperation with the supervisory authority (Article 31); (e) the implementation of the security measures (Articles 32–34); (f) the execution of the DPIA (Article 35); (g) the designation of a data protection officer (DPO, Article 37); and (h) the compliance with data subject's requests (e.g., for the exercise of rights). It may be noticed that these obligations are indirectly indicated in the list of principles released by the EC in the Recommendation described above.[18]

Consequently, even in the interoperability context data controllers should implement both organizational and technical measures (a, b, and e) for ensuring data protection and for avoiding the administrative fines set by the GDPR.[36] A wide variety of safeguards should be applied, and certifications may be used to demonstrate compliance with the obligations.[37] Several technical aspects have been explained in section "*Issues at technical layer.*" The DPbD and by default measures (b) are central to develop compliant EHR systems for minimizing the risks. The cross-border information exchange should be designed with data protection in mind too, meaning that appropriate measures should be embedded in the network infrastructure to secure the access and the data sharing. The approach for complying with DPbD obligation is risk-based and many criteria should be taken into account.[38] As a result, on the one hand, there is no ready-made recipe for compliance with the data protection rules and only guidelines could lead the controllers (EDPB, 2019); on the other hand, the technical specifications and best practices released by the EC for the European EHR Exchange Format are the baseline for any implementation. Enforcing obligations by applying international standards is also recommended by the eHealth Network (eHealth Network, 2019).

Additionally, in the cross-border exchange each controller should maintain the record of the activities carried out since the processing includes special categories of data (c).[39] In the interoperability context, data controllers could and should cooperate with the data protection authority established in their Member State (d). The cooperation between the authorities, which may be highly recommended in this cross-border context, could be achieved through the agency of the EDPB. Moreover, as mentioned in section "*Issues at organizational layer*," carrying out a DPIA (f) may be crucial for assessing the impact of this peculiar processing. Joint methodologies could be supported at EU level and open risks analysis tools could be shared among stakeholders. It may be suggested that the DPO designated by the controller (g) should have a deep knowledge of the data protection concerns at all the different layers. Finally, as previously specified, technical functions of the systems should be implemented for ensuring compliance with data subject's requests and the exercise of their rights.

Concluding Remarks

The heterogeneity of EHR systems and the lack of technical interoperability across the EU are mentioned frequently as the main problem for the use of these digital solutions and for the cross-border access to healthcare. With the implementation of the EC's Recommendation, European citizens could be empowered to access abroad their health data for a medical treatment or consulting. Nevertheless, in the absence of specific EU legislation, the progress to achieve interoperability remains upon the Member States and, actually, upon the market of EHRs. However, after the latest recommendations, the EU countries have to consider the cross-border interoperability of EHRs as a priority in the development of the national and regional EHR.

Interoperable systems implementation should comply with data protection provisions. The GDPR lays down the requirements that operators must comply with. According to the data protection by design and by default obligations, a higher level of protection for personal health data must also be guaranteed by design in the EHR systems. So, to improve the use and exchange of personal health data, not only must interoperability and access be compliant with the law, but also EHR systems should be designed ex ante to guarantee data protection rules. Therefore, a minimum set of EU standards could just be the starting point toward a productive interoperability. As the GDPR obligations are applicable in all Member States, a common EU strategy on DPbD measures for EHR systems could enhance the fair and complaint flow of personal health data across EU (and so, of patients and products). Moreover, this strategy could lead developers of EHRs to find clearer and well-defined rules to be followed during systems design.

In this field, further research may be required to analyze the recommended technical specifications and standards for the European EHR Exchange Format and their concrete implementation across EU, in order to investigate the extent to which they address data protection concerns and GDPR requirements.

Funding Statement. This work received no specific grant from any funding agency, commercial, or not-for-profit sectors.

Competing Interests. The author declares no competing interests exist.

Authorship Contributions. Conceptualization, G.B.; Formal analysis, G.B.; Investigation, G.B.; Methodology, G.B.; Writing-original draft, G.B.; Writing-review & editing, G.B.

Data Availability Statement. Data availability is not applicable to this article as no new data were created or analyzed in this study.

Notes

[1] European Commission (2018) *Commission Staff Working Document Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Enabling the Digital Transformation of Health and Care in the Digital Single Market.* Brussels: SWD, 126 final.

