Kalpa Publications in Computing

Volume XXX, 2022, Pages 21–23

Proceedings of V XoveTIC Conference. XoveTIC 2022

Strategy for data Cybersecurity in European Health Data Ecosystem

Henrique Curado[1], Paulo Veloso Gomes[1], Marc Jacquinet[2], António Marques[1] and Javier Pereira[3]

[1] LabRP, Center for Rehabilitation Research, School of Health, Polytechnic of Porto, Portugal

[2] CEIO, Universidade do Algarve e CEMRI, Universidade Aberta, Portugal

[3] CITIC, Research Center of Information and Communication Technologies, Talionis Research Group, University of A Coruña, A Coruña, Spain

hct@ess.ipp.pt, pvg@ess.ipp.pt, marc.jacquinet@uab.pt, ajmarques@ess.ipp.pt, javier.pereira@udc.es

Abstract

This study aims to analyze the Strategy for Data Cybersecurity in the European Health Data Ecosystem, to be implemented in 2025. The document analysis was carried out to map the different proposals for a regulation of the European Parliament and of the Council, regarding the sharing of the Electronic Health Record in the European space, and the General Data Protection Regulation implemented in the European Union.

After an exhaustive documentary analysis, inconsistencies or flaws were detected that could compromise the rights of citizens enshrined in the General Data Protection Regulation.

1 Introduction

The creation of a European Health Data Area (EHDA) presupposes a joint analysis of conflicting interests, namely, the ease of access to information, whether for therapeutic or research purposes, but also, on the other hand, the greatest vulnerability inherent in the sharing of sensitive and highly valuable data over a network.

Two types of objectives emerge from the proposed regulation for the creation of the EHDA: access to health information for EU citizens outside their country for prescribing and purchasing medicines (primary use of data); sharing information for scientific research purposes, given its relevance to medical innovation as well as to the development of health policies and regulations (secondary use of data).

Notwithstanding the unquestionable advantages, given the possibility of sharing data online between health professionals from different countries, from the summary of the medical history, the result of tests and complementary means of diagnosis, as well as the respective prescription, the

success of the system presupposes greater vulnerability than if the data were contained in the universe of the country of residence of each citizen. Reason enough for the implementation of innovation, policy formulation and regulation to be accompanied by the European data strategy, of which health information security is important for two reasons. The creation of an EHDA, in the event of an attack, will make it impossible to consult a citizen's historical summary, the means of diagnosis and the prescription itself. As well, mass data capture means loss of privacy, associated with the possible misuse of this data. The sale of data to economic groups can leave many citizens vulnerable and exposed to economic interests, which may conflict with their citizenship rights, for example when they wish to take out simple health insurance associated with a housing loan or car loan.

It is important to understand the scope of "Communication from the Commission to the European Parliament and the Council - A European Health Data Space: harnessing the power of health data for people, patients and innovation 2022" in concerning of the introduction of requirements on data sharing between healthcare providers, mandatory requirements for interoperability, protection and privacy, self-certification of electronic health records covering interoperability and security.

Indeed, although it is also stated that "individuals will have greater control over their health data", it is nevertheless imposed, in certain circumstances, to share their data, which, once carried out, raises doubts about their knowledge and control of the access to that information. In fact, it follows from the EHDA that in certain circumstances, the public interest resulting from the use of the data prevails over the interests of data subjects to freely dispose of the data they hold. Wherea 57, Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Parliament and European Council, 2022).

2 Trust in European Health Data Space

It is important to evaluate questions from the dual perspective. In effect, the former must serve the latter and do so in a complete manner, i.e., seek to safeguard the security of highly sensitive personal information, in such a way that the citizen not only knows of the legitimate and illegitimate accesses to his personal data, but may, without a great deal of effort, set in motion the mechanisms capable of putting an end to that intrusion.

