Bond | HEALTH CARE INFO MEMO

MAY 17, 2018

European Privacy Regulation Will Impact U.S. Health Care Organizations

Effective May 25, 2018, the European General Data Protection Regulation ("GDPR") imposes new obligations on persons or entities that are "controllers" or "processors" of "personal data"[1] about individuals in the European Union ("EU"). Unlike U.S. or even current privacy laws in Europe, the GDPR: (i) can apply to entities that are located *entirely outside* of the EU; and (ii) applies to personal data about *anyone in the EU*, regardless of whether they are a citizen or permanent resident of an EU member state.[2] As a result, the GDPR has significant extraterritorial reach.

The GDPR covers "personal data" defined broadly to include information that identifies or is identifiable about an individual, including health care, financial, and social information ("Personal Data"). U.S. health care providers and institutions – including health systems, health plans, academic medical centers, hospitals, physicians, payers, nursing homes, and alcohol and drug treatment centers – will be subject to the GDPR if they have the requisite relationship to Personal Data about individuals in the EU, directly or through vendors or contractors. For example, the GDPR could apply to U.S. health care providers and institutions that:

- Treat patients in the EU in-person or remotely via telemedicine, teleradiology or other means;
- Continue to monitor EU patients after they are treated in the U.S.;
- Conduct clinical programs involving data subjects in the EU, including through health care facilities located either in the U.S. or the EU;
- Employ providers or staff from the EU who provide Personal Data to their employer while in the EU as part of the application process or otherwise;
- Participate in scientific or clinical research that involves receipt of Personal Data from the EU;
- Engage in certain kinds of targeted marketing in the EU, such as by attempting to recruit EU persons to be become patients of a U.S. health care facility or service provider; or
- Employ certain vendors within the EU (i.e., "processors").

Controllers and Processors

As mentioned above, the GDPR applies to persons or entities that are "controllers" or "processors" of Personal Data. A controller is an individual or legal entity that, acting alone or with others, determines the purposes and means of processing Personal Data. A processor, on the other hand, processes Personal Data on behalf of the controller, including activities such as data analytics, data storage, and data alteration. For example, if a U.S. health care institution targets EU individuals in a marketing campaign, and retains an email or marketing agency to assist in the campaign, the health care institution would be the controller and the email or marketing agency would be the processor with respect to any associated Personal Data. Or, if a U.S. hospital uses a call center to help monitor patients who had been treated in the United States after their return to Europe, the hospital would be the controller and the call center would be the processor of the personal data.

1 These terms are defined below.

2 Each EU member state will likely adopt its own rules with respect to GDPR compliance; thus businesses with significant contacts in the EU may need the assistance of local counsel in connection with each applicable EU member state. Currently, the U.K. has indicated it intends to follow the GDPR; however, post-Brexit, it is unclear whether the U.K. will implement its own separate set of rules.

Personal Data Protected by the GDPR

In some respects, the GDPR is similar to the HIPAA Privacy and Security Rules that have applied to U.S. health care providers for over 15 years. Both regulatory regimes mandate that certain organizations ("covered entities" and "business associates" under HIPAA, "controllers" and "processors" under the GDPR) protect the privacy and security of certain categories of information. In contrast to HIPAA which applies to "protected health information" (PHI),[3] the GDPR covers all Personal Data about an identified or identifiable individual residing in the EU, even if temporarily. Accordingly, U.S. health care organizations subject to the GDPR will have to adjust their privacy and security policies to account for the broader definition of protected information under the new EU regulation.

Moreover, under the GDPR, certain kinds of Personal Data are subject to stricter privacy and security requirements. In addition to data about race, ethnicity, political opinions and religious beliefs, among other personal characteristics, this special category includes the following types of health-related information:

- "Data Concerning Health" – Personal Data related to the physical or mental health of an individual, including the provision of health care services, which reveals information about the individual's health status. This category of protected data is similar but not identical to "protected health information" under HIPAA.
- "Genetic Data" – Personal Data relating to the inherited or acquired genetic characteristics of an individual which give unique information about the physiology or health of that individual and which result, in particular, from an analysis of a biological sample from the individual.
- "Biometric Data" – Personal Data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of an individual, which allow or confirm the unique identification of that individual, such as facial images.

Under the GDPR, health, genetic, and biometric data generally can be processed only with the individual's express consent, or if processing is necessary in connection with an individual's medical diagnosis or treatment, for certain public health functions, for research, or for other limited purposes defined in the GDPR. The exceptions to the requirement of patient consent under the GDPR are different from and arguably more limited than those under HIPAA; for example, the exceptions do not encompass the broad categories of treatment, payment and operations.

What are the Major GDPR Requirements?

Among other things, the GDPR requires a covered institution to:

- Appoint a person (called a "Data Protection Officer") to oversee protection of Personal Data;
- Provide notice regarding the Personal Data it collects, and how it uses such Personal Data;
- Record the uses and disclosures it makes of Personal Data;
- Obtain specific consent for collection of certain kinds of Personal Data;
- Allow individuals whose Personal Data was collected to object to such collection or processing, and ultimately honor an individual's "right to be forgotten," unless a legitimate basis exists to maintain the data;
- Ensure that all vendors and third parties to which it provides Personal Data have adequate privacy and security protections;
- Enter into contracts containing specific provisions when transferring Personal Data outside of the EU (including transferring within the institution); and
- Notify EU regulators, and potentially impacted data subjects, as soon as possible (where feasible, within 72 hours) after becoming aware of a data breach.

3 For this purpose, health information means information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Building GDPR Policies on the Framework of HIPAA

Many of the policies and operational steps to implement the GDPR are similar to HIPAA. For example, the requirement to appoint a Data Protection Officer to oversee the policy and data protection tracks closely to the obligations for a Privacy Officer. Similarly, the requirements to track the use and disclosure of Personal Data, to provide an accounting upon request, and enter into agreements to protect Personal Data with third parties that receive the data, are all similar to the requirements of HIPAA. For this reason, health care providers can build their GDPR policies on the framework of their HIPAA policies. At the same time, other elements of the GDPR are distinct from HIPAA and will require health care providers in the U.S. covered by the GDPR to adopt new privacy policies and procedures.

Conclusion: Preparing for the GDPR

U.S. health care organizations covered by the GDRP, directly or through the exchange of data with vendors, may be required to review and make appropriate modifications to a host of policies, including: (i) employment policies; (ii) data collection policies and procedures; (iii) policies for patient consent, especially when one or more of the special data categories are involved (see above); (iv) research protocols; and (v) procedures governing patient monitoring. Business Associate Agreements must also be modified to cover certain mandated GDPR clauses.

If you have any questions about this memorandum, or the steps necessary for GDPR compliance, contact Tracy E. Miller, Robert W. Patterson, or Lisa A. Christensen, or the attorney at Bond with whom you are regularly in contact.

Contacts

For more information, contact one of the individuals below:

Tracy E. Miller
646.253.2308
tmiller@bsk.com

Robert W. Patterson
716.416.7040
rpatterson@bsk.com

Lisa A. Christensen
315.218.8279
lchristensen@bsk.com

BOND SCHOENECK & KING ATTORNEYS