Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Frontier Of US Health Info Regulation Comes From EU

By **Nancy Libin and David Saunders** (June 19, 2018, 2:04 PM EDT)

Nancy Libin

Over the past year, in this space we have examined the declining trend of Health Insurance Portability and Accountability Act enforcement actions by the U.S. Department of Health and Human Services Office of Civil Rights since the start of the current presidential administration. While OCR continues to investigate claims of HIPAA violations, the undeniable fact is that the pace of announced enforcement actions has slowed to a trickle. The last OCR HIPAA-related enforcement action dates back to February of this year, and there have only been two announced enforcement actions this calendar year. This pace seems to be the new normal of this presidential administration. So it's time for covered entities and business associates everywhere to relax, right? Not so fast.

David Saunders

As the readers of this article are undoubtedly aware, on May 25, 2018, a new data protection sheriff came to town, and the specter of that new enforcement rubric should keep every covered entity and business associate on its toes. We are talking, of course, about the General Data Protection Regulation, or GDPR. While the GDPR is a creation of the European Union, it has extraterritorial reach and teeth. The GDPR imposes strict data protection requirements on companies that monitor, or offer goods and services to, consumers in the EU, no matter where the companies are located. Because of its extraterritorial reach and uniform application to all personal data, the GDPR promises to increase privacy protections not just for consumers in the EU, but for U.S. consumers, too. Moreover, it imposes heightened requirements with respect to the processing of "special category" data, which includes health-related information. Therefore, if a covered entity or business associate that offers services to people located in the EU has not yet implemented a privacy program to comply with GDPR, it better cancel its summer plans and begin to do so now.

While OCR recently has been quiet with respect to HIPAA enforcement actions, the newly empowered EU data protection authorities will be eager to flex their muscles and show that GDPR's extraterritorial reach is not only real, but that noncompliance can be painful. We therefore spend the remaining part of this article examining which covered entities and business associates need to pay attention to GDPR if they have not already.

Whom the GDPR Covers

The GDPR applies to both data controllers[1] and data processors[2] that, as noted above, (1) are established in the EU, or (2) that are not established in the EU, but that offer goods and services to EU residents or track EU residents online (for marketing purposes, for example). The GDPR could cover — for example — multinational hospital chains, medical insurance companies, medical billing companies, electronic medical records companies, and an assortment of other HIPAA-covered entities.

Being a HIPAA business associate rather than a covered entity does not get you off the GDPR hook. The GDPR reaches business associates, just as HIPAA does. If you are a HIPAA business associate based in the U.S. and you think that you handle exclusively U.S. data, it would nonetheless be wise to check with your covered entities and upstream business associates to see if they are covered by the GDPR. Because if your upstream business partners are covered, there is a real risk that you may be handling the personal data of people located in the EU and are therefore covered too.

What the GDPR Requires

The GDPR requires companies to implement measures to incorporate the following principles into their data processing activities: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; security; and accountability. Companies will have to conduct thorough assessments of the personal data that they collect, maintain, use and disclose, as well as review their contracts with vendors and their policies and procedures with respect to such data, so that they can make any necessary changes to ensure compliance with the GDPR. Practically speaking, this means that HIPAA-covered entities and business associates may have to develop, among other things, new policies, amend existing business associate or services agreements, and implement new technical safeguards to protect the data being collected, used and stored.

In addition, companies must identify a "legal basis" for the processing of personal data of consumers in the EU. And because health-related data is sensitive, the GDPR requires that companies also either obtain explicit consent from the individual (e.g., a signed statement consenting to the processing of health-related information) before processing such data, or be able to show that processing is necessary for the provision of health care and that the company is subject to certain secrecy obligations under EU or EU member state law.

The GDPR offers six possible legal bases: (1) consent; (2) necessary to perform a contract; (3) necessary to fulfill a legal obligation; (4) necessary to protect someone's vital interests (such as life or health); (5) necessary to perform a task in the public interest; or (6) necessary to fulfill the company's legitimate interests, provided that such interests are not outweighed by the rights and freedoms of the individual. In the HIPAA space, it is not difficult to imagine any one of the six legal basis applying. For example, an EU resident might consent to the use of their personal data for medical care or billing. (As noted above, if the processing relates to health-related data, the consent must be "explicit.") The processing of EU resident data also might be necessary for a medical billing company to process bills or for an insurer to pay benefits on behalf of an EU resident. In addition, HIPAA-covered entities and business associates may need to use EU resident data to alert authorities of a health emergency or outbreak of disease. All of these would be permissible uses under the GDPR. However, GDPR requires that the entities using the personal data have a basis before using the information.

In addition, the GDPR requires that companies take steps to safeguard data, some of which are similar to the restrictions that HIPAA already imposes. A noninclusive list of safeguards that GDPR-covered

entities must take include: (1) providing notice to individuals regarding certain aspects of an entity's data processing activities; (2) processing personal data only for purposes compatible with the purpose for which the data was collected; (3) collecting, using and disclosing only the data that is necessary for the underlying purpose of processing; (4) ensuring that the data is accurate and correct; (5) deleting data when it is no longer necessary to maintain; and (6) maintaining adequate security safeguards. These obligations mirror certain rights that consumers have under the GDPR, such as the right to request access to and correction of personal data, deletion of data and restriction of processing; the right to object to processing; the right to withdraw consent; and the right to data portability. Consumers also have the right to withdraw consent, when processing is based on consent.

After reading this article, hopefully you realize that even if you are just a HIPAA business associate operating in the United States, you need to confirm that none of your covered entities or business associates are GDPR-covered entities — or that your own operations do not trigger GDPR obligations. If you do not take action, then you are risking hefty penalties for noncompliance, with fines running as high as 40 million euros or 4 percent of a company's total global annual turnover, whichever is higher.

The bottom line is that covered entities and business associates cannot take too much comfort that OCR may be moving slower than it did under the last administration. The GDPR is in force and its enforcers are on the beat. If you have not already asked the question of whether you are covered by the GDPR, it is past time to do so.

Nancy C. Libin is a partner and chairwoman of the data privacy and cybersecurity practice at Jenner & Block LLP. She previously served as chief privacy and civil liberties officer of the U.S. Department of Justice.

David P. Saunders is a partner at Jenner & Block.

[1] Data controller is a European term used to describe a company that, alone or with others, determines how personal data will be processed and for what purpose.

[2] Data processors are companies, such as cloud providers, that process personal data on behalf and at the instruction of data controllers.