INFOBRIEF

Topic: How Health Apps and Fitness Trackers Impact Employer HIPAA Compliance

ISSUED 04/17/19

In recent FAQs, the Department of Health and Human Services (HHS) provided additional guidance on covered entities HIPAA obligations amid the growing wellness trend of utilizing health applications and fitness trackers to monitor health trends and progress.

Forbes reports that "worldwide wearables sales will grow by an average of 20 percent each year over the next five years, becoming a $29 billion market with 243 million unit sales by 2022." Likewise, a 2012 Pew Research Center Mobile Health Report found that one in three cellphone owners used their phones to look for health information while one in five smartphone owners downloaded a health app, with exercise, diet, and weight apps being the most popular. By 2015, a national survey showed as much as 58% of mobile phone users had downloaded a health-related mobile app, but that nearly half of the users had stopped using the apps partly because of the high data entry burden.

To ease their manual data entry burden, many covered individuals are requesting that the covered entity (the health plan or health care provider), provide their electronic protected health information (ePHI) directly to the third-party app. For covered entities that must ensure it has appropriate measures in place to protect its covered individuals' ePHI, these apps and trackers can pose unique challenges when trying to balance HIPAA obligations to protect data and avoid a breach, and the covered individual's right to access their ePHI.

HHS HIPAA Professional FAQs 3009, 3010, 3011, 3012, and 3013 provide important insight into what liability the covered entity has for the app's use or disclosure of ePHI, whether the covered entity is liable for sending ePHI to an app using an unsecured method, and if a covered entity can refuse to disclose ePHI to an app based on concerns about how the app will use or disclose the ePHI. Additionally, HHS provides guidance on the relationship between the covered entity and the app developer, including which entity is liable under HIPAA and when a business associate agreement is required.

In summary, the FAQs provide the following guidance:

Does a HIPAA covered entity that fulfills an individual's request to transmit ePHI to an app or other software bear liability under the HIPAA Rules for the app's use or disclosure of the health information it received?

- If the individual's app – chosen by an individual to receive the individual's requested ePHI – was

not provided by or on behalf of the covered entity (and, thus, does not create, receive, transmit, or maintain ePHI on its behalf), the covered entity would not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app.

- If the app was developed for, or provided by or on behalf of the covered entity – and, thus, creates, receives, maintains, or transmits ePHI on behalf of the covered entity – the covered entity could be liable under the HIPAA Rules for a subsequent impermissible disclosure because of the business associate relationship between the covered entity and the app developer.

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?

- Under the individual right of access, an individual may request a covered entity to direct their ePHI to a third-party app in an unsecure manner or through an unsecure channel.
- In such a circumstance, the covered entity would not be responsible for unauthorized access to the individual's ePHI while in transmission to the app.
- With respect to such apps, the covered entity may want to consider informing the individual of the potential risks involved the first time that the individual makes the request.

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?

- No. The HIPAA Privacy Rule generally prohibits a covered entity from refusing to disclose ePHI to a third-party app designated by the individual if the ePHI is readily producible in the form and format used by the app.
- The HIPAA Rules do not impose any restrictions on how an individual or the individual's designee, such as an app, may use the health information that has been disclosed pursuant to the individual's right of access.

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?

- If the EHR system developer does not own the app, or if it owns the app but does not provide the app to, through, or on behalf of, the covered entity and not as part of its business associate relationship with any covered entity – the EHR system developer would not be liable under the

HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app.

- If the EHR system developer owns the app or has a business associate relationship with the app developer, and provides the app to, through, or on behalf of, the covered entity, then the EHR system developer could potentially face HIPAA liability (as a business associate of a HIPAA covered entity) for any impermissible uses and disclosures of the health information received by the app.

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?

- An app's facilitation of access to the individual's ePHI at the individual's request alone does not create a business associate relationship. Such facilitation may include API terms of use agreed to by the third-party app (i.e., interoperability arrangements).

- HIPAA does not require a covered entity or its business associate (e.g., EHR system developer) to enter into a business associate agreement with an app developer that does not create, receive, maintain, or transmit ePHI on behalf of or for the benefit of the covered entity (whether directly or through another business associate).

- If the app was developed to create, receive, maintain, or transmit ePHI on behalf of the covered entity, or was provided by or on behalf of the covered entity (directly or through its EHR system developer, acting as the covered entity's business associate), then a business associate agreement would be required.