Does GDPR Regulate Clinical Care Delivery by US Health Care Providers?

Article By:

Bernadette M. Broccolo

Daniel F. Gottlieb

Summary

The General Data Protection Regulation establishes protections for the privacy and security of personal data about individuals in the European Economic Area countries, and potentially affects the medical tourism programs and other clinical activities of health care providers in the United States.

In Depth

The General Data Protection Regulation (GDPR) has important implications for the operations and privacy practices of US health care providers’ medical tourism programs and other international clinical activities that involve the use of personal data (Personal Data) about individuals located in the European Union (EU) and other European Economic Area (EEA) countries. GDPR, which establishes protections for the privacy and security of Personal Data, becomes effective on May 25, 2018, and EU data protection authorities have stated there will not be a compliance grace period.

The EEA countries include the EU member states, Norway, Iceland and Liechtenstein. In addition, other countries, such as Switzerland, have adopted or are expected to adopt privacy regimes similar to GDPR during 2018. For more information about implementation of GDPR compliance, please see our recent publications: “The General Data Protection Regulation: Key Requirements and Compliance Steps for 2018”; and “Does GDPR Regulate My Research Studies in the United States?”

What is GDPR?

GDPR regulates the collection, use, disclosure or other “processing” of Personal Data by controllers and processors.

Controllers

A “controller” is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. US
health care providers and payers that are “covered entities” under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) typically act as controllers when performing their core treatment and payment functions. For example, a health care provider that collects Personal Data from an individual located in the EU to provide treatment to the individual would typically be a controller.

**Processors**

A “processor” is a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller. A processor performs activities similar to a business associate under HIPAA. For example, an entity in the United States that enters into a service agreement that involves the analysis or other processing of Personal Data about individuals in the EU would be a processor.

The GDPR:

- Establishes the circumstances under which it is lawful to process Personal Data, including when a health care provider collects or otherwise uses Personal Data about individuals in the EU to recruit them to be a patient in the United States;

- Establishes certain rights of individuals in the EU, including rights of access, amendment (called “rectification” under GDPR) and restriction, which are similar to patients’ rights of access, amendment and additional restrictions under the HIPAA Privacy Rule;

- Requires Personal Data controllers and processors to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk to Personal Data, which are similar to covered entities’ obligations to secure protected health information under HIPAA Privacy Rule’s reasonable safeguards standard and the HIPAA Security Rule; and

- Requires notification to data protection authorities and affected individuals following the discovery of a “personal data breach,” which is breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**What data is “Personal Data” protected by GDPR?**

Analogous to HIPAA, which only permits the use of disclosure of protected health information if permitted or required by the Privacy Rule, GDPR requires controllers and processors to have a lawful basis for the processing any Personal Data about an individual in the EU. However, unlike HIPAA, which only protects the privacy of an individual’s “protected health information,” GDPR applies broadly to all categories of health or other data regarding an individual. Personal Data is “any information relating to an identified or identifiable natural person” who is in the EU, regardless of the individual’s EU citizenship status. An individual is identified or identifiable if the individual can be “identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” Thus, the 18 individual identifiers under HIPAA would generally render an individual identifiable for purposes of both GDPR and HIPAA.
When does GDPR have extra-territorial reach to clinical activities in the United States?

The GDPR has direct extraterritorial reach to Personal Data processing of a controller or processor organization located in the United States or otherwise outside the EU if the organization processes the Personal Data:

- In the context of the activities of a business or other establishment in the EU such as a health care facility physically located in the EU;

- Related to the “offering of goods or services” (even if for free) to individuals in the EU, such as by advertising that targets individuals in the EU to be patients or other customers even if the services will be provided only in health care facilities located in the United States. The offering of goods or services is more than mere access to a website or an email address. For example, the “offering of goods or services” in the EU would include marketing activities intended to recruit individuals in the EU to be patients at a hospital in the United States; or

- Monitors the behavior of individuals in the EU, such as by continuing to monitor patients after they return to the EU, for example, as part of post-discharge patient engagement to prevent hospital readmission.

In addition, GDPR has extraterritorial reach to Personal Data processors in the United States if the controller is in the EU.

Does GDPR regulate Personal Data concerning health to the same extent as other Personal Data?

GDPR requires heightened protections for certain special categories of Personal Data (Sensitive Personal Data), including: Personal Data concerning health; genetic data; biometric data; and Personal Data revealing racial or ethnic origin.

- “Data concerning health” is Personal Data related to the physical or mental health of an individual, including the provision of health care services, which reveals information about the individual’s health status.

- “Genetic data” means Personal Data relating to the inherited or acquired genetic characteristics of an individual which give unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual.

- “Biometric data” means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of an individual, which allow or confirm the unique identification of that individual, such as facial images or dactyloscopic data.

These heightened protections apply regardless of whether a health care provider holds the Sensitive Personal Data as a health care provider, as an employer or in another capacity. For example, see the
below discussion of consent requirements for Sensitive Personal Data.

May EU member states adopt privacy laws that impose different rules than GDPR for Sensitive Personal Data concerning health?

While GDPR is intended to harmonize privacy law throughout the EU, EU member states are permitted to maintain additional limitations and other conditions regarding the processing of Personal Data that is genetic data, biometric data or data concerning health. Accordingly, before collecting and processing such Personal Data, health care providers should review individual EU member states’ health information privacy law for any conditions that are more restrictive than GDPR similar to the consideration of US state law that is more restrictive than HIPAA.

Does GDPR require a US health care provider to obtain consent to collect and further process Sensitive Personal Data concerning the health of a patient in the EU?

