Center for Health and Wellness Law, LLC

Navigating GDPR for the Health and Wellness Industries
May 25, 2018

By Barbara J. Zabawa, JD, MPH
Center for Health and Wellness Law, LLC

On May 25, 2018, the General Data Protection Regulation (GDPR) in the European Union (EU) takes effect. The premise behind GDPR is to recognize that the protection of natural persons in relation to the processing of personal data is a fundamental right. GDPR Recital 1. Many health and wellness companies in the United States may wonder what, if anything, must they do to comply with this new law. If your health or wellness company has an internet presence, such as through a website, read on to see if GDPR applies to your company and if so, what you need to do about it.

To Whom Does GDPR Apply?

In general, GDPR applies to "controllers" and "processors." The law defines controllers as an entity that determines the purposes and means of processing personal data. GDPR Article 4.7. This may include an employer or health care organization, for example. The law defines "processor" as an entity that collects, records, organizes, structures, stores, adapts, alters, retrieves, consults, uses, discloses, disseminates, combines, restricts, erases or destroys personal data. GDPR Article 4.1 and 4.8. "Personal data" is data that relates to an identified or identifiable natural person (i.e., "data subject"). GDPR Article 4.1.

Controllers may hire processors to work with personal data on some level. So, one useful analogy may be to compare controllers with "covered entities" under HIPAA, and processors with "business associates" under HIPAA. If you are a health or wellness company that works with personal data, such as through a wellness portal or application, you must next determine whether your company interacts with any "data subjects" under the GDPR.

There are three types of companies that interact with data subjects and who therefore fall under the auspices of the GDPR:

1. Companies that are established in the EU, regardless of whether the processing of personal data occurs within the EU. GDPR Article 3.1. So, if your company has a physical presence in the EU, the GDPR applies to you.
2. Companies that are not located in the EU but conduct data processing activities related to the offering of goods or services, irrespective of whether the data subject must pay for those goods or services, to data subjects in the EU. To fall within this category, the company would need to specifically target EU data subjects, such as include on its website language used by an EU country, allow for payment by a currency used by an EU country, or mention customers or users who are in the EU. Merely allowing access to

the company's website in the EU without adding any features that specifically target the EU would not be enough to make the company subject to the GDPR.

3. Companies that are not located in the EU when the company monitors the behavior of data subjects located in the EU. For example, companies who track EU data subjects on the internet for purposes of profiling those subjects so that the company can predict his or her personal preferences, behaviors and attitudes would be subject to GDPR.

It is important to note that GDPR application is not tied to EU citizenship. Thus, EU citizens located outside the EU would not be protected by GDPR. Likewise, US citizens located in the EU would be protected by the GDPR. GDPR applies to "natural persons" located within the EU, regardless of their citizenship. It does not apply to "legal persons," such as corporations. GDPR Recital 14.

If GDPR Applies to My Company, What Must it do to Comply?

While spelling out all the legal requirements and details of the GDPR is beyond the scope of this post, there are some overarching requirements of which health and wellness companies subject to GDPR should be aware.

1. **The company may not process health or biometric data unless the data subject gives explicit consent**. Explicit consent can be electronic or on paper, but the consent should be an "affirmative act." An affirmative act could include a signature or clicking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data. GDPR Recital 12.

   If the consent is given in the context of a more global privacy policy or "terms and conditions" document, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. So, health and wellness companies subject to GDPR may want to separate their consent for processing health or biometric data from the rest of the company's privacy policy or terms and conditions statement.

   Health and biometric data subject to GDPR includes information derived from the testing or examination of a body part or bodily substance, or any information on a disease, disability, disease risk, medical history, clinical treatment or physiological or biomedical state of the data subject. It doesn't matter who collects this data. If the company that has the data is subject to GDPR, then that company must not process that data unless it obtains the data subject's consent and follows the other GDPR requirements. See GDPR Recital 35.

2. **The company must provide certain rights to the data subject**. First, the company must provide information about the data being collected from the data subject. This

information includes, among other things, the purposes for which the data is being collected, who will receive the data, and whether the data will be transferred outside the EU. GDPR Article 13.

Second, the data subject has the right to correct inaccurate personal data about him or her. GDPR Article 16. Third, the data subject has the right to "be forgotten." That is, if the data subject requests it, the company must erase personal data about the person if, for example, the data are no longer necessary in relation to the purposes for which they were collected. GDPR Article 17. Fourth, the data subject has the right to object to processing their personal data for direct marketing purposes. GDPR Article 21.

3. **The Company Must Implement Certain Measures to Ensure Compliance with GDPR.** These measures include, for example: a) implementing technical and organizational measures to protect data security (GDPR Article 31); b) notifying certain authorities of a data breach within 72 hours of discovering the breach, as well as the individual in cases of high risk to the rights and freedoms of individuals (GDPR Articles 33 and 34); and c) designating a data protection officer (GDPR Article 37).

Conclusion

Health and wellness companies that are subject to GDPR have a number of new obligations under the law. A robust data privacy and security compliance program will help health and wellness companies comply with the new requirements, and help clients of those companies feel confident in the company's privacy and security practices. With almost daily reports of data privacy intrusions, more legal protections are certain to appear. Implementing strong policies and procedures to protect data privacy and security now will not only lighten the load of GDPR, but future laws as well.