POLSINELLI

in the news

Health Care Technology

March 2016

OCR New Guidance Aims to Help Medical Mobile App Developers Predict when HIPAA Obligations Might Apply

In this Issue:

Predicting whether the activities of a mobile health application (app) developer trigger legal obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) presents some new challenges – not surprising when 20th century law is extrapolated to apply to 21st century technology.

In recognition of the complexity introduced by rapidly evolving and innovative digital health technology, the Office for Civil Rights (OCR) on Feb. 11, 2016, issued new guidance on its mHealth Developer Portal (http://HIPAAQsportal.hhs.gov) titled "Health App Use Scenarios & HIPAA." OCR released the guidance in hopes that it "will help developers determine how federal regulations might apply to products they are building" and "will reduce some of the uncertainty that can be a barrier to innovation."

The new guidance describes six scenarios involving a mobile health app, accompanied by OCR's analysis and determination under each scenario as to whether the app software developer would be considered a business associate under HIPAA. In each scenario, the app collects, stores, maintains, or transmits health information from the consumer and/or the consumer's provider.

The apps in these various scenarios range in function from tracking the user's diet, exercise, and weight; enabling the user to enter certain health metrics collected by other devices (e.g., blood glucose levels and blood pressure readings obtained using home health equipment); helping users manage chronic conditions; to providing users with a mobile version of their Personal Health Records (PHRs), as offered by the users' health plan.

The new guidance provides insight into OCR's approach that attempts to strike a balance between protecting consumer health information and minimizing uncertainty that can stifle innovation. While app developers may

be able to navigate HIPAA more clearly, they will still have to navigate other potentially applicable federal laws and state privacy laws.

When Health App Developers Are Subject to HIPAA

Out of the six scenarios outlined in the guidance, OCR concludes that only two scenarios result in the creation of a business associate relationship between a covered entity and the app developer. In the first case, a health care provider contracts with an app developer for patient management services, including remote patient health counseling, monitoring of the patients' food intake and exercise, patient messaging, and electronic health records integration.

In the second scenario where OCR determined a business relationship would be created, the mobile PHR app was offered by the consumer's health plan to enable users in its network the ability to request, download, and store health plan records and check the status of claims and coverage decisions. The rationale for OCR's findings in both scenarios is that the app developer is "creating, receiving, maintaining, or transmitting" protected health information on behalf of a covered entity. The critical factor is whether such services are being provided for or "on behalf of a covered entity." The mere fact that health information is collected from the consumer and that such information may be shared with the consumer's health care provider, or that this information is combined with the consumer's other health information contained in the provider's EHR, does not necessarily create a business associate relationship.

When Health App Developers Are Not Subject to HIPAA

OCR's guidance tackles a spectrum of scenarios, from the scenario where a consumer downloads the app and inputs his/her own glucose levels and blood pressure reading, without interaction with a health care provider, to several others, with increasing interaction and data exchanges with his/her health care provider. For example, in one scenario: "Doctor counsels a patient that his BMI is too high, and recommends a particular app that tracks diet, exercise, and weight. The consumer downloads app to his/her smartphone and uses it to send a summary report to the doctor before his/her next appointment." Here, OCR states the app developer is not a business associate.

OCR explains that "the doctor's recommendation implies her trust in the app, but there is no indication that the doctor hired the app developer to provide services to patients involving the handling of PHI. The consumer's use of an app to transmit data to a covered entity does not by itself make the app developer a BA of the covered entity." The key here is that the developer was not "hired" to provide the services on behalf of the provider.

In another scenario, even where the health care provider and app developer have entered into an interoperability arrangement to facilitate "secure exchange of consumer information between the provider EHR and the app," so as to enable the consumer to transmit information to the provider's EHR, and for the consumer to access test results from the provider, OCR concludes that a business associate relationship is not created.

In the scenario above where OCR concluded that the software developer that offers a mobile PHR app on behalf of a health plan is a business associate, OCR also concluded that if the developer also offers a separate, direct-to-consumer version of the product that is not provided "on behalf of" a covered entity or other business associate, the developer's activities "with respect to that product are not subject to the HIPAA rules."

OCR determined that while the software vendor is a business associate of the health plan with respect to the mobile PHR app, it is not a business associate when offering the direct-to-consumer services. Therefore, "as long as the developer keeps the health information attached to these

two versions of the app separate, so that information from the direct-to-consumer version is not part of the product offering to the covered entity health plan, the developer does not need to apply HIPAA protections to the consumer information obtained through the 'direct-to-consumer' app."

