OCR HIPAA Guidance for Mobile Health Developers

May 4, 2016 Jennifer Kreick

PRACTICES Healthcare and Life Sciences, Healthcare Transactions and Regulatory, Health Privacy (HIPAA) and Healthcare IT

With the recent increase in health information technology, developers in this area are finding themselves facing a web of complex federal and state regulations and are often left with more questions than answers. However, the cost of hiring legal advisors and experts to help untangle this web can be insurmountable for some individuals and start-up companies. An interactive web platform released by the U.S. Department of Health & Human Services Office of Civil Rights ("**OCR**") could help those trying to navigate some of these difficult issues.

In October 2015, OCR launched a web platform for mobile health developers to help identify and address issues specific to developers of health information technology with regards to the Health Insurance Portability and Accountability Act ("**HIPAA**"). The site allows users to interact with OCR by submitting questions and receiving feedback directly from OCR and other users of the site and also acts as a repository for guidance and links helpful to mobile health developers. As explained on the site, OCR recognizes that there is "an explosion of technology using data about the health of individuals in innovative ways to improve health outcomes."[1] However, many developers of this technology may be unfamiliar with HIPAA and its regulations. OCR is using this site to understand what guidance on HIPAA regulations would be helpful to developers. If users wish to submit a question or comment, they must register with the site using their email address; however, their identities and email addresses remain anonymous to OCR.

In February 2016, OCR published a set of six specific scenarios on the site to assist developers in determining when HIPAA applies to them. OCR emphasized that the scenarios are highly dependent on the facts and circumstances, and that even a slight change in facts could change the analysis. For example, OCR stated that when a consumer downloads a health app to her smartphone and populates it with her own information (such as blood glucose levels and blood pressure readings she obtained herself using home health equipment), the app developer is not a business associate under HIPAA. OCR made clear that the developer in this scenario is not creating, receiving, maintaining, or transmitting protected health information ("**PHI**") on behalf of a covered entity or business associate.

Likewise, if a consumer uses a health app that is designed to help her manage a chronic condition and then adds her own information to the app (even if she downloads the data from her doctor's electronic health record through a patient portal and then uploads it into the app), the developer is still not a business associate, because the consumer obtains the health information from her provider and then inputs it into the app for her own purposes.

OCR also stated that an app developer is not a business associate if a doctor recommends to a patient a particular app to track diet, exercise, and weight, and the patient downloads the app and uses it to send a summary report to her doctors before her next appointment. The developer is not a business associate because the developer is not creating, receiving, maintaining or transmitting PHI on behalf of a covered entity or business associate (note that the patient initiated the transmission to her physician). Thus, although the doctor recommended the app, there is no indication that the doctor hired the developer to provide services to patients involving PHI.

OCR's guidance clarifies that a developer becomes a business associate under HIPAA only when the developer provides goods or services to or on behalf of a covered entity or business associate that involve the use or disclosure of PHI. For example, OCR stated the following scenario would not render an app developer a business associate:

1. a consumer downloads a health app to her smartphone;
2. the consumer requests that her health care provider and the app developer enter into an interoperability arrangement that allows for secure exchange of the consumer's information between the provider's electronic health record and the app;
3. the consumer populates information on the app and directs the app to transmit the information to the provider; and
4. the consumer is able to access her test results from the provider through the app.

In this scenario, the app developer is providing a service to the consumer at the consumer's request and is not using or disclosing PHI on behalf of the covered entity. "The app developer is transmitting data on behalf of the consumer to and from the provider."[2] The interoperability agreement alone is not enough to make the app developer a business associate of the provider since "the arrangement exists to facilitate access initiated by the consumer."[3]

In contrast, an app developer would be a business associate of a provider if the provider "has contracted with app developer for patient management services, including remote patient health counseling, monitoring of patients' food and exercise, patient messaging, EHR integration and application interfaces."[4] The patient, at the direction of her provider, downloads the health app, and the information the patient inputs is automatically incorporated into the provider's electronic health record. In this scenario, the app developer contracts with the provider for certain services that involve the use and disclosure of PHI, and the app is a means for providing the services.

Similarly, an app developer is a business associate if an app is offered by a health plan and the app allows users in the network to request, download, and store health plan records and to check the status of claims and coverage decisions. The health plan "analyzes [the] health information and data about app usage to understand effectiveness of its health and wellness offerings."[5] However, the app developer would not be a business associate of the health plan if it offered a direct-to-consumer version of the app that consumers could use to store, manage, and organize their health records and to send health information to providers, because the product is not provided on behalf of a covered entity or business associate, as long as the app developer keeps the health information in the two versions of the app completely separate.

OCR's web platform provides a unique tool for developers and others in the mobile health industry to interact with OCR and also gain insight into OCR's enforcement perspective. As we continue to see health care technology developments, this platform will likely play an important role in developing and shaping OCR's guidance in this area. View the web platform and guidance.

*Portions of this text originally appear in *SMU Science and Technology Law Review*, Vol. XVIII.

[1] Dep't of Health & Human Servs., Office of Civil Rights, OCR Invites Developers to Ask Questions about HIPAA Privacy Security, (last visited Apr. 7, 2016).

[2] Dep’t of Health & Human Servs., Office of Civil Rights, Health App Use Scenarios & HIPAA (Feb. 2016).

[3] *Id.*

[4] *Id.*

[5] *Id.*