Building Continents of Knowledge in Oceans of Data: The Future of Co-Created eHealth
A. Ugon et al. (Eds.)

OpenEHR Based Systems and the General Data Protection Regulation (GDPR)

Mariana SOUSA[a,1], Duarte FERREIRA[a,b] Cátia SANTOS-PEREIRA[b] Gustavo BACELAR[a,c] Samuel FRADE[a,d] Olívia PESTANA[e] Ricardo CRUZ-CORREIA[a]

[a]*CINTESIS, Porto, Portugal*
[b]*HealthySystems, Portugal*
[c]*VirtualCare, Portugal,* [d]*Marand, Slovenia*
[e]*Faculty of Arts of the University of Porto, Portugal*

Abstract. The concerns about privacy and personal data protection resulted in reforms of the existing legislation in European Union (EU). The General Data Protection Regulation (GDPR) aims to reform the existing measures on the topic of personal data protection of the European Union citizens, with a strong input on the rights and freedoms of people and in the establishment of rules for the processing of personal data. OpenEHR is a standard that embodies many principles of interoperable and secure software for electronic health records. This work aims to understand to what extent the openEHR standard can be considered a solution for the requirements needed by GDPR. A list of requirements for a Hospital Information Systems (HIS) compliant with GDPR and an identification of openEHR specifications was made. The requirements were categorized and compared with the specifications. The requirements identified for the systems were matched with the openEHR specifications, which result in 16 requirements matched with openEHR. All the specifications identified matched at least one requirement. OpenEHR is a solution for the development of HIS that reinforce privacy and personal data protection, ensuring that they are contemplated in the system development. The institutions can secure that their Eletronic Health Record are compliant with GDPR while safeguarding the medical data quality and, as a result, the healthcare delivery.

Keywords. GDPR, openEHR, Hospital Information Systems, Data Protection, Requirements

Introduction

Healthcare activities strongly rely on information with focus on the medical record. Information Technology (IT) became a critical tool to support the needs of the health care institutions, being responsible for processing heath data. It's important to understand the IT's impact on personal data processing and, in particular, on data protection. Privacy needs to be considered during systems design and implementation. (1). GDPR is a regulation that concerns the processing of personal data of EU citizens. It provides a framework that guides the use of personal data in all kind of institutions, imposing rules and obligations regarding the privacy and protection of data. OpenEHR

[1] Corresponding Author: Ricardo Cruz-Correia, E-mail: rcorreia@med.up.pt.

presents a set of specifications for an interoperable EHR systems architecture based on a multi-level, single source modelling approach.(2) This work aims to understand to what extent openEHR standard addresses the requirements mandatory to GDPR.

1. Methods

We first identified the requirements for an HIS compliant with GDPR. The regulation was analysed and a total of 16 requirements that were identified as a specification or obligation of the institutions were considered (3). Secondly, we identified 8 specifications of openEHR based systems, through the analysis of "OpenEHR Architecture overview". Finally, we made a table matching the GDPR requirements and the openEHR specifications. We defined that one specification could match more than one requirement and a requirement could be matched by more than one specification. If the openEHR specification meets the requirement in a direct way, by simply using the openEHR architecture, then it was considered a match.

2. Results

2.1. Matching GDPR requirements with openEHR specifications

The specification Access Control - access list and Access Control - configurations were matched with the following requirements:

Integrity and confidentiality - the access list ensures the maintenance of patient's privacy by allowing access to the related users; the configurations set the individuals that can change the configurations of the access list, maintaining the integrity of the access.

Data subject access - it enables the possibility of accessing the data, which allows the possibility of getting a copy of the data. If the data subject is not present in the control list, he will not be allowed to access and to have a copy; the configurations allow the data subject to set who can access his data, allowing a copy to be made.

Data subject direct access - it enables the data subject access directly to its personal data. The EHR allows the data subject access only if he is identified on the access list; by defining a gatekeeper in the configurations, it allows the data subject to be identified as such and, therefore, access the data.

Data protection by default. By defining the individuals that can access the data, the possibility of improper access is limited. It also ensures access restriction and limitation to personal data, preventing unwanted processing; the configurations allow the access list to be defined for an EHR, ensuring the integrity of the access.

