Data protection issues in cross-border interoperability of EHRs systems within the European Union

Giorgia Bincoletto

University of Bologna and University of Luxembourg
giorgia.bincoletto2@unibo.it

Abstract

This study investigates the data protection concerns arising in the context of the cross-border interoperability of Electronic Health Records (EHRs) systems in the European Union. The paper first introduces the policies on digital health and examines the related interoperability issues. Secondly, 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 GDPR to be taken into account when developing interoperable EHRs. According to the data protection by design and by default provision, EHRs systems should be designed *ex ante* to guarantee data protection rules.

Keywords— Digital health; EU policy; EHR; Interoperability; Data protection by design.

1 Introduction

Digital technologies have deeply transformed the provision of health care 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 Health Care 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. Secondly, the EC calls for improving the data quality for research purposes, disease prevention and for enabling personalised healthcare. In the end, the Commission claims that further action at EU level is crucial for developing digital tools for citizens' empowerment and person-centred 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) – i.e. 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 European Commission proposed to make some recommendations on how EHRs 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 authorised 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].

[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 (2018) 126 final.

[2] European Commission (2018). 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; empowering citizens and building a healthier society. Brussels: COM (2018) 233 final.

[3] Article 29 Working Party (2007). Working Document on the processing of personal data relating to health in electronic health records (EHR). Brussels: WP (2007) 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 9 March 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)

The cross-border interoperability and the secure access to EHRs 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 EHRs 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 EHRs systems demands the definition of clear legal rules. So, the study contributes to the ongoing debate by analysing 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 scrutinised. 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 2 will revolve around the "transformation of health and care" policy and the interoperability issue. Then, in Section 3 the last Recommendation of the European Commission is analysed. The paper will focus on the data protection concerns and will investigate the requirements settled by the GDPR to be taken into account in Section 4, giving particular attention to the data protection by design (hereinafter: DPbD) and by default obligations[9]. Conclusions are presented in Section 5.

2 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, personalised, effective and efficient healthcare and for reducing errors and length of hospitalisation[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 standardisation 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, 2016). Interoperability implies not only that information can be exchanged between many systems or services, but that 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, organisational and legal interoperability should be distinguished. Firstly, technical interoperability allows the exchange of data from system A to system B neutralising 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 organisational interoperability ensures that separated business processes are aligned[14]. Finally, legal interoperability concerns

2019/243 of 6 February 2019 on a European Electronic Health Record exchange format. Brussels: COM (2019) 800 final.

[8]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.

[9]This work by no means includes the concerns related to the secondary use of non-personal health data (e.g. anonymised 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). Retreive from: `https://ec.europa.eu/health/funding/future_health_budget_en`. Last Accessed on 5/12/2019.

[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. Brussels: 1.12.2009.

[13]European Commission (2004). Communication on eHealth - making healthcare better for European citizens: An action plan for a European eHealth Area. Brussels: COM (2004) 356 final.

[14]European Commission (2017). New European Interoperability Framework, Promoting seamless services and data flows for European public ad-

how to ensure that organisations 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 record 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 neighbouring and non-neighbouring Member States[16]. Healthcare interoperability covers, for examples, prescriptions for medications or investigations, examination reports, 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, organisational and legal levels, adding a political one (that is leveraging investments, 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 EHRs systems implementation was not available neither for the national nor for the EU frameworks. In 2017, during an online public consultation of the EC high importance was assigned to supporting interoperability with harmonised 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 delivered interoperable and open EHRs solutions[1]. As a reply, and in order to avoid proprietary solutions creating vendor lock-in, the EU Council invited the Member State 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 in place to achieve interoperability: (a) a thorough understanding of the operational environment; (b) the identification of interrelationships 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 analysed in the next Section.

3 The new Recommendation

The Recommendation of February 2019 follows all the EU efforts on the interoperability issues and aims at the creation of a European Electronic Health Record 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 EHRs 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: (i) the principles that should govern the access and the exchange of EHRs across borders; (ii) a set of common techni-

ministrations. Luxembourg: Publications Office of the European Union.

[15]The projects and studies funded by the EU at `https://ec.europa.eu/digital-single-market/en/news/ehealth-studies-overview`. Last Accessed on 5/12/2019.

[16]European Commission (2008). Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems. Brussels: COM (2008) 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.

cal specifications in certain health information domains (i.e. the baseline for the exchange format); (iii) 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 organisational measures to secure the EHRs 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 Electronic Health Record 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. Firstly, it could conceivably be hypothesised 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 a EU legislation will better harmonise the standards than the present soft-law approach. Nevertheless, high importance is assigned to privacy and data protection concerns. As Section 4 will investigate, data security and privacy are significant challenges for the interoperability of EHRs systems.

[18]European Commission (2019). Annex to the Commission Recommendation on a European Electronic Health Record exchange format. Brussels: COM (2019) 800 final.