On the European Health Data Space Webpage, it is stated that "trust is a key enabler for the success of the European Health Data Space (EHDS)." As such, the EHDS will provide a trusted environment for secure access and processing of a wide range of health data, which is further based on the General Data Protection Regulation (GDPR Parliament and European Council, 2016), the proposed Data Governance Act (Data Act Parliament and European Council, 2020), the draft Data Act (Parliament and European Council, 2022), and the Network and Information Systems Directive (Directive (EU) 2016/1148). Two other important documents should be mentioned, the European Strategy for Data (European Commission, 2020) and the Proposal for a regulation - The European Health Data Space (Parliament and European Council, 2022).

Reading those documents, some doubts remain, as the Data Governance Act aims to be a specific piece of legislation in relation to the GDPR, as it points out when stating the difficulty of its uniform application. However, it does not bring clarity, nor solutions, to some of the issues that the GDPR has already raised, as it is not enough to state that the citizen has full control over their health information, as well as that secondary access (clinical research) will be done in a totally anonymous way.

If at the beginning of the reading of those documents we could ask ourselves, e.g., if the citizen learns that there has been an improper access to his health information from a third state, which procedural mechanism would be appropriate, that of his country or of the third state, or, unlikely, if there would be a European mechanism of an extrajudicial nature, but with identical effects, similar to the arbitration centers, we find that there is not.

The documents are sparse in terms of concerns regarding the procedures available to citizens in defense of their personal rights, which raises two types of questions. On the one hand, the instruments are those already existing in each State, as occurs, for example, with the Portuguese personal data protection law, (Lei n.º 58/2019, 08/08), establishing mechanisms for administrative and jurisdictional protection (CAP. VII). While it is true that the national supervisory body (the National Commission for Data Protection - CNPD) *has the legitimacy to intervene in legal proceedings in the event of violation of the provisions of the GDPR and domestic law, and must report to the Public Prosecutor's Office any criminal offenses of which it becomes aware, in the exercise of its functions and because of them, as well as carry out the necessary and urgent precautionary acts to ensure the means of proof*, the fact remains that most situations will not come to its attention. Either because they are not known about unofficially, or because the injured party, the citizen whose privacy is violated, cannot report it, as they will never know about it. A second concern is the difficulty of prosecuting the abusive use of personal data at the international level, to which the internal mechanisms are unable to respond.

3 Conclusion

It is important to understand that the protection of privacy, based on a system that merely refers to the GDPR, does not provide effective protection, bearing in mind the exchange of health information, which is highly sensitive, despite its unquestionable contribution to individual and collective health. As mentioned by (Curado, 2017), the protection of privacy in situations of international movement of personal data will appear practically unviable, since recourse to international jurisdictions - the Court of Justice of the European Union and the European Court of Human Rights - will have to be triggered on an individual basis, with undeniable difficulties for a citizen to sue another State.

References

Curado, H. (2017). Las bases de datos de adn y derechos fundamentales: la respuesta desde el derecho portugués. Em A. G. Domínguez, & S. Á. González, *Un nuevo reto para los derechos fundamentales: los datos genéticos* (pp. 163-187). Madrid: Dykinson S.L. ISBN:9788491483908.

Data Act Parliament and European Council. (25 de 11 de 2020). Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). *COM(2020) 767 final*. Brussels.

Directive (EU) 2016/1148. (19 de 07 de 2016). Parliament and European Council, concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union, L 194. ISSN: 1977-0774*, 30.

European Commission. (19 de 02 de 2020). A European strategy for data COM(2020) 66 final. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Brussels.

GDPR Parliament and European Council. (2016). Regulation (EU) 2016/679. General Data Protection Regulation. *Official Journal of the European Union*.

Lei n.º 58/2019. (08/08). Lei da Proteção de dados Pessoais. *Diário da República nº 151/2019*.

Parliament and European Council. (23 de 02 de 2022). Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). *COM(2022) 68 final*. Brussels.

Parliament and European Council. (03 de 05 de 2022). Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. *COM(2022) 197 final*. Strasbourg.