U.S. hospitals will continue to grapple with GDPR compliance in 2019

January 31, 2019

When the European Union's General Data Protection Regulation (GDPR) became effective on May 25, 2018, many U.S.-based hospitals struggled to determine whether they were subject to the GDPR and, if so, what they must do to attain full compliance. While recent guidance has made these determinations somewhat easier, questions and confusion around GDPR compliance will likely continue throughout 2019.

GDPR enhanced existing protections for the personal data and privacy of individuals in the EU. It also extended the reach of those protections beyond organizations based in the EU, including U.S.-based hospitals that "offer goods and services" to individuals in the EU or "monitor the behavior" of such individuals. Organizations subject to GDPR on one or both of these bases must comply with restrictions on data that go beyond the reach of the Health Insurance Portability and Accountability Act (HIPAA).

GDPR regulates a wider range of data than HIPAA, as it applies to any information related to a natural person that can be used directly or indirectly to identify that person. Individual rights are broader under GDPR as well, including unrestricted rights of access and accountings of disclosures, the "right to be forgotten" (i.e., erasure), and the right to bring a distinct cause of action against an organization that

Chris Bennington
Partner
Cincinnati
513.870.6572
cbennington@bricker.com

controls or processes data. A particularly challenging element of GDPR compliance is the notice of breach requirement, which mandates that individuals be notified of a breach of their information within 72 hours of its discovery (as opposed to 60 days under HIPAA).

In November 2018, the European Data Protection Board (EDPB) issued draft guidance to clarify the territorial scope of GDPR. The comment period on that guidance remains open until January 18, 2019, and the EDPB will then issue final guidance. While the guidance is not yet final, it is instructive as to the EDPB's thinking on the issue of GDPR's territorial scope.

With regard to "offering goods or services," the EDPB guidance clarified that an organization must have the intent to offer goods or services to individuals in the EU in order to be subject to the GDPR. Hospitals that actively and intentionally market services to individuals in the EU may, therefore, be subject to GDPR. With regard to "monitoring," the EDPB stated that GDPR may apply even without an intention to target an individual in the EU but also clarified that the mere collection of data from an individual might not constitute "monitoring." The EDPB will focus on the purpose of the data processing and any further behavioral analysis or profiling of individuals in the EU. Hospitals that conduct research involving individuals in the EU may be engaging in "marketing" that subjects them to GDPR.

U.S. hospitals should look for the final guidance in 2019. If the determination is made that a hospital is subject to GDPR, it should promptly enact the necessary policies and procedures and take other steps to achieve full compliance.