Ready or Not, EU's General Data Protection Regulation (GDPR) Is Here

Insights 06.01.18

With the European Union's new data privacy law, the General Data Protection Regulation (GDPR)[1] taking effect on May 25, 2018, health care entities in the United States should assess whether the GDPR is applicable to their organization and, if so, what steps to implement for purposes of compliance.

PROFESSIONAL

ANDREA FREY
Partner
San Francisco
San Diego

KELLY A. CARROLL
Partner
Washington, D.C.

STEPHEN K. PHILLIPS
Partner
San Francisco

The GDPR could apply to a health care entity for a variety reasons, ranging from engagement in certain clinical research activities and medical tourism to offering products in the health technology sector, when such activities involve the personal information of an individual in the EU. This article sets forth a summary of the circumstances in which the GDPR could be applicable to a health care entity in the United States, an overview of some of the key components of the GDPR, and discussion of some of the key similarities and differences as compared to the Health Insurance Portability and Accountability Act (HIPAA).

Applicability of the GDPR to U.S. Health Care Organizations

At a high level, the objective of the GDPR is to protect the personal data of individuals (referred to as data subjects) in the EU in the "processing" of such data, while also promoting the free flow of such data throughout the EU. Notably, while applicability of the GDPR rests on the geography of the data subjects within the EU and not the citizenship of those individuals, the GDPR has a global reach that extends well beyond entities established or located in the EU, representing a significant shift from the existing EU Directive. The GDPR recitals note that the flow of personal data to and from countries outside of the EU is necessary for the expansion of international trade and international cooperation, but also recognize that an increase in the flow of data creates new challenges and concerns with respect to data protection.[2]

Article 3 of the GDPR provides that the regulation applies:

to the processing of personal data of subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related 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 behavior as far as their behavior takes place within the Union.[3]

Given the broad scope of this "monitoring behavior" and "offering goods or services" language, the GDPR could apply to health care entities in the United States in a number of ways.

For example, the GDPR will apply to U.S. research entities that conduct research at physical locations in the EU, recruit individuals in the EU to participate in research, or continue to monitor individuals in the EU (*e.g.*, following research conducted in the U.S.). On the other hand, data collected from EU citizens as part of research conducted wholly in the U.S. does not become "personal data" under the GDPR simply because of the EU citizenship of the research participant. The applicability of the GDPR focuses on where the behavior is occurring and being monitored, and where services are being offered. Clinical research sites in the United States that sponsor or have some control over study analysis and data processing for global studies should examine whether they receive personal data from individuals in the EU or recruit subjects for a study in the EU.

Further, if relying on a research subject's consent for processing his or her personal data as part of a research study, research entities should note the consent requirements under the GDPR, which defines consent as "any freely given, specific, informed and unambiguous indication" of agreement to the processing of his or her personal data.[4] Among other requirements, the GDPR requires that a data subject be informed of his or her right to withdraw consent at any time and be able to withdraw easily, consent should be given by a clear affirmative or opt-in action (i.e., default or pre-checked boxes would not constitute consent), and consent forms must be presented separately from other matters and must use clear and plain language.[5]

As another example, entities in the wearables technology sector, whether health care specific or not, may also be subject to the GDPR. For example, companies that develop and sell fitness trackers or other similar health and wellness technology to consumers on an international basis would be offering a good or service to individuals in the EU.

In addition, if a vendor of wearables does not market, sell or operate in the EU but processes the information of a customer who lives in the EU (and purchased the product while on vacation abroad) by receiving the wearable information and maintaining it on the vendor's servers, the vendor is monitoring the behavior of an EU resident and therefore subject to the GDPR. Notably, many of these entities employ a direct-to-consumer business model, under which they are not subject to HIPAA as either a covered entity or a business associate; for such direct-to-consumer businesses, the becoming GDPR compliant will be no small task, akin to what health care providers and other covered entities faced when HIPAA was first enacted.

Overview of the GDPR Requirements

As referenced above, one of the key purposes of the GDPR is to regulate the processing of personal data by controllers and processors, as such terms are defined under the regulation.

The GDPR defines "personal data" as any information relating to "an identified or identifiable natural person,"[6] and "processing" is defined to mean any operation performed on personal data (*e.g.*, collection, use, disclosure, storage).[7]

A "controller" is a person or entity that determines the purposes and means of processing personal data.[8] Although the concept is broader than that of a "covered entity" under HIPAA, it is a similar concept. A "processor" is a person or entity which processes personal data on behalf of the controller,[9] similar to the concept of a business associate under HIPAA.

The GDPR limits the processing of personal data to six circumstances.[10] The first is where the individual consents to such processing. The other five all hinge on whether the processing is "necessary." The processing must be necessary for: (1) the performance of a contract to which the data subject is a party (or requested by data subject prior to entering into a contract); (2) compliance with a legal obligation; (3) the protection of the vital interests of the data subject or other natural person; (4) performing a task carried out in the public interest or in the exercise of official authority; or (5) legitimate interests, unless overridden by the interests, fundamental rights and freedoms of the data subject.

Certain categories of more sensitive information, including data concerning health, genetic and biometric information, are subject to more stringent protection. "Data concerning health" is a subset of personal data "related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health

status."[11] Processing such health data is prohibited unless, in addition to one of the six circumstances above being present, one of the following ten bases for sensitive data applies:

1. The individual has given explicit consent to the processing of those personal data for one or more specified purposes;
2. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
3. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. Processing relates to personal data which are manifestly made public by the data subject;
6. Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
7. Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional, subject to certain safeguards;[12]
9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or
10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[13]

In addition to setting the parameters with respect to processing of personal data, as further described below, the GDPR addresses a wide range of other topics, including, without limitation, rights of data subjects, security requirements, establishment of regulatory authorities to implement and enforce the regulation, and applicable penalties.

