COSMOS
Navigate the Compliance Universe

Compliance Today - September 2018
Is the sky falling? GDPR implications in the US

by Adam H. Greene, JD, MPH and Lyra Correa, JD

Adam H. Greene (adamgreene@dwt.com) is a Partner in the Washington DC office of Davis Wright Tremaine LLP and co-chair of its Health Information Practice Group. **Lyra Correa** (lyracorrea@dwt.com) is an Associate in the Washington DC office of Davis Wright Tremaine LLP.

- linkedin.com/in/adam-greene-bb0a4933
- linkedin.com/in/lyra-correa-73a245160

Pop quiz: An injured Belgian tourist appears at your door for treatment. Do you:

A. Pay to medevac her across the Atlantic and unceremoniously dump her on the shores of Achill, Ireland (the closest spot to the U.S. in the European Union (EU)

B. Handwrite all her medical notes on the back of napkins and burn them at discharge

C. Shutdown the facility for a week while you scramble to come into compliance with the EU's General Data Protection Regulation (GDPR)[1]

D. Treat her like a regular patient and protect her information in accordance with the Health Insurance Portability and Accountability Act (HIPAA)[2]

If you answered A, B, or C, then it's time to take a deep breath and relax. And possibly revisit your Emergency Medical Treatment and Active Labor Act (EMTALA) compliance.

The most reasonable answer is D. Although there are many frantic headlines regarding GDPR, it will likely have limited impact on most US healthcare providers. US healthcare providers should carefully review whether they fall under GDPR, including through marketing efforts and website information collection. If GDPR is applicable, then it is not too late to begin compliance, and HIPAA is a very good place to start.

What is the GDPR?

GDPR is a new set of rules drafted by the EU that are designed to provide a stronger set of protections to give individuals in the European Economic Area (EEA) (i.e., the 28 EU countries plus Norway, Iceland, and Liechtenstein) more control over their personal data. GDPR regulates the collection, use, disclosure, and other "processing" of personal data by "controllers" and "processors." A "controller" is an entity that determines the purposes and means of the processing of personal data, while a "processor" is an entity that processes the personal data on behalf of the controller. The relationship of the controller and processor is analogous to the relationship between a covered entity and a business associate. The processor (business associate) processes data on behalf of a data controller (covered entity) and is required to protect the data the same way that a controller would. Like HIPAA, GDPR also requires controllers and processors to implement technical and organizational measures to prevent breaches of the personal data. GDPR does not refer to "citizens" or "residents," but rather applies to the processing of personal data of any person in the EU (a "data subject"), even if the person is only in

the EU temporarily.

Stateside impact?

HIPAA may not apply to entities located outside of the U.S. because neither the HIPAA statute nor the regulations address extraterritoriality, and Congress gave no indication that it intended HIPAA to apply outside of the U.S. Unlike HIPAA, GDPR has direct extraterritorial reach to entities that process the personal data of EU data subjects, regardless of whether the processing takes place within the EU. The good news is that GDPR will not affect a majority of US healthcare providers and only affects healthcare providers that are:

- Physically located in the EU,
- Market to EU data subjects, or
- Monitor data subjects' behavior for activities taking place in the EU.

Marketing to EU data subjects involves more than EU data subjects having mere access to a US healthcare provider's website or general global marketing. However, if a US healthcare provider actively pursues EU data subjects (e.g., by converting to EU currency on the provider's website, offering a website specific to an EU country, marketing in the language of the EU country), then GDPR will apply.

Monitoring the behavior of EU data subjects relates to collecting information about an EU data subject's activities while the data subject is in the EU. For example, as we go from website to website, different websites track information about us, such as what we click on, for purposes of building a profile about us. This is often used to target specific advertisements to us. If a US company collects this information while an individual is using the Internet from the EU, then the US company will become subject to GDPR.

In the scenario above, if the US provider that treated the Belgian patient did not market to the EU to try to attract EU patients and does not continue to provide treatment to the patient after she returns to the EU (e.g., telemedicine), then GDPR is unlikely to apply. However, if the US healthcare provider has a website specifically designed to attract Europeans, or uses website cookies for purposes of creating profiles about the online behavior of patients (or anyone else for that matter) when they are in the EU, then GDPR may become applicable to the US healthcare provider.

In determining whether GDPR is applicable, US healthcare providers should focus on questions such as:

- Do we have offices in the EU?
- Do we operate in the EU, such as by performing clinical research in the EU in partnership with EU institutions?
- Do we advertise in the EU?
- Does our website include features clearly aimed at attracting EU patients (not just international patients generally)?
- Does our website include monitoring of patients or other website visitors (e.g., tracking website visitors' behavior through website cookies or other means) that may capture behavior of EU data subjects?

Even if not directly subject to GDPR, US healthcare providers and other healthcare entities should also be careful about contractually agreeing to comply with GDPR. For example, certain online service providers may interpret that they are required to pass on GDPR-related contractual provisions to anyone who uses their services.