Does GDPR Regulate My Research Studies in the United States?

Article By

Bernadette M. Broccolo
Daniel F. Gottlieb
Amy C. Pimentel

McDermott Will & Emery

Related Practices & Jurisdictions

- Communications, Media & Internet
- Global
- All Federal
- European Union

Monday, February 5, 2018

Summary

The General Data Protection Regulation (GDPR) establishes protections for the privacy and security of personal data (Personal Data) about individuals in the European Union (EU) single market countries, and potentially affects the clinical and other scientific research activities of academic medical centers and other research organizations in the United States.

In Depth

The General Data Protection Regulation (GDPR), which establishes protections for the privacy and security of personal data (Personal Data) about individuals in the
European Union (EU) single market countries, becomes effective May 25, 2018. The GDPR potentially affects the clinical and other scientific research activities of academic medical centers and other research organizations in the United States if the research involves Personal Data about individuals located in those countries regardless of the individuals’ citizenship status in the countries, but generally will not affect Personal Data collected from individuals then residing in the United States.

The EU single market countries include the EU member states, Norway, Iceland, Liechtenstein and Switzerland. In addition, other countries outside Europe have adopted or are expected to adopt privacy regimes similar to GDPR during 2018.

What is GDPR?

The GDPR replaces the EU Data Protection Directive and is designed to update and harmonize data privacy laws across the EU, to protect the privacy of individuals in the EU and to reshape the way organizations with operations or customers in the EU approach data privacy. The GDPR:

- Establishes the circumstances under which it is lawful to collect, use, disclose, destroy or otherwise “process” Personal Data, including when conducting clinical research activities;
- Establishes certain rights of individuals in the EU, including rights to access, amendment (called rectification under GDPR) and erasure (often referred to as the right to be forgotten);
- 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; 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.

GDPR regulates the collection, use, disclosure or other processing of Personal Data by controllers and processors. 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. A “processor” is a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

Does GDPR generally have extra-territorial reach to the United States?

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

- Creates an establishment in the EU;
• Offers goods or services (even if for free) to individuals in the EU, such as by advertising in the EU. The “offering of goods or services” is more than mere access to a website or email address, but could be evidenced by the organization’s use of language or currency generally used in one or more EU member states with the possibility of ordering goods/services there, and/or mentioning customers or users who are in EU. Likewise, an organization outside the EU that targets individuals in the EU would be subject to the GDPR. The “offering of goods or services” and targeting of individuals in the EU would include recruitment of individuals in the EU to participate in a research study;

• Monitors the behavior of individuals in the EU, such as by continuing to monitor patients after they return to the EU as part of, for example, post-discharge care. The monitoring of behavior will occur, for example, where individuals are tracked on the internet by techniques which apply a profile to enable decisions to be made/predict personal preferences, etc. This means in practice that a company outside the EU which is targeting consumers in the EU will be subject to the GDPR.

In addition, GDPR could indirectly apply to a United States organization if the organization has contractual relationships with research vendors or other third parties who are subject to the GDPR.

What data is “Personal Data” protected by GDPR?

GDPR requires Personal Data “controllers” and “processors” to protect individual’s Personal Data. 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.” For example, the 18 individual identifiers under the privacy standards adopted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) would generally render an individual identifiable for purposes of GDPR as well as HIPAA.

Does research data become Personal Data protected by GDPR if a United States academic medical center or other research organization collects the data from an EU citizen at a facility in the United States?

No, data is not Personal Data merely because it concerns an EU citizen. Instead, the data must concern an individual located in an EU single market country. Generally, individually identifiable data collected from an EU citizen at a location in the United States will be subject to United States law unless the data was solicited from an individual in the EU or the organization continues to monitor the EU citizen after the citizen returns to the EU.

Can Personal Data be de-identified and used for research
outside the limitations of GDPR?

Unlike the HIPAA de-identification standard, GDPR does not provide specific methods for de-identifying Personal Data. Instead, data would be “de-identified” (i.e., not Personal Data) if the data cannot be used to identify any individual, directly or indirectly, 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 individual. Generally, EU data protection authorities deem data to be de-identified if there is no reasonable means through which someone who has access to the data could use the data to re-identify an individual who is the subject of the data. As necessary to achieve de-identification under HIPAA, for key-coded data to be de-identified under the GDPR, the holder of the data must not have access to the re-identification key or possess any other means to re-identify the individuals who are the subjects of the data. Documenting the safeguards established to preserve the de-identification of the data is an important compliance step—such as in a written agreement with the data user or written policies for internal users, or both.

What are Personal Data controllers and processors in the context of clinical research?

GDPR regulates the collection, use, disclosure or other processing of Personal Data by controllers and processors. When engaged in clinical research activities involving Personal Data about individuals in the EU, a medical center or other research organization could be either a controller or a processor. Generally, the organization would take on a controller role if it participates in the design, direction or control of the research study (e.g., as a sponsor, lead investigator or primary research site) or directly recruits research subjects in the EU. An organization will take on a processor role if it collects and/or processes Personal Data only on behalf of and at the direction of the controller (e.g., as a clinical research organization).