COMPARISON TO THE HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA and the GDPR are driven by similar public policy objectives, and therefore many of the same concepts apply. Generally, an entity that is subject to HIPAA, whether as a covered entity or a business associate, and that currently implements a robust compliance program under HIPAA, should not find it a significant adjustment to incorporate the GDPR requirements into its operations. Entities that are not subject to HIPAA, on the other hand, may find compliance to be a steep uphill climb.

At its core, the GDPR includes many of the same general requirements as HIPAA, although the terminology and nuances of the requirements vary. For example, GDPR has an equivalent concept to HIPAA's minimum necessary rule, requiring that personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')." As another example, the GDPR also includes requirements to implement safeguards to protect the security of information, requiring that personal data be "processed in a manner that ensures appropriate security

of the personal data, including protection against unauthorized or unlawful processing against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality'), and further requiring that the entity adopt internal policies and implement measures with respect to such security safeguards. GDPR also contains similar concepts with respect to an individual's information and access rights, as well as contractual requirements between controllers and processors similar to the requirements for business associate agreements.[14]

However, some significant differences between the GDPR and HIPAA exist, where the GDPR imposes additional or different requirements. Although not exhaustive, a few key differences are identified below:

- *Applicability to personal data:* GDPR applies to "personal data," which is a much broader array of data than protected health information under HIPAA. In this respect, the GDPR is more comparable to state-level consumer protection and data breach notification laws in the United States.15]
- *Heightened consent requirements:* As discussed above, consent will be required under more circumstances than under HIPAA, given the limited provisions under which an entity may process personal data without consent. For example, consent will in most instances be required for treatment, in stark contrast to HIPAA.
- *Right to be forgotten:* Under GDPR, a data subject has a "right to be forgotten."[16] The data subject has a right to have his or her personal data erased and no longer processed under certain circumstances, including if no longer necessary for the purposes for which it was initially collected, where the data subject withdraws a prior consent, or where the processing of the data otherwise does not comply with GDPR. There is no corresponding concept under HIPAA. However, some exceptions exist. For example, to the extent a health care entity is required to maintain the data pursuant to a legal requirement, such as for record retention purposes, such retention is permitted.
- *Breach reporting:* Under the GDPR, a controller must report a data breach to the applicable supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it," unless able to demonstrate that the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."[17] This is a significantly shorter timeframe than under HIPAA, which has an outside deadline of 60 days for notification of individuals and, in some cases, the media and the U.S. Department of Health and Human Services Office for Civil Rights (OCR).[18] Notification to the data subject is also required without undue delay, if the breach is likely to result in a high risk to the subject's rights and freedoms.[19]
- Unlike HIPAA, GDPR provides a right to compensatory damages for data subjects that suffer damage (whether or not material) as a result of a violation of the GDPR. This is a significant difference, since HIPAA does not include a private right of action, whereas violations of the GDPR could potentially be a basis for individual lawsuits or class actions on behalf of data subjects whose personal information is compromised. In addition, administrative fines can vary depending on the violation, but could be as much as "20 million EUR or, in certain cases, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher." Although settlements with OCR for HIPAA violations have in some instances been in the multi-million-dollar range, administrative fines under the GDPR could potentially be even higher. It is unclear how or whether penalties could be imposed against a United States entity at this time. However, at a minimum the implementation of the GDPR, and the amount at stake for entities in the EU, will likely lead to many such entities insisting on contractual covenants regarding compliance with the GDPR and corresponding indemnification provisions to do business with a United States entity (similar to the requirements many health care providers in the United States impose on offshore business associates, if willing to work with such companies at all).

In addition, a U.S. health care entity will need to update their privacy policy to incorporate additional disclosures, and may be required to appoint a representative in the EU, as well as a data protection officer, depending on the nature and scope of activities involving the personal data of individuals in the EU.

If an organization has not already assessed the applicability of the GDPR to their operations, they should do so without delay given that the regulations are now in effect. Although in many ways similar to HIPAA, some significant differences also exist, and an organization that is subject to the GDPR will need to update internal policies and procedures, consumer facing

materials, and business associate agreements, and adjust workflows as needed, to ensure compliance.

For more information, please contact Steve Phillips or Andrea Frey in San Francisco at 415.875.8500; Amy Joseph or Jeremy Sherer in Boston at 617.532.2702; or Kelly Carroll in Washington, D.C. at 202.580.7700.

[1] General Data Protection Regulation (E.U.), 2016/679, *available at* http://data.europa.eu/eli/reg/2016/679/oj.

[2] GDPR, Recital 101.

[3]] GDPR, Article 3(2).

[4] GDPR, Article 4(11).

[5] GDPR, Article 7, and Recitals 32 and 42.

[6] GDPR, Article 4(1).

[7] GDPR, Article 4(2).

[8] GDPR, Article 4(7).

[9] GDPR, Article 4(8).

[10] GDPR, Article 6(1).

[11] GDPR, Article 4(15).

[12] In particular, data must be processed "subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies." GDPR, Article 9(3). As discussed in this article, the practical impact is that consent will generally be required for treatment.

[13] GDPR, Article 9(2).

[14] In multiple cases, different terminology applies but the equivalent concept is in both sets of laws. For example, the right to "rectification" corresponds to the HIPAA concept of an individual's right to request an amendment.

[15] *See, e.g.,* Cal. Civ. Code § 1798.82; M.G.L. C. 93H; 201 CMR 17.00.

[16] GDPR, Article 17.

[17] GDPR, Article 33(1).

[18] 45 C.F.R. §§ 164.404, 164.406, & 164.408.

[19] GDPR, Article 34.

RELATED CAPABILITIES

Digital Health

Health Information Privacy and Security

Digital Health