Now & Next
Benefits Alert

October 20, 2023

Fiduciary governance: HIPAA and cybersecurity best practices

By **Damian A. Myers, Yelena Gray, Lena Gionnette, and Annie Zhang**

Learn more about the laws aimed at protecting sensitive data and best practices for handling employees' personally identifiable information in connection with their benefit plans.

What's the impact?

- Plans considered "covered entities" under HIPAA are subject to privacy and security rules governing individually identifiable health information.
- Plan sponsors must implement their plans' physical, administrative, and technical safeguards to protect e-PHI against cyberthreats.
- Fiduciaries should not stop at HIPAA-covered health data but should equally safeguard any personally identifiable information of employees in connection with their welfare benefit plans.

We shift gears in our Health & Welfare Fiduciary Governance Series to focus on an area of oversight and compliance that is essential in today's digital age. The importance of staying abreast of Health Insurance Portability and Accountability Act (HIPAA) compliance and cybersecurity best practices cannot be overstated as employers and health plan fiduciaries strive

to safeguard sensitive participant information from theft, breaches, and unauthorized access by increasingly sophisticated hackers and other bad actors.

Group health plans must comply with several laws aimed at protecting the sensitive data in their purview, including HIPAA, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Genetic Information Nondiscrimination Act (GINA), among others. HIPAA, as amended by HITECH, provides the most robust framework for group health plans to protect the protected health information (PHI) and electronic PHI (e-PHI) they use, maintain, and disclose in the course of plan administration.

In addition, the Department of Labor (DOL) has published guidance on cybersecurity best practices applicable to group health plans. Further, the Office for Civil Rights (OCR), the arm of Health and Human Services charged with enforcing HIPAA's privacy and security rules, has recently undertaken several significant enforcement actions against group health plans for HIPAA violations.

Cybersecurity concerns are undoubtedly fiduciary concerns. We discussed at length in prior installments of this series that plan fiduciaries owe a duty of prudence to participants and beneficiaries and must put the interest of participants and beneficiaries above all others, as a prudent person (or, indeed, a prudent expert) would do in similar circumstances. Safeguarding participants' and covered dependents' health data should, thus, be one of the top priorities for fiduciaries, and they need to take the utmost care in fulfilling this obligation on behalf of the individuals covered by their group health plans.

This alert will focus on the measures plan fiduciaries need to take to comply with HIPAA's privacy and security rules, including best practices fiduciaries should implement to adequately protect group health plan data. Fiduciaries should not stop at HIPAA-covered health data but should equally safeguard any personally identifiable information of employees in connection with their welfare benefit plans.

HIPAA Privacy and Security Rules

PLANS SUBJECT TO HIPAA'S PRIVACY AND SECURITY RULES

In implementing measures to ensure compliance with HIPAA's privacy and security rules, health plan fiduciaries need to first consider the following:

- What, exactly, constitutes PHI and e-PHI:
- Whether their plan is a covered entity subject to these requirements: and
- How PHI and e-PHI flow within, to, and from the plan.

PHI is individually identifiable health information that is transmitted or maintained by or on behalf of a covered entity, and e-PHI is the subset of PHI that is transmitted or maintained by or

in electronic media. Electronic media includes hard drives, flash drives, mobile devices, intranets, and cloud-based technologies. Some examples of PHI/e-PHI in the group health plan context include, among other things, any of the following items that commonly contain PHI/e-PHI: participant claims, explanations of benefits, medical flexible spending account (FSA) reimbursements, and provider bills. HIPAA's security requirements are a more targeted version of its privacy rule, applicable only to e-PHI, while its privacy rule applies more broadly to all PHI.

Notably, individually identifiable health information is not PHI (or e-PHI) when a plan sponsor holds the information in employment records solely in its role as an employer (e.g., for drug screening purposes, sick leave requests, and the like). That information may nevertheless be protected under other federal regulatory schemes or state laws.

The types of plans that are considered "covered entities" subject to HIPAA's privacy and security rules include most self-insured and some fully insured group health plans consisting of, generally, medical, prescription drug, dental, and vision benefits, medical FSAs, and employee assistance programs (EAPs). As covered entities, these plans need to ensure that PHI/e-PHI is used and disclosed only in accordance with the rules.