The specification Digital Signature matches the following requirements: *Integrity and confidentiality* - it assures the authentication, non-repudiation and integrity of the EHR, acting as an important security and integrity measure of the personal data and its processing. *Data protection by default* - digital signature ensures the access and availability of information, acting as a security measure.

Table 1. Matches found between the GDPR requirements (1st column) and openEHR specifications (1st line)

	Access Control-*access list*	Access Control-*configurations*	Digital Signature	Versioning	Separation EHR-demographic	Service Model	Audit Trail	Two-level Modelling
Data minimization					✓			
Limitation of personal data storage					✓			
Integrity and confidentiality	✓	✓	✓	✓			✓	
Verification of data subjetc's identity					✓			
Data subject access	✓	✓						✓
Personal data processing confirmation				✓			✓	
Data subject direct access	✓	✓				✓		
Portability of personal data								✓
Portability personal data between controllers								✓
Interoperability of formats and systems						✓		✓
Data protection by design					✓			
Data protection by default	✓	✓	✓		✓			
Records of the processing of personal data							✓	
Availability of records of the processing of personal data							✓	
Records of data breaches							✓	
Transfers of personal data to third parties								✓
Total of matches	**4**	**4**	**2**	**2**	**5**	**2**	**5**	**5**

The specification Versioning ensures the indelibility of the EHR preventing any information from being deleted. It matches with the following requirements: *Integrity and confidentiality* - the creation of new EHR versions is an important measure against the loss, destruction or accidental arm of the EHR data, guaranteeing trustworthy and reliable information in all moments of processing. *Personal data processing confirmation* - through records versioning, it's possible to identify the user that made the changes, the date and time and the justification for the action, allowing the confirmation to the data subjects of any processing occurring.

The specification Separation of demographic information and EHR matches the following requirements: *Data minimization* - it allows the limitation of data to the purpose of processing by minimizing the use of the demographic data. *Limitation of personal data storage* - the identity of the data subject is automatically preserved when the clinical and demographic information are separated. In that way, while the clinical data is stored for treatment, the demographic data is connected to the EHR through an external identifier. *Data protection by design* - it allows the pseudonymization of the data subject by separating the EHR from the identifiable demographic information, only relating them by an external identifier. *Data protection by default* - on the moment of the medical care, it only considers the health personal data, safeguarding the demographic information.

The Service Model matched the following requirements: *Data subject direct access* - the service model, through the Virtual EHR API and EHR Service, creates a view that allows the consultation of the EHR by the data subject. *Interoperability of formats and systems* - it allows creation of different interfaces using the same data in different systems around the institution. When the views that allow the consultation of the EHR are settled, the record keeps its singleness and structure, maintaining the interoperability. The specification audit trail matches the following requirements: *Integrity and confidentiality* - it allows the record of access logs, ensuring the integrity of the data. *Personal data processing confirmation* - considering the audit trail's traceability, it is possible to know if there is any action being performed on the data subject's EHR, allowing the confirmation of data processing. *Records of the processing of personal data* - the audit trail keeps a record of all the information related to the actions performed in the EHR. *Availability of records of the processing of personal*

data- through its traceability, the audit trail allows the creation of a record of personal data processing that can become available to the data authorities. *Records of data breaches* - it provides a record of the data breaches that occurred by keeping a record of non-authorized data and undue actions.

The specification Two-level Modelling matches the following requirements: *data subject access* - the archetype modelling allows data to be export and made available to the data subject. *Personal data portability* - it ensures the ability of extracting the required data in a structured and automatic format. *Personal data portability between controllers* - any developed system that uses openEHR architecture, even with different vendors, can support the same data (modelled as archetypes and templates), ensuring the portability between vendors. *Interoperability of formats and systems* - the implementation of the Reference Model on the software level is common to the EHR, while the archetype and template modelling allows the semantic interoperability of the data and, therefore, the systems. *Transfers of personal data to third parties* - it allows the transfer of data through portability and interoperability (associated to them due to the modelling of the archetypes and templates of the reference model).