[2] European Commission (2018) C*ommunication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; Empowering Citizens and Building a Healthier Society.* Brussels: COM, 233 final.

[3] Article 29 Working Party (2007) *Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHRs).* Brussels: WP, 131 final.

[4] European Commission (2018) Synopsis Report. *Consultation: Transformation Health and Care in the Digital Single Market.* Luxembourg: Publication Office of the European Union.

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

[6] European Commission (2018) *Road-Map.* Brussels: Ref. Ares (2018) 5986687, 22.11.2018.

[7] European Commission (2019) *Commission Recommendation (EU) 2019/243 of February 6, 2019 on a European Electronic Health Record Exchange Format.* Brussels: COM, 800 final.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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.

[9] This work by no means includes the concerns related to the secondary use of nonpersonal health data (e.g., anonymized for scientific or research purposes).

[10] Expert Panel on effective ways of investing in Health (EXPH) (2019) *Assessing the Impact of Digital Transformation of Health Services.* Luxembourg: Publications Office of the European Union.

[11] See also the Health policies in the future EU budget (2021–2027). Available at https://ec.europa.eu/health/funding/future_health_budget_en.

[12] Council of the European Union (2009) Council conclusions on safe and efficient healthcare through ehealth. *2980th Employment, Social Policy, Health and Consumer Affairs Council meeting*, Dec 1, 2019. Brussels.

[13] European Commission (2004) *Communication on eHealth—Making Healthcare Better for European Citizens: An Action Plan for a European eHealth Area.* Brussels: COM, 356 final.

[14] European Commission (2017) *New European Interoperability Framework, Promoting Seamless Services and Data Flows for European Public Administrations.* Luxembourg: Publications Office of the European Union.

[15] The projects and studies funded by the EU. Available at https://ec.europa.eu/digital-single-market/en/news/ehealth-studies-overview.

[16] European Commission (2008) *Recommendation of July 2, 2008 on Cross-Border Interoperability of Electronic Health Record Systems.* Brussels: COM, 3282 final.

[17] Council of the European Union (2017) Council Conclusions on Health in the Digital Society; Making Progress in Data-Driven Innovation in the Field of Health. 2017/C 440/05.

[18] European Commission (2019) *Annex to the Commission Recommendation on a European Electronic Health Record Exchange Format.* Brussels: COM, 800 final.

[19] Article 5 GDPR.

[20] Data subject's right to require information (Articles 12–14 GDPR), to access (Article 15 GDPR), to rectification (Article 16 GDPR), to erasure (Article 17 GDPR), to restriction of processing (Article 18 GDPR), and to data portability (Article 20 GDPR).

[21] Articles 4 (15) and 9 (1) GDPR: "data concerning health" is a special category and means "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

[22] See Article 9 (2) (h) (i) GDPR.

[23] An exception could be the case of joint equips that collaborate cross-borders for a medical treatment.

[24] Article 35 GDPR.

[25] European Data Protection Board and European Data Protection Supervisor. (2019). *EDPB-EDPS Joint Opinion 1/2019 on the Processing of Patients' Data and the Role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI).* Brussels: European Data Protection Board and European Data Protection Supervisor.

[26] Regulation (EU) 2018/1725 of the European Parliament and of the Council of October 23, 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.

[27] In the Opinion[25] the authorities asked the EC to specify its duties as processor in a future "Implementing Act."

[28] See Article 6 and Article 9 (2) (a) (c) (g) (h) (i) GDPR.

[29] In 2014, a detailed examination (Milieu and Time.lex, 2014) showed that no country required patient consent for the cross-border access. However, in the Recommendation 18, the EC states that "any processing of health data must be based on the explicit consent of the citizen concerned or on any other lawful basis, pursuant to Articles 6 and 9" GDPR.