Generally, fully insured plans that do not create or receive PHI/e-PHI, other than summary health information or enrollment information, are not subject to the privacy and security rules with some very limited exceptions. Instead, the insurance carriers must comply with HIPAA as the covered entity. Nor are self-insured, self-administered plans (i.e., those plans that do not rely on a third-party administrator) with fewer than 50 employees. However, even though HIPAA may not apply to these plans, sponsors or administrators of these plans should stay abreast of cybersecurity best practices to meet their fiduciary obligations to participants and beneficiaries.

INITIAL ASSESSMENTS

Plan fiduciaries would be well advised to take the time to conduct an initial analysis of the current compliance landscape of their covered plan(s). As a first step, plan sponsors should examine the flow of PHI/e-PHI within and with respect to their covered plan. For example, plan sponsors should examine how PHI/e-PHI is handled and stored in relation to a covered plan's enrollment process, COBRA administration, claims assistance, and claims payments. Further, payroll processing should be looked at to see whether and how PHI/e-PHI is implicated. It is also a good practice to document all of the covered entity's service providers, known as "business associates," that have access to PHI/e-PHI and use or disclose it on behalf of the plan. Business associates run the gamut from medical, dental, vision, and FSA third-party administrators, EAP providers, consultants and attorneys, and brokers to payroll vendors, IT consultants, and document shredding and storage contractors and are held to the same standards as covered entities in safeguarding, using, and disclosing breaches of PHI/e-PHI.

Finally, plan sponsors should look at how PHI/e-PHI is currently stored and disposed of to assess the adequacy of their current safeguards. For instance, is PHI stored in secured areas and under

lock and key? How are computer and printer hard drives secured? Is e-PHI available on mobile devices, and if so, what are the security measures in place on the mobile devices? Is two-factor authentication required to access e-PHI? The answers to these questions will help guide plan sponsors as to the additional safeguards they may need to implement, as further described in the "Safeguards and Cybersecurity Best Practices" section below.

To reduce the risk of mishandling PHI, the sponsors of most self-insured plans take a hands-off approach and arrange so that no employees of the employer have access to PHI, and only claims processing entities, brokers, and health benefit consultants may access PHI to the extent necessary to perform services for the plan.

POLICIES, PROCEDURES, AND DOCUMENTATION

Once plan fiduciaries determine that HIPAA's privacy and security rules apply to a covered plan and assess the current landscape of how PHI/e-PHI is used and accessed within and involving the plan, they should work with counsel to analyze, implement, and document the following HIPAA-compliant policies and procedures:

- **Creation of a privacy and breach notification policy:** Prepare and document a broad policy that outlines the sponsor's plans subject to HIPAA's privacy rule, describes the permitted and required disclosures of PHI and safeguards in place, summarizes the plan's breach notification policy if and when unauthorized disclosures of PHI occur, sets forth the responsibilities of the privacy officer (described below), outlines the sponsor's policy on employee HIPAA training, and provides information on how individuals can access their own PHI.
- **Designation of a privacy and security officer**: Designate an individual (or individuals) to oversee compliance with HIPAA's privacy and security rule and the covered entity's privacy and breach notification policy and memorialize the designation in writing. In some cases, it may make sense to have separate privacy and security officers.
- **Plan document required language:** Ensure that plan documents include HIPAA-required language pertaining to the privacy and security rules.
- **Creation of a notice of privacy practices**: Prepare a HIPAA and HITECH-compliant notice of privacy practices for the covered plan that outlines the permitted and required uses and disclosures of PHI and individuals' rights with respect to their PHI and ensure the notice is distributed in accordance with the rules.
- **Business associate agreements:** Ensure that the covered entity has a specific HIPAA and HITECH-compliant agreement in place with every single business associate. Agreements should be periodically reviewed to ensure continued compliance, especially if and when updated HIPAA rules are released. Business associate agreements set forth contractual obligations of the parties dealing with PHI and should not be signed (particularly if drafted

by a third-party service provider) without careful review and negotiations.

- **Ongoing HIPAA training:** Authorized employees should be adequately trained on HIPAA policies and procedures upon hire and on a periodic basis thereafter.
- **Creation of a written information security policy:** Prepare and document a broad policy that outlines the plans subject to HIPAA's security rule, summarizes the plans' risk analysis and risk management with respect to e-PHI, describes the security officer's responsibilities, describes the permitted and required disclosures of e-PHI and the safeguards in place, and summarizes the plans' breach notification policy.

