COSMOS
Navigate the Compliance Universe

Compliance Today - October 2018
GDPR compliance: Considerations for U.S. healthcare organizations

by Amy Joseph and Krietta Bowens Jones

Amy Joseph (ajoseph@health-law.com) is a Senior Counsel in the Boston office of Hooper, Lundy & Bookman PC. **Krietta Bowens Jones** (krietta_jones@dfci.harvard.edu) is Associate General Counsel at Dana-Farber Cancer Institute in Boston.

On May 25, 2018, the General Data Protection Regulation (GDPR),[1] a new data privacy law applicable to the European Union (EU) and countries in the European Economic Area (EEA), took effect, building upon and enhancing prior data protection requirements. The GDPR applies to the 28 member states of the EU as well as Liechtenstein, Iceland, and Norway, which are part of the European Economic Area. The United Kingdom has also implemented GDPR despite its planned exit from the EU. (For purposes of this article, the defined term "EU" is also intended to include the EEA for ease of reference.)

Specifically, the law regulates the processing of personal data of individuals in the EU, regardless of their citizenship status. "Personal data" is defined broadly as any information that can be used to identify a natural person.[2] The GDPR has extraterritorial reach and applies not only to organizations established in the EU, but also, under certain circumstances, to organizations established in the U.S. that process personal data of individuals in the EU. The public policy rationale behind the GDPR's expansive scope is the desire to balance the business purposes that necessitate the flow of information to and from countries outside of the EU with individuals' rights to privacy and control over their personal data.

In the months leading up to the effective date and immediately after, the GDPR received a flurry of media attention as certain U.S. organizations began rolling out GDPR-specific compliance measures (or, in some cases, opting to make services unavailable to individuals in the EU so as to avoid the GDPR's reach). The news primarily revolved around the impact on social media service providers and other technology companies that offer products or services internationally; however, the GDPR also has the potential to apply to some U.S. healthcare organizations, given the seemingly broad applicability test. For example, engaging in certain clinical research activities or offering medical tourism programs to EU residents could subject a U.S. healthcare organization to the GDPR's jurisdictional scope.

This article provides a high-level summary of the key questions and concepts for a U.S. healthcare organization to consider in order to determine if the organization is subject to the GDPR, and if so, what measures can be taken to ensure compliance with the new law.

Is my organization subject to the GDPR?

The GDPR applies to the processing of personal data of individuals in the EU by "controllers" or "processors" not established in the EU. "Processing" is defined to mean any operation performed on personal data (e.g., collection, use, disclosure, storage)[3] where the processing relates to:

> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring

> of their behaviour as far as their behaviour takes place within the Union.[4]

Given the broad scope of this language, the GDPR could apply to healthcare organizations in the United States in a number of ways.

A "controller" is a person or entity that determines the purposes and means of processing personal data. The concept is similar in some respects to a "covered entity" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A "processor" is a person or entity that processes personal data on behalf of the controller, similar in some respects to the concept of a "business associate" under HIPAA. Although controllers are mainly responsible for compliance with applicable data protection rules, the GDPR also imposes certain obligations on processors (e.g., security safeguards, recordkeeping requirements). A US healthcare organization could be a controller or a processor, or both, depending on the nature of its activities and relationships with other entities in the EU.

The following questions should be asked to determine if the GDPR applies to an organization's operations:

- Does the organization offer goods or services to individuals in the EU? For example, do marketing materials mention EU individuals (e.g., in testimonials) or EU currency in pricing information?
- Does the organization otherwise seek out patients from the EU for treatment purposes or to participate in research studies?
- Does the organization monitor the behavior of individuals in the EU? For example, does the organization offer telemedicine services to EU residents?
- In the research setting, does the organization conduct research at physical locations in the EU? Does the organization continue to monitor individuals in the EU following research conducted in the U.S.?