MY BENEFIT ADVISOR

Potential HIPAA Privacy Concerns for Employers Offering Mobile Apps

Issued date: 06/06/17

In an effort to help employees lead healthier lives, employers may offer employees access to mobile device applications ("apps") that collect, store, manage, organize, or transmit health information. Nutrition and weight could be logged. Health-tracking "wearables" such as Fitbits might, for example, monitor heart rate, calories burned, sleep quality, and fitness level. Other apps may send information to the employer's health plan for monitoring, continuity of care, or case management purposes in an effort to improve employee health and well-being and potentially reduce health care costs.

App as Part of the Health Plan

Health plans are considered "covered entities" under the Health Insurance Portability and Accountability Act ("HIPAA"). Covered entities must comply with the HIPAA Privacy and Security Rules. If an employer decides to integrate certain apps with the health plan, the employer should be aware of the various HIPAA issues and address them accordingly. Briefly:

- The rules prohibit covered entities and business associates from using or disclosing protected health information ("PHI") when not for treatment, payment, or health care operations purposes without participant authorization. Covered entities are also prohibited from using or disclosing more information than necessary and must keep PHI safe.
- "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.
- Business associates may delegate responsibilities to subcontractors. In this case, the business associate is responsible for the subcontractor's compliance. For example, a wellness company may be a business associate of a group health plan. The wellness company has a subcontractor agreement with an app developer. The wellness company is responsible for the subcontractor's compliance with HIPAA.
- 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).

Recently, HHS's Office for Civil Rights, the entity responsible for enforcing HIPAA's privacy and security rules, issued guidance on apps.

Example

A health plan offers a health mobile app that allows participants to download and store their health records, check claim status, and track their progress towards improving their health. The usage data is collected and analyzed by the health plan. The app developer offers a separate version of the app that is available directly to the consumer with the same functionality.

Conclusion

Since the health plan is a covered entity and is contracted directly with the app developer to create, receive, maintain, and transmit PHI on behalf of the plan, the app developer is a business associate and is subject to HIPAA with respect to the app offered by the health plan.

The employer's relationship could instead be with the wellness vendor who purchases the app from the developer. In this case, the wellness vendor would be the business associate. The developer may be considered a subcontractor of the wellness vendor.

App Not Part of the Health Plan

On the other hand, some employers sponsor wellness activities unrelated to their group health plan. For example, an employer could provide employees with step counters and award prizes to employees with the most steps taken during a month. This program likely would not fall within HIPAA's purview.

Employer Action

- Be aware that technology offered to employees that coordinates with the group health plan is likely subject to the HIPAA Privacy and Security Rules.

- Understand the flow of health information. Information could, for example, be transmitted from the user's smartphone to a website. Next, that website may transmit the data to a wellness vendor who collects and analyzes the data on behalf of the group health plan.

- Ensure the vendors contracting with the health plan understand their responsibilities under the HIPAA Privacy and Security Rules. This includes having safeguards in place to protect users' PHI such as encryption protocols.

- Confirm there are business associate agreements in place with those vendors. The agreements, in part, should make assurances that safeguards are in place and describe the breach notification process. Per OCR guidance, a covered entity must have a business associate agreement must be in place before allowing a business associate access to its PHI.

- Ensure employers do not receive any PHI from a third party vendor. To the extent that an employer wants to analyze information collected from participants' apps, it can receive that information from the vendor on an aggregated and de-identified basis.

Other Considerations

Other applicable laws not addressed in this article could include state privacy laws and other federal laws such as those enforced by the Federal Trade Commission. Employers should understand that other types of sensitive information could be collected and transmitted by these apps such as social security numbers and an employee's exact location (e.g., through GPS tracking). This information should also be protected.