Published: May 29, 2019

HIPAA FAQs for Health Apps

Charmaine Naut | Capital Management Enterprises, Inc | 610-265-9677 | cnaut@cme-group.com

Technological advancements over the last several years have made it easier than ever for employers and employees to collect, store, manage, organize, or transmit health information via applications and other software (collectively, "apps"). The Office of Civil Rights ("OCR"), the entity responsible for enforcing the Health Insurance Portability and Accountability Act ("HIPAA"), recently issued FAQs concerning HIPAA's applicability to apps. The FAQs clarify that once protected health information ("PHI") has been received by an app that is neither a covered entity nor a business associate, the information is no longer subject to the protections of the HIPAA rules.

Overview

Health plans are considered covered entities under HIPAA and must comply with HIPAA's Privacy and Security Rules. Briefly:

- The rules prohibit covered entities and business associates from using or disclosing PHI when not for treatment, payment, or health care operations purposes without participant authorization. Covered entities and business associates are also prohibited from using or disclosing more information than necessary and must keep PHI safe.

This document is designed to highlight various employee benefit matters of general interest to our readers. It is not intended to interpret laws or regulations, or to address specific client situations. You should not act or rely on any information contained herein without seeking the advice of an attorney or tax professional. ©2019 Emerson Reid, LLC. All Rights Reserved. CA Insurance License #0C94240.

- "Business Associates" include various third-party vendors who create, store, use, transmit, or access PHI on behalf of the group health plan. Wellness vendors and cloud providers that use PHI for functions such as consulting and analyzing health plan data are business associates. As such, the group health plans must have business associate agreements in place with these vendors before PHI may be shared.

- PHI is health information created or received by a covered entity or employer which relates to the health or payment for health care of an individual and identifies the individual (or the information can be used to identify the individual).

- The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that "covered entities" must put in place to secure individuals' electronic PHI ("ePHI").

HIPAA FAQs for Health Apps

Recently, OCR issued guidance in the form of FAQs to address common questions concerning HIPAA compliance related to the use of third-party health apps. Notably, the FAQs clarify the following:

- 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 under HIPAA, the information is no longer subject to the protections of the HIPAA Rules. In other words, if the individual's app 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 should not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app.

- If, on the other hand, 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.

Under HIPAA's individual right of access, individuals can direct a covered entity to transmit their ePHI to a third-party app in an unsecure manner or through an unsecure channel. The FAQs established that a covered entity transmitting ePHI to a third-party app via an unsecure manner or channel will not be responsible for unauthorized access to the ePHI while in transit, so long as the transmission was at the individual's request. For example, an individual may request his or her unencrypted ePHI be transmitted to an app as a matter of convenience. In this case, the covered entity would not be responsible for unauthorized access to the ePHI while in transmission to the app. However, the OCR specified that in this situation, the covered entity should advise the individual of the potential risks involved the first time the individual makes the request.

Finally, the OCR stressed that a covered entity is not allowed to refuse to disclose ePHI to an app chosen by an individual, even when the covered entity is concerned about the app's security or how the app will use or disclose the ePHI. The HIPAA Privacy Rule broadly prohibits covered entities from refusing to disclose ePHI to a third-party app selected by the

This document is designed to highlight various employee benefit matters of general interest to our readers. It is not intended to interpret laws or regulations, or to address specific client situations. You should not act or rely on any information contained herein without seeking the advice of an attorney or tax professional. ©2019 Emerson Reid, LLC. All Rights Reserved. CA Insurance License #0C94240.

individual, if the ePHI is "readily producible in the form and format used by the app." For example, a covered entity is not permitted to deny an individual's request to transmit their ePHI to a third-party app because the app does not encrypt the ePHI when stored in the app.

Employer Action

Employers, as plan sponsors of a health plan, should understand their responsibility under HIPAA as a covered entity and their relationship with any technology used to create, receive, maintain, or transmit ePHI. Accordingly, it is important for employers to:

- Be aware that technology offered to employees through the group health plan is likely subject to the HIPAA Privacy and Security Rules.
- Ensure any third-party vendors who transmit create, store, use, transmit, or access PHI on behalf of the group health plan understand their responsibilities under the HIPAA Privacy and Security Rules and confirm there are business associate agreements in place with these vendors.
- Abide by HIPAA's individual right of access, which allows individuals to direct their ePHI to any third-party app and request the ePHI be transmitted using an unsecure method or channel.

This document is designed to highlight various employee benefit matters of general interest to our readers. It is not intended to interpret laws or regulations, or to address specific client situations. You should not act or rely on any information contained herein without seeking the advice of an attorney or tax professional. ©2019 Emerson Reid, LLC. All Rights Reserved. CA Insurance License #0C94240.