Expert Q&A on HIPAA Compliance for Group Health Plans and Wellness Programs That Use Health Apps

PRACTICAL LAW EMPLOYEE BENEFITS & EXECUTIVE COMPENSATION

Search the Resource ID numbers in blue on Westlaw for more.

An Expert Q&A with Shannon Rushing of Dechert LLP addressing the use of health apps and compliance considerations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Employer group health plans and other entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are increasingly relying on health apps that encourage employees to lead healthier lifestyles and reduce health claim costs. However, the use of health apps raises important compliance considerations under HIPAA. Practical Law asked Shannon Rushing of Dechert LLP to explain how HIPAA applies to health information that is created, managed, or organized through health apps.

Ms. Rushing concentrates her practice on employer group health plan and health care provider compliance matters. Ms. Rushing has significant experience advising covered entities and business associates on privacy and security issues relating to HIPAA compliance. Ms. Rushing also advises employers on their health and welfare plans and retirement plans.

Is all health information received in connection with employer-provided benefits protected under HIPAA?

A common misconception is that all health information received by an employer is subject to HIPAA. For HIPAA compliance purposes, the key distinction is whether the information is created, received, or maintained in connection with an employer's group health plan.

HIPAA governs the privacy and security of protected health information (PHI), which is individually identifiable health information that is created, received, or maintained by a HIPAA covered entity, or on a covered entity's behalf by a business associate (for example, a third party administrator or wellness vendor), and that relates to an individual's past, present, or future physical or mental health or condition (see Practice Note, HIPAA Privacy Rule: Types of Information Covered By the Privacy Rule (4-501-7220)).

HIPAA covered entities include:

- Health plans (for example, employer-sponsored group health plans, health insurance companies, and health maintenance organizations (HMOs)).
- Health care providers that conduct electronic transactions (for example, hospitals, doctors, medical clinics, psychologists, dentists, nursing homes, or pharmacies) (see Practice Note, HIPAA Electronic Transactions Under the ACA (9-517-3369)).
- Health care clearinghouses.

(45 C.F.R. § 160.103; see Practice Note, HIPAA Privacy Rule: Entities Subject to the Privacy Rule (4-501-7220).)

Employers may receive health information in connection with administering other employee benefits (for example, workers' compensation claims, disability claims, or life insurance) that are not maintained by the group health plan and therefore are not subject to HIPAA compliance.

Employers that sponsor group health plans and related wellness programs face new issues involving how and when HIPAA applies to health information that plan participants create, manage, or organize using a health app.

What guidance is available regarding HIPAA's applicability to health apps?

In February 2016, the Department of Health and Human Services (HHS) issued guidance in the form of "Health App Use Scenarios" (HHS Scenarios) addressing how HIPAA applies to health information that is created, managed, or organized through the use of a health app, including limited guidance applicable to health plans. (HHS Office for Civil Rights, Health App Scenarios & HIPAA (2016).)

The HHS Scenarios were intended to assist an app developer in determining when it may be required to comply with HIPAA. However, the HHS Scenarios may be instructive for employers that sponsor group health plans and wellness programs in determining whether and when the use of health apps by their employees requires compliance with HIPAA's administrative simplification provisions (see Practice Note, Wellness Programs (6-518-5321)). (As background, HIPAA's administrative simplification provisions include privacy,

security, and breach notification requirements, as well as standards for transactions and code sets used in electronic transactions. For more information on these HIPAA compliance obligations, see the HIPAA Toolkit (7-502-6708).)

Is all information created, received, or maintained on a health app subject to HIPAA?

No. HHS has distinguished between health apps that are offered:

- Directly to individuals as consumers.
- On behalf of a covered entity (such as a health plan or health care provider).

(See Health App Use Scenarios & HIPAA, at 3-4.)

Under the HHS Scenarios, an employer should consider three threshold questions in evaluating whether HIPAA applies in the health app context. First, the employer should consider whether the health app creates, receives, maintains, or transmits identifiable information. The second question is whether the health app was independently selected by an individual plan participant or employee (for example, an individual consumer) and, if so, whether the individual controls all decisions about whether to transmit his data to a covered entity or one of its business associates. Third, the employer should consider whether the health plan or health insurance company (or business associate acting on its behalf) has a relationship with or directly pays for services provided in connection with the health app.

A related consideration is whether the health plan or health insurance company (or business associate acting on its behalf) directs the health app, health app service provider, or app developer to create, receive, maintain, or disclose information related to a health plan participant.

HHS has clarified that if an individual consumer (for example, a plan participant) independently selects an app, and the consumer can control all decisions about whether to transmit his data to a third party, then the health information is not subject to HIPAA. (Health App Use Scenarios & HIPAA, at 3-4.)

If a health plan recommends that plan participants use a health app that provides wellness tools (for example, tracking the participant's progress toward improving health), will use of the app trigger HIPAA compliance obligations?