SAFEGUARDS AND CYBERSECURITY BEST PRACTICES

In its security policy, a plan sponsor must describe the physical, administrative, and technical safeguards it has in place to protect its plans' e-PHI. Appropriate safeguards are crucial as more and more health plan data are digitized. It is no secret that we live and operate in a digital world vulnerable to attacks and theft. Group health plans are no exception, and health plan data is an extremely valuable commodity to hackers. The data contains financial information, demographic information, health history, and often, Social Security information that can be accessed and sold on the dark web. Of late, sophisticated cybercriminals have accessed plan data by posing as participants or beneficiaries and obtaining credentials to log into a participant's account.

The threat of participant complaints and OCR enforcement alone should encourage plan sponsors to adhere to HIPAA's privacy and security rules. But beyond that, real dollars are at stake when data breaches occur, as a plan sponsor's reputation is on the line, and the plan and fiduciaries become vulnerable to class action lawsuits. Further, given the fiduciary implications, protecting participant data should be performed under the highest standard of care. Therefore, plan fiduciaries should armor themselves with the latest and greatest in cybersecurity best practices in developing their HIPAA-compliant security programs.

Covered entities developing HIPAA-compliant security programs have several resources at their disposal, including the Department of Labor's guidance outlining cybersecurity program best practices. In addition, depending on the size of a plan sponsor's business, it may be able to leverage its existing cybersecurity efforts and apply them to the covered plans.

Plan sponsors should also strongly consider purchasing cyber liability insurance for their plans. Data breaches and cyberattacks are generally not covered by a company's existing insurance policies. Plan sponsors should weigh the relatively high cost of this insurance against their current safeguards and practices to determine whether cyber liability insurance will operate to effectively address any gaps.

In addition, plan sponsors should ensure that their service agreements with group health plan third-party administrators and other vendors include current market terms for cybersecurity best practices. In negotiating these agreements, plan sponsors should ensure that vendors and their

subcontractors commit to complying with industry standards and best practices, notifying plan sponsors of any cybersecurity breaches, making participants whole for any losses, and allowing periodic audits of their controls and systems.

We outline here several best practices for implementing appropriate safeguards:

- **Physical safeguards to protect onsite PHI/e-PHI:**
  - Require visitors to a plan sponsor's facilities to check in and do not leave them unattended.
  - Require key card access to enter the facilities.
  - Ensure that cabinets and rooms containing PHI are always locked and that locks are regularly checked.
  - Require laptops to always be secured via password and set to a locked screensaver after a period of inactivity.
  - Require individuals with access to e-PHI to use a privacy screen on their computers so unauthorized individuals cannot view the information on their screen.
- **Technical safeguards to protect and control access to e-PHI**:
  - Access to e-PHI should be blocked after multiple unsuccessful attempts to gain access.
  - Passwords should be complex and consist of a lengthy combination of alpha-numeric characters and symbols, and they should be required to be changed frequently.
  - Multi-factor authentication is encouraged where possible.
  - Data on laptops, USB drives, email messages, and other external media should be encrypted so it is unreadable without the use of a confidential process or key.
  - The covered entity should implement and manage a secure system development life cycle (SSDLC) program.
- **Administrative safeguards to limit access to e-PHI:**
  - The covered entity's security officer (if different from the privacy officer) should be the only individual authorizing individuals' access to systems containing e-PHI, and that access should be limited only to those individuals who require it for legitimate business purposes.
  - The plan sponsor's information technology department should maintain and review system logs.
  - Anti-virus and anti-spyware software should be maintained and routinely updated, with no opt-outs.
  - Employees should be regularly trained on cybersecurity awareness to avoid data security breaches, and records should be kept of such training.
  - The covered entity should ensure that any data stored in a cloud or managed by a third-party service provider is subject to appropriate security reviews and independent security assessments.
  - The covered entity should regularly conduct third-party audits of security controls to expose any risks, vulnerabilities, and weaknesses and appropriately address them.

Takeaways

As described above, health plan fiduciaries are tasked with a number of compliance action items to ensure they fulfill their fiduciary responsibility to protect participant and beneficiary data and comply with the various laws governing data protection. These measures generally include developing a robust HIPAA compliance system of policies and procedures; following the latest cybersecurity standards; ensuring health plan providers adhere to strict data security protections; negotiating appropriate business associate and data security agreements with plan vendors and training employer personnel in approaching protected and sensitive information.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Damian A. Myers
202.585.8485
dmyers@nixonpeabody.com

Yelena F. Gray
312.977.4158
yfgray@nixonpeabody.com

Lena Gionnette
585.263.1669
lgionnette@nixonpeabody.com

Annie Zhang
202.585.8606
azhang@nixonpeabody.com