The Importance of Health Informatics in Public Health during a Pandemic
J. Mantas et al. (Eds.)

doi:10.3233/SHTI200490

Legal Challenges for IT Service Providers in Pharmacogenomics

Lea MEIER [a,1], Kevin TIPPENHAUER [a] and Murat SARIYAR [a]
[a] *Institute for Medical Informatics I4MI, Bern University of Applied Sciences, Switzerland*

Abstract. IT providers offering services based on genetic data face serious challenges in managing health data in compliance with the General Data Protection Regulation (GDPR). Based on a literature research and our experiences, an overview of GDPR compliant processing of sensitive data is given. The GDPR requirements for processing sensitive data were specified for a use case concerning a service provider of a pharmacogenomic decision support system. Start-ups who want to enter into the health market also have to comply with the Medical Device Regulation (MDR). The associated efforts for legal compliance constitute an impediment for many start-ups. We created a comprehensive overview, which aligned the requirements of the GDPR with the life-cycle of a medical device. This overview shall help start-ups to grasp and overcome the regulatory hurdles faster.

Keywords. general data protection regulation, GDPR, data management, sensitive data, genetic data

1. Introduction

Pharmacogenomics (PGx) deals with genetic effects on the metabolic pathways of drugs [1]. Even though, clear targets are defined in guidelines [2], there is a lack of PGx testing, especially due to paucity of knowledge and implementation know-how. This explains the existence of IT service providers in this domain, offering, for example, workflows for PGx clinical decision support. However, such providers are facing serious challenges with respect to health data management, which can lead to sub-optimal service delivery.

Here, we describe challenges posed by the General Data Protection Regulation (GDPR) with the aim to comprehensively guide IT providers offering services based on sensitive and in particular genetic/genomics data. Especially, GDPR compliant storage and transfer of sensitive data are central issues that will be addressed. In addition to that, we will also discuss implications of the Medical Device Regulation (MDR) and ways to integrate its requirements into an overall perspective.

2. Methods

Information on the GDPR and its references to genetic data was obtained with a PubMed research using the MeSH terms (GDPR[Title/Abstract]) AND (genomic[Title/Abstract]

[1] Corresponding Author, Lea Meier, Bern University of Applied Sciences, Quellgasse 21, 2502 Biel/Bienne, Switzerland; E-mail: lea.meier@bfh.ch.

OR genetic[Title/Abstract] OR sensitive[Title/Abstract]). The resulting articles were analyzed and categorized according to their relevance. We relied on PubMed rather than legal databases as our focus was on practical approaches to establish conformance with the GDPR. The analysis was enriched by considering additional challenges implied by the MDR and our own experiences at the intersection between research and the market.

3. Results

3.1. GDPR Compliant Processing of Sensitive Data

Our PubMed research led to 17 articles, including four relevant articles for our purpose to provide some guidance for the practice [3–6]. Sariyar et al. [7] discuss GDPR related issues around different types of genetic data. They emphasize that the GDPR is demanding higher protection and stricter requirements for genetic data than for other sorts of personal data, as genetic data may contain sensitive information about the data subject and their blood relatives [8]. However, there are no additional data protection implications related to genetic data compared to other forms of sensitive data such as data concerning health, sexuality or sexual orientation.

The GDPR also defines fundamental rights of the data subject (defined as 'identified or identifiable natural person' (Art. 4) from which data is being collected, held or processed). The controller, defined as 'natural or legal person (...) which (...) determines the purposes and means of the processing of personal data' (Art. 4), is obliged to provide information such as the purposes of the processing for which the personal data are intended as well as the legal basis for the processing (Art. 13 (1) lit c). Moreover, the controller is responsible for the implementation of appropriate technical and organizational measures to ensure data processing according to the regulation (Art. 24 (1)). Organizational measures are, for example, the provision of explicit consent forms to the users, the assignment of roles for access control and the carrying out of a Data Protection Impact Assessment (DPIA). The technical measures include implementation such as authentication (Recital 57) and access control (Recital 39), encryption (Recital 83), pseudonymization (Recital 78) etc. The stored data must be provided in a structured, commonly used and machine-readable format (Art. 20 (1)). As the data subject has the right to rectification (Art. 16), to erasure (Art. 17 (1)) and/or to restriction of processing (Art. 18 (1)) the data, the data controller must be able to carry out these tasks.

Besides the data controller, the GDPR also defines the role of a data processor, which processes personal data on behalf of the controller (Art. 4). Processing by a processor is governed by a contract or other legal act that is binding on the processor with regard to the controller (Art. 28 (3)). From the GDPR perspective, the data processor is primarily responsible for applying technical measures described above. In addition to data controller and data processor, further roles such as data protection officer have to be assigned as well under certain conditions (Art. 37 (1)).

3.2. Scenario: PGx Service in an B2B Environment

In the following, we concretize how the regulatory requirements can be fulfilled based on the use case of an PGx CDSS service provided for health professionals. Four roles have to be differentiated in such a setting:

1. Patient (Data subject): the person whose personal data is being collected.
2. Health Organization (Data controller): a laboratory or hospital performing gene sequencing & analysis and storing the corresponding data.
3. Health Professional (Data processor): a physician or other professionals working in a health organization.
4. Service provider (Data processor): a company offering the PGx service.