My organization only conducts research activities in the United States and has no operations in the EU. Could GDPR apply to us?

We address four common clinical research scenarios involving United States academic medical centers (AMCs), other hospitals or other research organizations in the bullets below. GDPR does not apply if the organization does not collect or otherwise process Personal Data about individuals in the EU. In each scenario involving processing of Personal Data about individuals in the EU, the organization’s status as a controller or a processor regulated by GDPR turns on whether the organization directs or controls how Personal Data is processed.

- If the organization participates in a research study, but only recruits for the study, and collects and processes information about, individuals in the United States, the activities would be outside the scope of the GDPR even if: (1) one or more of the research subjects is an EU citizen who lives in the United States because the processing activities do not involve the processing of Personal Data about individuals in the EU, and/or (2) the organization has a presence in the EU for other wholly unrelated activities.
• On the other hand, if the organization participates in a global research study and conducts outreach and recruitment of individuals who are located in the EU to participate in the study and receives Personal Data about the individuals, the organization’s collection and processing of identifiable data of such individuals would be subject to the GDPR as a Personal Data controller.

• If the organization is a United States site for a global study and has the role of the primary research site and/or the lead investigator in a study, it is likely to have meaningful control over the study data analysis and reporting. In such case, the organization’s activities would likely be within scope of the GDPR as a controller (or joint controller with the sponsor of the study) if it receives Personal Data of individuals in the EU from EU research sites.

• The organization will typically be a processor subject to GDPR even if it merely collects and/or processes Personal Data about individuals in the EU in connection with the study and does so only on behalf of and at the direction of a third-party controller. For example, clinical research organizations engaged by research sponsors to perform specific activities at the sponsor’s direction are often processors rather than controllers.

**If a research organization relies upon an individual’s consent as the basis for processing Personal Data for a research study, what consent requirements apply under GDPR?**

GDPR permits an organization to rely upon consent from research subjects as a lawful basis for processing Personal Data for research purposes. As discussed below, to obtain a valid consent to processing an individual’s Personal Data for research purposes under GDPR, the individual’s consent must be freely given, specific, informed and unambiguous 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. The extent to which GDPR permits research organizations to obtain less than a specific and granular consent to process Personal Data for future research purposes, as now contemplated by the 2017 changes to the federal Common Rule that are now scheduled to become effective on July 1, 2018, is discussed further in the next section below and in our recent publication regarding these Common Rule changes, *HHS Finalizes Toned-Down Version of Common Rule Overhaul*.

• **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.
In addition, for the processing of genetic data, biometric data, health data and certain other sensitive categories of Personal Data (Sensitive Personal Data), the individual’s consent must be “explicit.” 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 hand-written 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.

**May a research organization process Personal Data for future uses beyond the purpose for which consent was initially obtained?**

Similar to the liberalized consent requirements for future use of data for research purposes in the amended version of the Common Rule adopted in 2017, GDPR Recital 33 suggests that research organizations may rely upon an individual’s consent at a more general level for the use of Personal Data for future research purposes that cannot be fully specified at the outset of a research study. Recital 33 provides as follows:

“It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.”

However, the Article 29 Consent Guidance includes guidance with respect to specificity of consent to future research uses that seems more restrictive than GDPR Recital 33 and the 2017 Common Rule revisions. The Guidance suggests that a broad consent to unclear future research purposes may not suffice and that GDPR requires a consent with a “well-described” purpose statement for each stage of research or other safeguards. Such safeguards may include data minimization, anonymization, data security or transparent communications to individuals as research activities progress. Accordingly, a research organization should carefully analyze the adequacy of proposed consent forms that seek broad consents to use Personal Data for undefined research purposes.

**Does GDPR include Personal Data Breach response and reporting obligations?**

Both controllers and processors subject to the GDPR have obligations to respond to a Personal Data Breach similar to the obligations of covered entities and business associates under the HIPAA breach notification standards. A “Personal Data Breach” is a 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. As under the HIPAA breach notification standards and certain US state breach notification laws, a Personal Data Breach may affect Personal Data in any form or medium and is not limited to unauthorized access to electronic data. A controller must report a Personal Data Breach to the data protection authority in the affected individual’s country without undue delay, and where feasible within 72 hours of becoming aware of the Personal Data Breach, unless the Personal Data Breach is unlikely to result in a risk to affected individuals. GDPR sets forth minimum requirements for the content of such notification. In the event of a Personal Data Breach causing a high risk to affected individuals, a controller must notify the affected individuals without undue delay, unless it qualifies for one of several enumerated exceptions. Like a business associate under the HIPAA breach notification standards, a processor must report a Personal Data Breach to the controller without undue delay.

***

The GDPR imposes a complex privacy regime that differs in key respects from HIPAA and the Common Rule. Academic medical centers and other research organizations should carefully consider these differences before embarking upon studies that involve Personal Data about individuals in the EU.

© 2021 McDermott Will & Emery

National Law Review, Volume VIII, Number 36

Source URL: https://www.natlawreview.com/article/does-gdpr-regulate-my-research-studies-united-states