Unlike the HIPAA Privacy Rule which makes obtaining a patient’s consent for use of protected health information for treatment, payment and health care operations activities optional, GDPR generally requires a US health care provider either to obtain an individual’s consent to process Personal Data or to have another lawful basis for processing the Personal Data. GDPR only allows a limited exception to the consent requirement for the processing of Sensitive Personal Data for purposes of the provision of medical diagnosis or treatment by health care professionals in the EU who are subject to the obligation of professional secrecy established under the EU’s or a EU country’s law or under the rules established by national competent bodies in an EU country.

To obtain a valid consent to process an individual’s Personal Data under GDPR, the individual’s consent must be freely given, specific, informed and unambiguous agreement to the processing. For the processing of Personal Data about health or other Sensitive Personal Data, the consent must also be an “explicit” agreement to the processing:

- **Freely given**: The individual must have a realistic choice, or the realistic ability to refuse or withdraw consent without detriment. Similar to US law, coerced consents are not compliant with GDPR.

- **Specific**: The consent must include a specific, transparent statement of each purpose, including, without limitation, purposes other than treatment.

- **Informed**: An individual must be informed of the nature and extent to which the individual is consenting.

- **Unambiguous**: GDPR requires a statement or “clear affirmative act” (e.g., checking an unchecked box in an online context) that indicates the individual has agreed to the proposed processing activities. Silence, pre-ticked boxes and inactivity are insufficient for purposes of consent.

- **Explicit**: For the processing of Sensitive Personal Data, the individual’s consent must be explicit, which is a higher standard than unambiguous. The GDPR does not define “explicit” consent or describe how it compares to the “clear affirmative act” requirement of a regular consent to process Personal Data. However, GDPR interpretive guidance issued on
November 28, 2017 (Article 29 Consent Guidance) issued by the Article 29 Data Protection Working Party, an EU advisory body, includes several examples of explicit consent: a handwritten signature, an electronic signature, an uploaded scanned document carrying a signature or two-stage verification of consent where individual must click on a verification link by email or text message after initially consenting.

In addition, GDPR imposes the burden of proof of a valid consent on the controller. Accordingly, it is prudent for a controller to implement an audit trail or other reasonable procedures for consents obtained electronically.

**Does HIPAA protected health information become Personal Data protected by GDPR if a United States health care provider does nothing more than collect the data from an EU citizen at its facility in the United States?**

No, protected health information is not Personal Data merely because it concerns an EU citizen. Instead, the data must concern an individual *located in* an EEA country. Generally, individually identifiable data collected from an EU citizen at a location in the United States will be subject to US law unless the data was solicited from an individual while the individual was physically located in the EU or the organization continues to monitor the EU citizen after the citizen returns to the EU, such as part of post-discharge patient engagement programs.

**Is consent required for a health care provider in the United States to transfer protected health information about an American who is a tourist in the EU to a health care provider in the EU for treatment purposes?**

GDPR only applies to the US provider based on the three jurisdictional bases discussed above. Accordingly, if an EU health care provider requests a copy of medical records or other protected health information about the individual for the EU provider’s treatment purposes, GDPR would not regulate the US provider’s transfer of the protected health information merely because the information is being transferred to the EU. This is because the *ad hoc* transfer of records or other information alone should not constitute being an establishment, the offering of goods or services or monitoring individuals in the EU. The US provider would need to comply with any consent requirements under US. federal and state privacy laws. Note, however, that when an American travels to the EU for business, vacation or other purposes, an EU health care provider must protect the individual’s privacy in accordance with GDPR while the individual is in the EU.

**Does a US health care provider need to change the way its website operates in order to comply with GDPR with respect to site visitors who are located in the EU?**

GDPR has extra-territorial reach to the collection and processing of Personal Data about individuals in an EEA country over the Internet or through mobile applications if the processing is related to the “offering of goods or services” (even if for free) to individuals in the EU or part of online monitoring of individuals in such countries. The offering of goods or services and monitoring are more than mere access to a website by individuals in the EU. Monitoring that implicates GDPR occurs, for example, when individuals are tracked on the internet by cookies and other techniques which apply a profile to enable the website operator to make decisions about the individual or predict personal preferences.
US health care provider should also consider whether website pages that collect Personal Data to sign up individuals for newsletters, marketing materials or other communications target individuals in the EEA such as by pricing services in Euros or translating text into a national language (e.g., German) of an EEA country.

**May a US health care provider satisfy GDPR’s security requirements for electronic Personal Data with the same security measures adopted to comply with the HIPAA Security Rule?**

GDPR establishes high-level security standards but does not require controllers and processors to follow any particular set of security standards or code of conduct. Analogous to the Security Rule, GDPR requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security for Personal Data that is appropriate to the risk. Under GDPR, controllers and processors must assess and determine the appropriate level of risk to Personal Data taking into account the state of the art for security, the costs of implementation and the nature, scope, context and purposes of processing as well as the likelihood and severity of the risks to individuals’ privacy rights. Thus, it is possible for a US health care provider to comply with GDPR’s security requirements for electronic Personal Data through data security measures adopted to comply with the HIPAA Security Rule or that follow the security framework of the National Institute of Standards and Technology of the US Department of Commerce upon which the Security Rule is based.

To avoid any unintended gaps in security for electronic Personal Data, however, US health care providers should revisit security risk assessments performed for HIPAA compliance purposes to determine whether they assess the risks relative to the security of Personal Data (and not only electronic protected health information). In addition, GDPR requires a controller or processor to consider, as appropriate, whether “psuedonymisation,” which is similar to de-identification under the HIPAA Privacy Rule, and other data minimization techniques are appropriate security measures.

The GDPR imposes a complex privacy regime that differs in certain key respects from the HIPAA regulations. Health care providers should carefully consider these differences before recruiting patients from the EU or conducting other clinical activities involving individuals in the EU.

© 2024 McDermott Will & Emery

National Law Review, Volumess VIII, Number 57