2.2. GDPR Requirements not met by openEHR specifications

This section presents the GDPR requirements that were not matched by the openEHR specifications:

Regarding the requirements related to the principles of processing, the specification didn't match the requirements: *Limitation of personal data processing*, *Personal data accuracy*, *Storage limitation*, *Accountability* and *Demonstration of accountability*. The specifications also didn't match the requirements related to consent: *Explicit consent*, *Record of consent*, *Data subjects consent withdrawal*, *Characteristics of consent* and *Lawfulness of processing after consent's withdrawal*. Regarding requirements related to legitimate interest, the following requirements were not matched: *Legitimate interest of processing*, *Legitimate interest information*, *Data subjects objection to legitimate interest*. Some requirements related to data subjects were also not matched: *Information provided to the data subject*, *Means to provide information to data subjects*, *Deadline to answer data subjects request*, *Format for data subject's request answer*, *Data subject's notification of new processing*, *Answer form for data subject's request*, *Data subjects access to processing information*, *Response data subject's request*, *Data subjects objection to data processing* and *Personal data erasure*. Regarding the requirements related to privacy notices, the specifications didn't match: *Privacy notices*, *Moment of privacy notification* and *Deadline of privacy notification*. Some requirements related to the limitation of processing were also not matched: *Limitation of personal data processing at data subjects request*, *Limitation of processing* and *Notification of processing limitation cancellation*. The specifications didn't match some requirements related to data breaches such as: *Development of data breach notification procedures*, *Records of data breaches*, *Data breach description* and *Deadline for data breach notification*.

Regarding the requirements related to DPIA, the specification didn't meet: *DPIA records preservation* and *DPIA consultation*. Other requirements that were not met by specifications were: *Communication with other entities*, *Record of personal data protection policies*, *Format of records of processing activities*, *DPO involvement*, *Compliance with codes of conduct*, *Compliance with certification processes* and *Personal data transfers assurance*.

3. Discussion

OpenEHR acts mainly on requirements that either shape the functional layer of the system or relates to data traceability, integrity and confidentiality. Data protection by design, portability and interoperability are ensured by openEHR's architecture, due to the two level modelling and separation of clinical and demographic data. Personal data integrity and confidentiality are mainly answered by the access control, versioning and audit trail specifications. Still, openEHR is a valuable tool for the fulfilment of the requirements that are not directly matched. It should be noted that some of the GDPR requirements, namely the ones related to the organizational processes, hardly could be met by any EHR specification standard. However, it is important to note that the organizational reforms that must be conducted require actions at the level of their organizational processes and services, but also specifically at the level of their systems.

We propose the implementation of openEHR based systems to enforce the fulfilment of GDPR requirements. OpenEHR is a promising approach to the development of HIS compliant with GDPR, serving as an important support for solutions focused on the privacy and data protection by design. It provides an integrated environment, focused on the provision of health care and access to quality information but ensures the privacy and protection of personal data.

Acknowledgement

The authors would like to acknowledge the project NanoSTIMA(NORTE-01-0145-FEDER-000016), which is financed by the North Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, and through the European Regional Development Fund (ERDF).

References

[1] Cavoukian A, Prosch M. Privacy by ReDesign: Building a better legacy. Inf Priv Comm Ontario. 2011;(May).

[2] Beale T, Heard S. openEHR - Architecture Overview. OpenEHR Found [Internet]. 2008;1–79. Available from: http://www.openehr.org/releases/1.0.2/architecture/overview.pdf

[3] The European Parliament, The European Council. General Data Protection Regulation. Off J Eur Union. 2016;2014(March 2014):20–30.

[4] Bacelar-Silva GM, Cesar H, Braga P, Guimaraes R. OpenEHR-based pervasive health information system for primary care: First Brazilian experience for public care. Proc 26th IEEE Int Symp Comput Med Syst U6 - 2013;572–873. Available from: http://uvic.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2BQSDFPM0xMMkk2SzNIS0mxSEoGnYCXYm6RZJFokmRunIKydQypNHcTYmBKzRNlUHFzDXH20AVddhJfADlzId4A3JoxM7EwTE1NNE5ONhBjYAH2j1MBzswbfQ

[5] Sociedade Brasileira de Informática em Saúde. Manual de Certificação para Sistemas de Registro Eletrônico em Saúde. Ed Marcelo Lúcio da Silva [Internet]. 2013;91. Available from: http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2013_v4-1.pdf

[6] Yamamoto R. Large-scale health information database and privacy protection. Japan Med Assoc J [Internet]. 2016;59(2–3):91–109. Available from: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85013421213&partnerID=40&md5=c88c927d6c1951bbf7176acc1a77fb93