[30] Article 9 (2) (a) GDPR.
[31] See Articles 12–14 GDPR.
[32] See Article 15 GDPR.
[33] In this matter, it can be applied also the EU directive 2016/1148 on security of network and information systems (NIS Directive). EHRs could be identified as information systems that process and store digital health data. According to Annex II of the Directive, healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU[5] (i.e., "any natural or legal person or any other entity legally providing healthcare on the territory of a Member State") are listed as "types of entities for the purpose of point (4) of article 4" in the health sector and its sub-sector health care settings (including hospitals and private clinics). Therefore, providers of EHR systems are operators of essential services subjected to the additional requirements of NIS Directive and to its national transpositions.
[34] A number of researchers are proposing interesting technical models for minimizing data protection risk (Conley and Pocs, 2018) (Anjum et al., 2018). The eHealth Network established under article 14 of Directive 2011/24/EU5 has lately listed technical specifications, standards, and protocols based on the European Electronic Health Record Format (eHealth Network, 2019).
[35] See Article 25 GDPR.
[36] Article 83 GDPR.
[37] See Articles 24 (3), 25 (3), 32 (3) GDPR.
[38] According to Article 25 (1) GDPR, the criteria are: "the state-of-the-art, the costs of implementation, the nature, scope and purposes of the processing, the risks of varying likelihood and severity for rights posed by the processing."
[39] Article 30 (5) GDPR.

References

Abedjan Z Boujemaa N, **Campbell S**, **Casla P**, **Chatterjea S**, **Consoli S Costa-Soria C**, **Czech P**, **Despenic M**, **Garattini C**, **Hamelinck D**, **Heinrich A**, **Kraaij W**, **Kustra J**, **Lojo A**, **Sanchez MM**, **Mayer MA**, **Melideo M**, **Menasalvas E**, **Aarestrup FM**, **Artigot EN**, **Petkovic M**, **Recupero DR**, **Gonzalez AR**, **Kerremans GS**, **Roller R**, **Romao M**, **Ruping S**, **Sasaki F**, **Spek W**, **Stojanovic N**, **Thoms J**, **Vasiljevs A**, **Verachtert W and Wuyts R** (2019). Data science in healthcare: Benefits, challenges and opportunities. In *Data Science for Healthcare*. Springer: Cham, pp. 3–38.

Anjum A, **Choo K-KR**, **Khan A**, **Haroon A**, **Khan S**, **Khan SU**, **Ahmad N and Raza B** (2018) An efficient privacy mechanism for electronic health records. *Computers & Security*, *72*, 196–211.

Arak P and Wójcik A (2017) Transforming ehealth into a political and economic advantage. *Polityka Insight.*

Blobel B (2018) Interoperable EHR systems–challenges, standards and solutions. *European Journal for Biomedical Informatics 14* (2), 10–19.

Conley E and Pocs M (2018) GDPR compliance challenges for interoperable health information exchanges (HIEs) and trustworthy research environments (TREs). *European Journal of Biomedical Informatics 14*(3), 48–61.

EDPB (2019) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 1.0 for public consultation.

eHealth Network (2019) ehealth Network Guidelines to EU Member States and the European Commission on an interoperable ecosystem for digital health and investment programmes for a new/updated generation of digital infrastructure in Europe.

ENISA (2017) Handbook on Security of Personal Data Processing. Available at www.enisa.europa.eu.

Flaumenhaft Y and Ben-Assuli O (2018) Personal health records, global policy and regulation review. *Health Policy 122*(8), 815–826.

IEEE SA (2016) *Standards Glossary.* Piscataway, NJ: IEEE SA.

Kouroubalia A and Katehakis DG (2019) The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of Biomedical Informatics 94*, 103166.

Lupiáñez-Villanueva F, **Folkvord F and Faulí C** (2018) *Benchmarking Deployment of eHealth among General Practitioners*. Luxembourg: Publications Office of the European Union.

Milieu L and **Time.lex** (2014) *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Report.* Brussels: 201/65.

Romanou A (2018) The necessity of the implementation of privacy by design in sectors where data protection concerns arise. *Computer Law & Security Review 34*(1), 99–110.

Saripalle R, **Runyan C and Russell M** (2019) Using hl7 fhir to achieve interoperability in patient health record. *Journal of Biomedical Informatics 94*, 103188.

Soceanu A (2016) Managing the interoperability and privacy of e-health systems as an interdisciplinary challenge. *Systemics, Cybernetics and Informatics 14*(5), 42–47.

Van Langenhove P, **Decreus K**, **Rogala A**, **Olyslaegers T and Whitehouse D** (2013) eHealth European Interoperability Framework. Vision on eHealth EIF, a study prepared for the European Commission by the Deloitte team.

Cite this article: Bincoletto, G. 2020. Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union. *Data & Policy* 2: e3, 1–11, doi:10.1017/dap.2020.2