COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 5. May 31, 2018 'Embrace' GDPR With Compliance Framework Already In Place for HIPAA Privacy, Security

By HCCA Staff

Beginning this month, health care privacy and security officers have more than just the HHS Office for Civil Rights (OCR), the Federal Trade Commission and the various state attorneys general to worry about when it comes to protecting patient data: GDPR.

The compliance date is May 25 for GDPR, the acronym for the General Data Protection Regulation, although it's likely many HIPAA compliance officials know it simply as GDPR. And chances are they don't actually know a whole lot about the law, even though the effective date was two years ago following adoption by the European Parliament and Council of the European Union (EU).

If they haven't already, covered entities (CEs) and business associates should take some time to understand the specifics and implications of GDPR on their organizations. When it comes to GDPR, experts who spoke at the Health Care Compliance Association's (HCCA) recent annual Compliance Institute say the foundation that should be in place for HIPAA compliance will serve them well (hint: "should be in place" is key).

Basics of Regulation

Under GDPR, affected organizations are called "controllers" or "processors."

The regulation "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor" in the EU and "to the processing of personal data of data 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 behaviour as far as their behaviour takes place within the Union."

Processing is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Personal data is defined as "any information relating to an identified or identifiable natural person," who is referred to as a "data subject." Further, "an identifiable natural person is one who 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."

As the regulation states, "for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation." By definition, the consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by

a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Depending on the circumstances, the regulation requires the appointment of a data protection officer, the development of a data protection impact assessment, and notification to authorities within 72 hours of knowledge of a breach and as soon as possible to the individual. An exception is when "the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

GDPR also provides individuals with the "right to be forgotten," an aspect that has grabbed some headlines when it has resulted, for example, in Google having to purge references to certain people.

For the full text of GDPR, see https://tinyurl.com/ydb6gtqu.