Health plans are taking advantage of the digital health trend to promote employees' active involvement in their own health (and thereby reduce health plan costs). For example, a health plan might recommend use of a health app that offers wellness tools to monitor blood pressure, achieve fitness and nutrition goals, or track overall progress toward improved health.

This situation may trigger HIPAA compliance obligations, depending on the specific facts and circumstances. The issue is whether recommending use of an app creates a business associate relationship between the app developer and the health plan. If the health plan pays the app developer for use of the app and directs the app developer to create, receive, maintain, or disclose information related to its health plan participants, the app developer likely is acting as the health plan's business associate. As a result, HIPAA would protect the health information being created, received, maintained, or transmitted by the app.

One of the HHS Scenarios describes a similar fact pattern that involves a doctor as the covered entity, rather than a health plan. In the scenario, a patient downloads an app that is recommended by his doctor to help manage a chronic condition. The patient populates the app and directs it to transmit the information to his doctor's electronic health record. According to HHS, the information is directed on the consumer's behalf and this activity does not create a business associate relationship between the app developer and the doctor.

A key distinction, which may apply to employer-sponsored health plans, is whether the recommendation to use the app is based on either:

- Confidence that the app is a useful tool to assist plan participants in engaging in healthier lifestyles for their independent use.
- A paid or contractual relationship between the health plan and app developer, which makes it more likely that the app developer is a HIPAA business associate.

Assume the same situation as in the previous question, except that health information is monitored by or provided directly to a third-party wellness vendor that uses data tracked in the health app to determine eligibility for certain incentives offered under an employer-sponsored wellness program. Is HIPAA compliance required?

If a wellness program is offered in connection with an employer-sponsored group health plan, then individually identifiable health information received in connection with the wellness program is subject to HIPAA's compliance obligations. (Health App Use Scenarios & HIPAA, at 3.)

Third-party wellness vendors that create, receive, maintain, or transmit health information in connection with an employer group health plan therefore must sign a business associate agreement with the group health plan (see Standard Document, HIPAA Business Associate Agreement (3-501-6706)). If the wellness vendor in turn contracts with a third-party app developer to assist with collecting PHI, then the app developer is considered a downstream business associate of the wellness vendor. As a result, the wellness vendor must enter into a business associate agreement with the app developer that complies with the restrictions and conditions agreed to in the upstream agreement with the group health plan (45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2)).

From a HIPAA compliance perspective, is there a difference between the following two apps: (1) a health app offered in connection with a fully-insured group health plan that allows plan participants to request, download, and store health plan records and check the status of claims and coverage decisions; and (2) the direct-to-consumer version of this same app that allows individuals to store, manage, and organize their health records, improve their health habits, and send health information to providers?

Yes, in one of the examples in the HHS Scenarios, the agency distinguished between apps that appear to be the same except that:

- One version is offered in connection with the health plan.
- The other version is offered directly by the app developer as a direct-to-consumer version.

The app developer need not apply HIPAA's protections to the consumer information obtained through the direct-to-consumer app version if the following conditions are met:

- The health app is not provided on behalf of a covered entity (or its business associate).
- The app developer keeps the health information attached to the two versions completely separate, so that information from the direct-to-consumer version is not part of the product offered by the health plan.

(Health App Use Scenarios & HIPAA, at 3.)

What are the consequences of a breach of unsecured PHI involving the transfer of health plan-related data from the app developer to the group health plan?

As a business associate, the app developer has regulatory obligations and is directly liable under HIPAA if it uses or discloses PHI in a manner not authorized by the business associate agreement, required by law, or otherwise permitted under the HIPAA privacy rule. The app developer also is directly liable if it fails to either:

- Safeguard electronic PHI under the HIPAA security rule (see Practice Note, HIPAA Security Rule (5-502-1269)).
- Notify the group health plan of the discovery of a breach of unsecured PHI (see Practice Note, HIPAA Breach Notification Rules for Group Health Plans (1-532-2085)).

Under HIPAA's regulations, an employer group health plan also has its own HIPAA compliance and breach notification obligations. However, before entering into a business associate agreement with a health app developer, it is best practice for the group health plan to conduct due diligence to ensure that the app developer has mechanisms in place to protect participants' PHI consistent with HIPAA. For example, this may include requesting the health app developer's most recent risk analysis and risk management plan conducted under HIPAA's administrative safeguards and implementation specifications (under 45 C.F.R. Section 164.308). The plan also may request information about the encryption mechanisms used by the health app developer to protect the security of electronic data and secure transfer of health plan-related data (see Practice Note, HIPAA Enforcement and Group Health Plans: Penalties and Investigations: Examples of Resolution Agreements (2-519-1055)).

Additionally, a group health plan should consider including in the business associate agreement an audit provision giving it the right to review or request proof of ongoing HIPAA compliance mechanisms (see Standard Document, HIPAA Business Associate Agreement (3-501-6706)). These steps will help ensure the security of electronic PHI, prevent breaches, and avoid potentially expensive enforcement settlements following an HHS investigation.