PEARLS AND PITFALLS OF DATA PROTECTION IN HEALTH CARE

An overview of the GDPR's impact on hospitals and health care professionals.

BY CÉCILE E. VAN DER HEIJDEN, LLM

In May 2018, the General Data Protection Regulation (GDPR) became applicable in the European Economic Area (EEA; consisting of EU member states, Norway, Iceland, and Lichtenstein). Its impact has been felt worldwide, including in the health care sector. This article provides an overview of several important aspects of the GDPR that affect health care professionals (HCPs).

The GDPR has increased the attention to data subject autonomy and compliant data handling. *Data subjects*, as noted in article 4(1) of the GDPR, are the identified or identifiable persons to whom the personal data relate. The GDPR increased the autonomy of data subjects by creating several data subject rights, such as the right to request deletion of personal data (see *What Is Data Processing?*), and it introduced obligations for the parties responsible for the processing of personal data. For example, the GDPR requires these parties to comply with data processing principles such as purposes limitation, data minimization, implementing a certain level of security, and assessing the impact and risks of specific processing activities (articles 5, 32, and 35).

Although several GDPR requirements already existed under national sectoral or data protection legislation in many European countries, this legislation introduced more stringent data processing rules on a European (harmonized) level. Nevertheless, national deviations from the GDPR are permissible in relation to genetic data, personal data concerning health, and biometric data, as found in article 9(4). This has led to differences in national legislation affecting the processing of personal data for health care and research purposes in particular.

CONTROLLERS AND PROCESSORS

The GDPR clearly defines two roles—the *controller* and the *processor*.

The controller. This is the party that determines the what, why, and how of the processing. In legalese, the controller determines the means and purposes of the processing, as stipulated in article 4(7).

The processor. This party only processes the personal data on behalf and under the instruction of a controller, as covered in article 4(8) and 28(3)(a). Most obligations under the GDPR are imposed on controllers.

The relationship between controllers and processors. The GDPR has increased awareness of data handling practices, as evidenced by renewed attention to relationships with service providers, including software providers and the distributors of medical devices. In practice, the focus is often on the relationship between controllers and processors, which is formalized in a data processing agreement, as specified in article 28. Less attention seems to be given to other forms of external and internal collaboration.

A hospital in the EEA typically qualifies as a controller and thus must comply with the GDPR. In general, employees process personal data on behalf of their employer and do not individually classify as a party under the GDPR. If, however, a hospital consists of several legal entities or if the physicians jointly operate their practices as separate legal entities, collaborations often take the form of so-called *joint controller relationships* because the various parties jointly determine the means and purposes of the processing. The GDPR requires joint controllers to enter a joint controller arrangement in which their respective obligations under the GDPR are defined (article 26).

Service providers often act as processors, but this is not a given. If a service provider determines the means and purposes of the processing, that service provider qualifies as a controller. Examples include a

WHAT IS DATA PROCESSING?

Processing concerns any operation or set of operations that is performed on personal data or sets of personal data, per article 4(2) of the General Data Protection Regulation.

manufacturer of medical devices that determines the categories of personal data processed by analytical software (software as a service) and a clinical trial where an HCP collaborates with an external sponsor and participates in the drafting of the study protocol.[1]

LEGAL BASIS AND EXCEPTIONS

The processing of personal data under the GDPR requires a *legal basis*. The GDPR recognizes six legal bases, of which one is consent. Processing of personal data from special categories, including health and genetics, ethnicity, religious affiliation, and sex life/sexual orientation, is prohibited unless one of the exceptions listed in the GDPR applies. In general, exceptions are granted if the processing of such personal data is necessary for the provision of treatment. Details are available in articles 6 and 9.

A thorough assessment of the legal basis and exceptions for treatment purposes is common practice at hospitals. Consideration, however, is also required for other processing activities such as in collaborations with manufacturers of medical devices where the data will be processed to assess the safety and improvement of the devices under the upcoming Medical Devices Regulation (Regulation 2017/745/EU, article 83).