Figure 1 shows the central processes: 1) The patient gives his explicit consent by signing the corresponding form provided by the health organization, 2) his blood sample is taken by the health professional and 3) analyzed & stored by the health organization. 4) The related pseudonymized data is transmitted to the service provider 5), where it is stored. 6) During drug prescription, the drug information and the present medication of a patient together with its pseudonym is sent to the software provider, which infers PGx information. 7) This information is provided to the physician in order to ensure 8) a PGx safe drug therapy. Central tasks of the health organization are pseudonymization prior to transmission to the software provider, assigning roles, access control, and carrying out an DPIA. The software provider is responsible for fulfilling further requirements of the GDPR, e.g. providing the functionality for erasure (Art. 17 (1)), provide data in machine-readable format (Art. 20 (1)) etc.

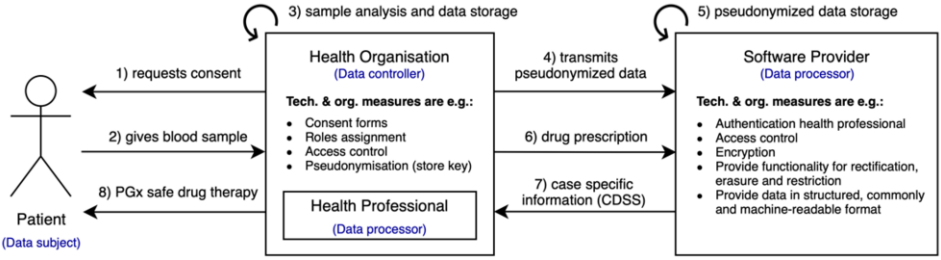

Figure 1. Processes in the PGx service scenario, listing some technical and organizational measures for the data controller and data processor.

3.3. Considering the MDR for an Overall Perspective

Processing of genetic data for research purposes is mainly regulated by the GDPR. However, companies operating in the health sector need also to be compliant with the MDR and acquire a corresponding medical device certification. The associated efforts constitute one central reason why many start-ups shy away from entering into the market and prolong their time within the research environment. With the MDR, further requirements, such as a comprehensive quality management system (QMS) according to ISO 13485, have to be met. Table 1 summarizes the main regulatory requirements that need to be considered by a health IT service provider in each phase of its product cycle, from the product idea to post-market surveillance (PMS).

Table 1. Actions to fulfill GDPR and MDR requirements along the product life-cycle.

	MDR	GDPR
Idea	Define intended purpose. Classify product (MDR Annex VIII). Implement QMS (ISO 13485).	Identify collected data and requirements.
Design	Consider risk management measures (ISO 14971).	Consider security, privacy and compliance requirements.
Development	Develop the product and document the development process (MDR Annex II).	Add supporting tools (Consent tracking, access control etc.).
Audit	Proof the conformity with the regulations. If necessary, audit with notified body.	Data privacy certification (voluntary, see Art. 42 (3)).
Release	UDI registration (MDR Art. 29) and CE marking (MDR Art. 20).	-
PMS	Surveillance and monitoring (MDR Art. 83 seq.).	Ensure data security, consent tracking etc.

4. Discussion/Conclusions

The main goal of the GDPR is to enhance effectiveness and harmonization of data protection in the EU; however, deviations from it are existent in several countries. In Switzerland, for example, the data subjects' rights are different and not defined in the corresponding Federal Act of Data Protection, but regulated by other regulations within the Swiss legal system, e.g. the Federal Act on Human Genetic Testing HGTA (abbreviated as GUMG in German). It is important to take such deviations into consideration, when providing services throughout Europe. For the MDR, no such deviations are to be expected. However, for countries like Switzerland an authorized representative has to be established within one of the EU 27 member states.

Acknowledgements

This research was supported by Swiss universities and Gebert Rüf Stiftung through the program 'BREF – First Ventures'.

References

[1] Roden DM, et. al., Pharmacogenomics: The genetics of variable drug responses. Circulation 2011;123: 1661–1670. doi:10.1161/CIRCULATIONAHA.109.914820.
[2] Wang L, McLeod HL, Weinshilboum RM. Genomics and drug response. N. Engl. J. Med. 2011;364: 1144–1153. doi:10.1056/NEJMra1010600.
[3] Townend D, Conclusion: harmonisation in genomic and health data sharing for research: an impossible dream?, Hum. Genet. 2018;137: 657–664. doi:10.1007/s00439-018-1924-x.
[4] Shabani M, Borry P, Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. Eur. J. Hum. Genet. 2018;26: 149–156.
[5] Phillips M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). Hum. Genet. 2018;137: 575–582. doi:10.1007/s00439-018-1919-7.
[6] Molnár-Gábor F, Korbel JO, Genomic data sharing in Europe is stumbling—Could a code of conduct prevent its fall?, EMBO Mol. Med. 2020;12: doi:10.15252/emmm.201911421.
[7] Sariyar M, Suhr S, Schlünder I. How Sensitive Is Genetic Data?, Biopreservation Biobanking 2017;15: 494–501. doi:10.1089/bio.2017.0033.
[8] de Paor A. Regulating genetic information--exploring the options in legal theory. Eur. J. Health Law 2014;1: 425–453. doi:10.1163/15718093-12341335.