4 The data protection concerns and the obligations settled by the GDPR

Surveys highlighted that privacy concerns are considered as deterrent from adopting e-health systems by legal practitioners (Lupiáñez-Villanueva et al., 2018). So, as mentioned above, the cross-border interoperability of EHRs is inevitably bound with data protection issues because of the processing of personal data. 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[19].

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. The GDPR lays down the conditions for 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 minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability[20]. Moreover, it provides many data subject's rights[21]. In the EHRs systems the data collected is mostly sensitive[22]. 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).

Within the cross-border interoperability context, the patient's data is firstly 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]. All of the different actors should comply with the data protection rules separately, but in the

[19]The points order reflects the order of the principles in the GDPR.

[20]Article 5 GDPR.

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

[22]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".

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

same way. This issue could be considered in the organisational interoperability level.

The "patient profile" in the EHR system is created in one national state, then it is exchanged. So, the further processing abroad should be lawful and the legal ground should be present as in the first processing[24]. The cross-border exchange and use of the EHR should be possible only if the legal ground is still lawful or another ground applies in the concrete case. However, as collected data is related to the health status of the data subject, the consent should be explicit[25]. Therefore, 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. Additionally, 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[26]. So, in the next Member State the information could be provided in the mother language of the subject, or another one well-known by him or her. As previously, this issue could be considered in the organisational interoperability layer.

Another fundamental concern that emerges in the interoperability context is the possible circumvention of the purpose limitation principle. No different use and cross-border exchange is allowed if the patient data is 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]. According to the data minimisation principle, the data in the EHR should be limited to what is necessary for the healthcare purpose and be adequate and relevant. This statement is still applicable for the interoperability scenario. Pseudonymisation techniques could achieve this goal (Abedjan et al., 2019).

Moreover, during the cross-border exchange, the patient's data should be accurate and kept up to date in all the interoperable EHRs 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[27], and one the other hand there are the accesses of the health professionals in another Member State. As regards the first situation, the patient has the right to access, to erasure, to rectification, to data portability and the right to know who accessed the EHR. Granting these rights means that the EHRs interoperable systems should have the functions to execute the patient's requests.

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 o 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 standards to prevent any unauthorised access[18]. For these concerns, and the next ones, the attention should be paid at technical interoperability layer.

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 Articles 32 of the GDPR, systems should be properly secure with measures to ensure a security level appropriate to the concrete risks[28]. The protection against unauthorised access or unlawful processing, accidental loss, disclosure, destruction or damage, identity theft or fraud, should be granted in each EHR system (Conley and Pocs, 2018). Auditing, archiving of the access and back-up mechanisms are common security measures for an interoperable EHR systems[18]. However, harmonised standards for their implementation are required.

In addition, the controllers should be responsible and demonstrate compliance (i.e. accountability principle). Documents on the cross-borders processing could be shared among the actors. 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[29]. Moreover, according to Article 25 of

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

[25] Article 9 (2) (a) GDPR.

[26] See Articles 12-14 GDPR.

[27] Article 15 GDPR.

[28] In this matter it can be applied also the EU directive 2016/1148 on security of network and information systems (NIS Directive).

[29] Article 35 GDPR.

the GDPR, EHRs technologies should integrate DPbD and by default technical and organisational 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[30]. To apply DPbD requirement a solution might be using an open and extendable architecture with privacy-by-design modelling and embedded risk analysis tools, in order to provide systematic protection for storage and interoperable exchange of health data (Abedjan et al., 2019).

By analysing the GDPR within the interoperability context, a number of obligations can be identified and summarised as follows: (a) the implementation of appropriate data protection safeguards (Article 24); (b) the implementation of the DPbD and by default technical and organisational 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) carrying out a data protection impact assessment (Article 35); (g) the designation of a data protection officer (Article 37) and (h) the compliance with data subject's requests (e.g. for the exercise of rights). Remarkably, these obligations are indirectly indicated in the list of principles released by the EC in the Recommendation described above[18].

5 Concluding remarks

The heterogeneity of EHR systems and the lack of technical interoperability across the EU is 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 EHRs 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 EHRs systems should be designed *ex ante* to guarantee data protection rules. Therefore, a minimum set of EU standards could just be the starting point towards a productive interoperability. As the GDPR obligations are applicable in all Member States, a common EU strategy on DPbD measures for EHRs 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 analyse the recommended technical specifications and standards for the European Electronic Health Record Exchange Format and their concrete implementation across EU, in order to investigate the extend to which they address data protection concerns and GDPR requirements.

[30] See Article 25 GDPR.

References

Abedjan, Z. et al. (2019). Data Science in Healthcare: Benefits, Challenges and Opportunities. In *Data Science for Healthcare*, pages 3–38. Springer.

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.

ENISA (2017). Handbook on security of personal data processing. www.enisa.europa.eu.

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

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

Lupiáñez-Villanueva, F. et al. (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.

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. et al. (2013). eHealth European Interoperability Framework. *Vision on eHealth EIF, a study prepared for the European Commission by the Deloitte team*, 1.