HEALTHCARE

APP USERS BEWARE: MOST HEALTHCARE, FITNESS TRACKER, AND WELLNESS APPS ARE NOT COVERED BY HIPAA AND HHS'S NEW FAQS MAKES THAT CLEAR
by Sara H. Jodka

Individuals who use healthcare apps such as fitness trackers, weight loss, wellness, exercise, etc., **BEWARE!** A couple of recent developments have highlighted the fact that most apps are not subject to HIPAA, which means that with broadly-worded privacy policy these healthcare apps can and do readily share healthcare and other data collected by the apps with third parties, including marketing and analytics companies, such as Google and Facebook. Some apps are sharing sensitive healthcare data even without a privacy policy.

The first eye-opening development was a study published in the journal JAMA Network Open (JAMA Study) reported that a number of healthcare apps marketed to people who wanted to stop smoking or who had depression were providing user data, including user health/medial information to third party advertisers and analytics companies such as Facebook.

Notably, the JAMA Study was clear that much of the data the apps reviewed shared did not immediately identify the individual user nor was it strictly medical. However, *all* but 3 of the 36 apps reviewed shared information that was a valuable predictor of individual behavioral conduct with advertisers or analytic companies. A few apps also shared sensitive information including substance use information app users had self-reported through the various apps.

The JAMA Study was certainly not the first study of its kind. The Wall Street Journal in a piece titled "You Give Apps Sensitive Personal Information. Then They Tell Facebook" revealed that Flo, a period-tracking app, shared users' health information, including period dates and pregnancy plans, with third-party sites such as Facebook.

Other health apps have self-reported security flaws and/or to sharing user personal health information with advertisers and analytic companies. Not surprisingly, the revelation that private health information was being shared to massive information-gathering powerhouses stirred up a lot of questions, such as:

- How could this happen?
- Isn't health/medical information private, not so easily shareable, or at least subject to higher privacy standards?
- What was communicated to the users about what information would be shared and how?
- What did the apps' privacy policies say about this information sharing or, rather, what *didn't* the privacy policies say?
- How can health app users make informed decisions about whether they want to use an app if they don't know who will be given access to their personal health information?

These are all very valid questions, which is why it is interesting that, around the same time that the JAMA Study was released, the Department of Health & Human Services Office for Civil Rights (HHS), which enforces HIPAA, issued five new FAQs addressing the applicability of HIPAA to health-related apps.

Before diving into HHS's FAQs, it is important to preface that most people assume that HIPAA protects health information from disclosure or at least provides some higher level of security over health information. However, HIPAA is narrower than most people believe, which it why the FAQs are interesting in that they demonstrate exactly where HIPAA's Privacy and Security Rule protections end, especially as it pertains to healthcare apps, and how health-information collection and sharing (as found in the JAMA Study) is so profound.

The key to understanding how these healthcare apps can disclose so much sensitive information unbeknownst to the users is understanding that, in most instances, the healthcare apps at issue are not covered by HIPAA and, therefore, not subject to HIPAA's Security Rule and Privacy Rule requirements. That means the healthcare data those app companies collect is also not protected by HIPAA's protections.

HIPAA does not provide a blanket, overarching protection to all medical/health/wellness information. HIPAA is limited to "covered entities" and their "business associates" who are sharing "protected health information" ("PHI" or "ePHI" when discussing electronic information) concerning "covered transactions". All of the quoted terms are specifically defined by HIPAA and most third-party healthcare apps do not qualify as a "covered entity", a "business associate", as having "PHI" or as engaging in a "covered transaction" for purposes of triggering HIPAA's requirements.

Looking to HHS's FAQs, they are specific to transactions between a patient, a healthcare provider, and the healthcare provider recommending a course of treatment that includes transmitting healthcare information to an app. This, in and of itself, sheds a tremendous amount of light as to how so much PHI information is *not* protected by HIPAA.

*** **FAQ 572** ***

> Does a HIPAA covered entity that fulfills an individual's request to transmit electronic protected health information (ePHI) to an app bear liability under HIPAA for the app's use or disclosure of the health information it received?

