U.S. Department of Health and Human Services Issues New "Guidance" on Mobile Health Applications

By: Daniel Ferhat and Laura Steven
Healthcare Alert
3.18.16

The U.S. Department of Health and Human Services, Office for Civil Rights (HHS) recently published new guidance to assist mobile health application developers determine whether they are "business associates," and therefore subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The HHS guidance includes a list of "Helpful Links," or frequently asked questions, designed to help mobile health application developers (developers) understand HIPAA regulations and compliance obligations. The HHS guidance includes predominantly general information about HIPAA and business associates, with one link geared toward developers: "Health App Use Scenarios & HIPAA." The HHS guidance page also features an interactive message board, where anonymous users can post specific questions and receive comments from other users and/or HHS employees.

The "Health App Use Scenarios & HIPAA" link uses concrete and practical examples to address: 1) how HIPAA applies to health information that a patient creates, manages or organizes through the use of a health app; and 2) when a developer must comply with the HIPAA rules. HIPAA compliance is mandatory if the app involves use or disclosure of protected health information (PHI), and the app developer is an employee of a covered entity, such as a health plan, healthcare clearinghouse, or most health care providers.

App developers who are not employees of covered entities, but instead create or offer the app on behalf of covered entities, or covered entities' contractors, may be considered business associates and must also comply with HIPAA. An app developer is a business associate if the developer creates, receives, maintains, or transmits PHI on behalf of a covered entity or a covered entity's business associate. For example, if a patient downloads a health app and inputs his or her own information, without the involvement of any providers, the app developer is *not* a business associate because the developer did not create, receive, maintain, or transmit PHI on behalf of a covered entity or covered entity's business associate. On the other hand, if a patient downloads a health app at the direction of his or her provider and inputs information that is automatically incorporated into the electronic health record, the developer *is* considered a business associate because the provider contracted with the app developer for patient management services that involved creating, receiving, maintaining and transmitting PHI. However, if an app developer and provider have entered into an interoperability agreement at the patient's request, whereby the patient inputs health information into the app and then directs the app to transmit the information to the provider's electronic health record, a business associate relationship does not exist because the patient is initiating the sharing of information.

In summary, the calculus of whether an app developer constitutes a business associate generally turns on the patient's role in transmitting or approving the transmittal of PHI. If a provider is working with an app developer and directing patients to use apps that would trigger a business associate relationship, that provider must enter into a written contract or other arrangement to protect the privacy of PHI. Further, if a provider finds that the business associate app developer violated the contract or otherwise committed a material breach, the provider must take steps to immediately cure the breach and, if it cannot, terminate the contract and/or report the business associate to HHS.

The HHS guidance is an excellent resource for covered entities and app developers to better understand when HIPAA applies and what obligations might attach. Given the proliferation of mobile health applications and their union with the electronic health record, HIPAA obligations and compliance are not always clear-cut. Because a HIPAA breach can result in significant financial and reputational harm, it is essential to consult with an expert who can help navigate the regulatory morass.

For more information on this matter, please contact Daniel Ferhat (ferhatd@whiteandwilliams.com; 215.864.6297) or another member of the Healthcare or Cyber Law and Data Protection Groups.

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only and you are urged to consult a lawyer concerning your own situation and legal questions.