CLINICAL RESEARCH

Both the applicable legal basis and the classification of collaboration must be considered when conducting clinical research. The EU member states take different stances on the legal basis and exceptions that are applicable to the processing of personal data in the context of a clinical trial. Several EU member states and the joint supervisory authorities maintain that consent should not be used as a legal basis for the processing of personal data in the context of clinical research and that consent therefore cannot truly be freely given. Other member states such as the Netherlands require explicit data subject consent for the processing of personal data in a research context (article 24 of the Dutch GDPR implementation Act).[2] National rules on the legal basis for the processing notwithstanding, consent should be obtained for the participation of a person in a clinical trial in all cases, as required by the Declaration of Helsinki, the Clinical Trial Directive (Directive 2001/83/EC), Medical Devices Regulation (Regulation 2017/745/EU), and various national state laws.

To comply with the GDPR, all processing of personal data is, in principle, limited by the purpose communicated to the data subject (purpose limitation). A separate legal basis for the processing is required for each purpose. Clinical research is never conducted solely for the sake of conducting research; it has additional purposes such as obtaining market access or the publication of results. These additional purposes must be subject to a legal basis and exception if the study results still qualify as personal data under the GDPR. This should be considered before patient enrollment. (Editor's note: For more on the topic of the use of patient data for clinical research, see "Patient Data Collection and Informed Consent," pg 30.)

OTHER AREAS OF IMPACT FOR HCPS

Pseudonymization. Before the GDPR became applicable, key coded data were often considered anonymous if the recipient was not in possession of the identification key. The GDPR introduced the concept of *pseudonymized data*—personal data that can only indirectly identify the data subject by combining a data set with a secondary data set. Now that a party does not have access to the key, the data involved no longer qualify as anonymous. In general, they qualify only as pseudonymized. If personal data are pseudonymized, the GDPR applies in full.

Transfers. International research collaborations are often subject to the GDPR's transfer restrictions, which state that providing personal data (including access to data) that are subject to the GDPR to a recipient established outside the EEA is only allowed under a transfer measure. All permitted transfer measures are listed in articles 45 through 49 of the GDPR. This includes, for example, situations in which physicians consult colleagues outside of the EEA.

HCPs should be aware that a recent decision by the European Court of Justice raised serious concerns about the feasibility of many transfers.[3] Currently, there is a lack of clarity about the use of the most common transfer measure, and a transfer measure covering only transfers to the United States (EU-US Privacy Shield) has been declared invalid. These developments have serious implications for transfers of personal data, including in relation to the use of non-EEA service providers and conduct of clinical trials. More information on this subject is available at bit.ly/vanderheijden1020.[4]

CONCLUSION

The GDPR neither offers nor allows a one-size-fits-all approach to data protection. Nevertheless, adequate consideration of this legislation to ensure compliance increases patients' (ie, data subjects') trust in how their sensitive data are being handled by HCPs and other involved parties. ■

1. European Data Protection Board. Guidelines 07/2020 on the concepts of controller and processor in the GDPR (version for public consultation). Adopted September 2, 2020. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf
2. European Data Protection Board. Opinion 3/2019 concerning the questions and answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b). Adopted January 23, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf
3. Decision of the European Court of Justice, 16 July 2020, C-311-18, ECLI:EU:C:2020:559.
4. Vollebregt ER, van der Heijden CE. The EU Court's Schrems II judgement – urgent revisiting of international personal data transfer mechanisms required. Accessed September 29, 2020. https://medicaldeviceslegal.com/2020/07/23/the-eu-courts-schrems-ii-judgement-urgent-revisiting-of-international-personal-data-transfer-mechanisms-required

CÉCILE E. VAN DER HEIJDEN, LLM
- Attorney at Law, Axon Lawyers, Amsterdam, Netherlands
- cecile.vanderheijden@axonlawyers.com
- Financial disclosure: None