For instance, the first FAQ addresses whether a covered entity is liable under HIPAA if it sends ePHI to an app at the patient's request and the app discloses that information. This FAQ is important for

understanding why third-party apps, which are wholly unaffiliated with any covered healthcare entity, can disclosure or otherwise share healthcare information without violating HIPAA.

As the FAQ answer makes clear, the key to determining how much protection a particular piece of PHI has is to understand the relationship between the healthcare provider that is recommending or requiring a patient to use a particular app and the app developer itself. If the app itself is developed by or on behalf of the healthcare covered entity, then the use of that app would be subject to HIPAA protections because the app developer would be either a covered entity or a business associate to the healthcare provider as defined by HIPAA. If, however, there is no such relationship and the app is strictly a third-party app with no affiliation to the healthcare provider, such as all those reviewed in the JAMA Network Open study, HIPAA would not apply or offer any protections for the disclosure of or sharing of PHI.

In other words, once health information is received from a covered entity, at the individual's direction by an app that is neither a covered entity nor a business associate (as defined under HIPAA), the information has lost its HIPAA protection it might have once had. This means that any subsequent use, disclosure, etc., of e-PHI by the non-covered entity would not trigger liability under HIPAA and no up-the-chain liability for the healthcare provider in the event of a breach, misuse, etc.

If, however, the app was developed for and/or provided on behalf of the covered healthcare provider, the covered healthcare provider would be liable for any breach or other improper disclosure of PHI.

Putting this into application, think about an app that is provided by and/or developed for a healthcare provider, such as a hospital. The app can be used to help patients check their records, schedule appointments, review their invoices, etc. That app and any use of the information provided by patients through the app would be subject to HIPAA's protections.

Conversely, a fitness tracking, wellness or health monitoring app that is advertised via Facebook, Instagram, or by other means, is found via the App Store, has no affiliation to a hospital or clinic, and was not recommended by a healthcare provider would not be subject to HIPAA.

*** **FAQ 573** ***

> What liability does a covered entity face if it fulfills an individual's request to send their ePHI using an unsecure method to an app?

The next FAQ is interesting because it analyzes whether a covered entity is liable if is grants an individual's request to send their PHI using an unsecured method to an app. It is not surprising that HHS determined that the covered entity would not be liable for unauthorized access to an individual's PHI if the individual requests their PHI be sent to an app via an unsecure method. It is surprising to most that this is even an option and that, somehow, an individual can somehow direct his or her PHI to be sent electronically through an unsecure channel.

The real issue identified here is not in HHS's answer, but rather brought to light with the knowledge that somehow individuals can consent to the unsecured transmission of their PHI because who would actually do that and why. As to the why, well, it is postured as a matter of convenience. As to who, well, the answer is that most people have no idea they are consenting to this. This consent is usually obtained when a patient arrives for a doctor's appointment and has to sign the HIPAA Privacy Notice that is put in front of them as the patient signs in for an appointment. Somewhere in that notice is a request for consent to allow PHI to be sent via unsecured channels if deemed quicker or more convenient by the healthcare provider.

The FAQ makes it clear that if PHI is sent this way via the individual's consent, the healthcare provider would not be liable for any loss that may occur during transmission to the app. HHS recommended, but did not require, that covered entities inform individuals of the potential risks involved in consenting to an unsecured transmission.

*** **FAQ 574** ***

> Where an individual directs a covered entity to send ePHI to a designated app, does a covered entity's electronic health record (EHR) system developer bear HIPAA liability after completing the transmission of ePHI to the app on behalf of the covered entity?

The next FAQ addressed liability after transmission by a covered entity's electronic health record system in the event a patient directs a covered entity to send PHI to a particular app. Again, and in line with the key issue identified initially above, HHS determined that the answer depends on the relationship, if any, between the covered entity, the EHR-system developer, and the app.

