akerman

Blog Post

GDPR: What You Need to Know Now

April 30, 2018

It is safe to say that there has been much fear and confusion over the European Union (EU) General Data Protection Rule, or GDPR. With an effective date of May 25, 2018, and little guidance as to how the GDPR applies to organizations that do not have a physical presence in the EU or do not target their goods and services to EU residents, companies, including healthcare entities, with few, if any, business contacts with EU members are challenged to bring their companies into compliance. We have outlined below the fundamental questions that healthcare entities are likely asking themselves regarding GDPR, including whether they must comply with yet another data privacy regulation.

What Is the GDPR?

Given today's headlines regarding hacking and invasion of privacy on social media platforms, it would be easy to presume that the GDPR was born out of the current environment. However, the GDPR is intended to update the EU's existing data privacy framework, which dates back to 1995. The GDPR creates an EU-wide set of rules that seek to protect an individual's data given the changes in technology and people's behavior over the last twenty years. GDPR applies to entities that are established in the EU and process personal data in the context of that establishment. GDPR also applies to entities that process the personal data of EU citizens, even if the entities do not have a physical location in the EU or the data processing does not take place within the

Related People

Elizabeth F. Hodge
Robert E. Slavkin

Related Work

Data Privacy and Security
Health Insurers and Managed Care Organizations
Healthcare
Hospitals and Health Systems

Health Law Rx Blog

Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

EU. Thus, U.S.-based healthcare entities may be subject to GDPR if they do any of the following:

- participate in joint ventures with EU-based organizations;
- conduct medical research involving EU residents;
- engage in telemedicine between a U.S. provider and an EU resident;
- maintain referral or consultation relationships with EU health care providers; or
- market services specifically to EU residents.

While some requirements of the GDPR are similar to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other U.S. privacy laws, GDPR gives individuals more rights in their personal data than does HIPAA and other U.S. laws. For example, GDPR protects "personal data" and "sensitive personal data," which include more identifiers than protected health information. Under the GDPR, personal data is defined as 'information relating to an identified or identifiable natural person ('data subject'); 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.' This broad definition includes IP addresses, a device ID or a customer reference number. Also, entities subject to GDPR must report breaches of personal data to an EU data protection authority within seventy-two hours of discovery.

Does My Company Need to Comply?

This is the $64,000 question, and there is limited guidance regarding how U.S.-based healthcare entities that do not envisage providing goods and services to EU residents should answer that question. Until the EU publishes more guidance,

health care entities should look to Recital 23 of the GDPR, which may provide some indication as to compliance obligations. The litmus test is whether or not the processing activities of EU residents' personal information is related to the offering of goods or services to individuals in the EU. Merely having a website that may be accessed by EU residents is not enough to be subjected to the requirements of the GDPR. Likewise, having an EU resident present to a hospital emergency room, without more, is not likely not sufficient to trigger GDPR requirements. Other factors that possibly impact this determination include whether or not the company website has been translated into languages used in the EU or whether the pricing has been converted to the Euro. Absent such indicators, it becomes more attenuated a connection to the EU, making it a lower probability that GDPR compliance is required.

What Is the Penalty for a Breach of Obligations under GDPR?

The potential financial penalties comprise the 'teeth' to the GDPR. Organizations face a fine of up to the *greater* of €10 million (roughly $12 million USD, based on the conversion rate at the time of publication) or 2% of global annual revenue from the prior year. In the case of non-compliance with key provisions of the GDPR, regulators can impose fines of up to the *greater* of €20 million (roughly $24 million USD, based on the conversion rate at the time of publication) or 4% of the company's annual global revenue. Note that in both scenarios, the key word in imposition of fines is 'greater'. The fines are stiff, possibly catastrophic to smaller businesses, and for companies with revenues in the tens of billions, these fines quickly become mind-boggling, at 2 or 4% of total annual revenue.

What Should We Do?

U.S.-based healthcare entities should take the following steps:

- Determine if your organization receives or exchanges personal data with EU countries. This includes determining what data you receive from or about EU residents, including through websites that your organization maintains;
- Analyze the risk, starting with an impact assessment of your organization's high-risk activities involving sensitive personal data. Can the organization reduce its risk by collecting less personal data or keeping it for a shorter time?
- If necessary, review and update existing privacy policies and notices to comply with GDPR;
- Assess your current vendors who process personal data. Can they satisfy GDPR requirements?

Additionally, healthcare entities should continue to monitor guidance and further regulations issued by the EU to assess if the GDPR applies to them and how best to bring their organization into compliance.