This indicates that just because a software developer functions as a business associate in a particular arrangement with a covered entity or business associate for a certain offering, does not mean the developer is a business associate subject to HIPAA requirements for all of its offerings (e.g., the direct-to-consumer version of a functionally similar product).

The guidance also drives home other key points – if a developer is not creating, receiving, maintaining, or transmitting protected health information (PHI) on behalf of a covered entity or another business associate, the developer is likely not a business associate. Similarly, if there is "no indication the provider…hired the app developer to provide or facilitate this service," it is likely not a business associate. Finally, if a consumer is using an app to help him/her manage and organize his/her own information without any involvement of a health care provider, the app is likely not a business associate.

Key Questions for Developers

The guidance also raises several key questions that app vendors (who are not already covered entities) should consider in determining whether or not they may be business associates:

- Does your health app create, receive, maintain, or transmit identifiable information?
- Who are your clients? How are you funded?
- Are your clients covered entities?
- Were you hired by, or paid by, a covered entity? Or another business contracted to a covered entity?
- Does a covered entity (or a business associate acting on its behalf) direct you to create, receive, maintain, or disclose information related to a patient or health plan members?
- Is your app independently selected by a consumer?
- Does the consumer control all decisions about whether to transmit the data to a third party (such as his/her health care provider or health plan)?
- Do you have a relationship with that third party entity (other than an interoperability relationship)?

OCR cautions app developers to keep in mind that "protecting the privacy and security of consumers' data is still important," even though they may not be covered entities or their business models do not include acting as business associates.

For More Information

For more information regarding this alert, please contact the authors or your Polsinelli attorney.

- Jean Marie R. Pechette | 312.873.3690 | jpechette@polsinelli.com
- Lindsay R. Kessler | 312.873.2984 | lkessler@polsinelli.com

To contact a member of our Health Care Technology team, click here or visit our website at www.polsinelli.com > Services > Health Care Services > Health Care Technology > Related Professionals.

To learn more about our Health Care Technology practice, click here or visit our website at www.polsinelli.com > Services > Health Care Services > Health Care Technology.

POLSINELLI

real challenges. real answers. SM

About Polsinelli's Health Care Practice

The Polsinelli Health Care practice represents one of the largest concentrations of health care attorneys and professionals in the nation. From the strength of its national platform, the firm advises clients on the full range of hospital-physician lifecycle and business issues confronting health care providers across the United States.

Recognized as a leader in health care law, Polsinelli is ranked as "Law Firm of the Year" in Health Care by *U.S. News & World Report* (November 2014), no. 1 by *Modern Healthcare* (June 2015) and nationally ranked by *Chambers USA* (May 2015). Polsinelli's attorneys work as a fully integrated practice to seamlessly partner with clients on the full gamut of issues. The firm's diverse mix of attorneys enables our team to provide counsel that aligns legal strategies with our clients' unique business objectives.

One of the fastest-growing health care practices in the nation, Polsinelli has established a team that includes former in-house counsel of national health care institutions, the Office of Inspector General (OIG), and former Assistant U.S. Attorneys with direct experience in health care fraud investigations. Our group also includes current and former leaders in organizations such as the American Hospital Association. Our strong Washington, D.C., presence allows us to keep the pulse of health care policy and regulatory matters. The team's vast experience in the business and delivery of health care allows our firm to provide clients a broad spectrum of health care law services.

About Polsinelli

real challenges. real answers.[SM]

Polsinelli is an Am Law 100 firm with more than 775 attorneys in 19 offices, serving corporations, institutions, entrepreneurs and individuals nationally. Ranked in the top five percent of law firms for client service*, the firm has risen more than 100 spots in Am Law's annual firm ranking over the past six years. Polsinelli attorneys provide practical legal counsel infused with business insight, and focus on health care and life sciences, financial services, real estate, technology and biotech, mid-market corporate, and business litigation. Polsinelli attorneys have depth of experience in 100 service areas and 70 industries. The firm can be found online at www.polsinelli.com. Polsinelli PC. In California, Polsinelli LLP.

** 2016 BTI Client Service A-Team Report*

About this Publication

POLSINELLI

real challenges. real answers. SM