Here, a business associate relationship exists if the entity creates, receives, maintains, or transmits PHI on behalf of a covered entity in order to execute covered transactions of the covered entity.

No such business associate relationship exists between an EHR-system developer if the EHR-system developer does not own the app or, if it does, does not provide the app to, through or on behalf of the covered entity. For example, if the EHR-system developer creates an app, makes it available via the App Store as part of an entirely separate revenue stream or business unrelated to its role as a business associate to a healthcare covered entity, then it would not be liable under HPAA for any PHI use or disclosure it receives via its app.

FAQ 575

> Can a covered entity refuse to disclose ePHI to an app chosen by an individual because of concerns about how the app will use or disclose the ePHI it receives?

Another FAQ addressed whether a covered entity could refuse to disclose a patient's PHI if it had concerns about the app's use or disclosure of the PHI. HHS determined that the covered entity's concerns were irrelevant because HIPAA general prohibits a covered entity from refusing to disclose PHI to a third-party app as requested by an individual if the PHI is in a form/format used by the app. This disclosure is allowed based on the individual's right of access under HIPAA. The other side of this is that the covered entity also does not bear responsibility for any misuse of the PHI during or after it transmits such data pursuant to an individual's request. And since the third-party app also bears no responsibility since it is not covered by HIPAA, it is really the individual who shoulders all the risk if he or she asks his/her ask their healthcare provider to transmit their PHI to a third-party app.

*****FAQ 576*****

> Does HIPAA require a covered entity or its EHR system developer to enter into a business associate agreement with an app designated by the individual in order to transmit ePHI to the app?

The last FAQ analyzed whether HIPAA requires a covered entity or its EHR-system developer to enter into a business associate agreement with an app designated by the individual before transmitting PHI to the third party's app. Again, the answer is dependent on the relationship between the app developer and the covered entity and/or its EHR-system developer.

As set forth in other FAQ analysis, HHS reasserted its position that HIPAA does not require a covered entity or its EHR-system developer to enter into a business associate agreement with an app developer if the app does not create, receive, maintain or transmit PHI on behalf of or for the benefit of the covered entity.

If, however, the app was developed on behalf of the covered entity or provided by the covered entity, then a business associate agreement would be required because HIPAA would be triggered by the nature of the relationship.

What about the apps' privacy policies?

The other interesting tidbit to come out of the JAMA Study was how little the apps' privacy policies disclosed about how PHI would be shared. In some cases, the privacy policies were completely silent in this area. The issue then, and rightfully so, is how can the app developers get away with inaccurate privacy policies? The answer is that the oversight for privacy policies that are not covered by HIPAA are also not enforced by HHS; rather, they are subject to enforcement by the Federal Trade Commission. The FTC has levied fines and penalties against some website and app developers for miscommunications in their privacy policies, as the FTC considers the issue a matter of fraud under Section 5 of the Federal Trade Communication Act, but enforcement in this area is behind the technology. So, while the FTC has the enforcement power to make these app developers be honest and clear about their information sharing and disclosing practices, it is likely that there are just too many to go after and information such as the findings of the JAMA Study is just starting to shed light on this situation.

Takeaways

The key takeaway here is that app users bear the bulk of responsibility when they choose to input their personal health or other information into apps. Health information does not have a universal protection and HIPAA is extremely limited as to its protections to such apps.
Even if the app is subject to HIPAA, there are a number of ways information can be disclosed via individual consent – and sometimes via consent the individual is not even sure they are granting.

When it comes to healthcare, wellness, fitness tracking, and other apps, it is critical for users to remember that the widespread information sharing to third party advertisers and analytics sites, such as Facebook and Google, applies exactly the same as it occurs with other information such as shopping preferences. An entity cannot share information that is not disclosed to it. So, unless an individual is sure the app he or she is using is covered under HIPAA and that does not otherwise allowed information to be shared to a third-party app via unsecured means, users must understand that information shared to an app may very well be shared to many other entities and people.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Labor and Healthcare law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka, CIPP-US is a Member in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.