HIPAA 101

For Employers

November 2023

© 2023 Benefit Comply, LLC

Table of Contents

While every effort has been taken in compiling this information to ensure that its contents are totally accurate, neither the publisher nor the author can accept any liability whatsoever for any inaccuracies or changed circumstances of any information herein or for the consequences of any reliance placed upon it. This publication is distributed on the understanding that the publisher is not engaged in rendering legal, accounting or other professional advice or services. Readers should always and without exception seek professional advice before entering into any commitments.

Introduction to This Guide

Employers often ask exactly what compliance with HIPAA privacy and security requirements entails. Is it enough to have a Notice of Privacy Practices? To train employees? To have a business associate agreement in place with a TPA? It's not uncommon for employers to have addressed a piece or several pieces of HIPAA privacy and security compliance but be missing a comprehensive compliance solution. Often, confusion stems from things like not understanding which plans are subject to HIPAA; not knowing how HIPAA applies to self-funded and fully-insured plans; and not understanding what protected health information (PHI) is or the types of PHI the employer interacts with for purposes of administering its health plan.

We have developed this guide to address the most common sources of confusion for employers in the broader context of explaining how HIPAA privacy and security requirements apply to employers.

HIPAA Privacy & Security: A Brief Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations ("Privacy Rule," "Security Rule," "Enforcement Rule," and "Breach Notification Rule") established standards for the privacy and security of individually identifiable health information (protected health information, or PHI). These standards apply to covered entities, which include the health plans sponsored by employers for their employees, and many of the requirements also apply to business associates (third parties who provide plan administration services that involve interaction with PHI).

HIPAA in Three Parts

There are three main areas of focus for HIPAA compliance purposes:

1. HIPAA privacy requirements, as articulated in the Privacy Rule, that are primarily concerned with appropriate uses and disclosures of PHI, individual rights with respect to PHI, and plan obligations with respect to safeguarding PHI.
2. HIPAA security requirements, as articulated in the Security Rule, that are primarily concerned with the confidentiality, integrity, and availability of electronic PHI (ePHI) and include completion of a security risk analysis; and
3. HIPAA breach notification and reporting requirements, as articulated in the Breach Notification and Reporting Rule, that establish standards for identification, reporting, and notification of breaches of unsecured PHI.

This guide will cover each of these parts and will also discuss the current regulatory enforcement and oversight environment and the potential penalties that may be assessed for non-compliance.

© 2023 Benefit Comply, LLC

A Note on Terminology

Throughout this guide, the terms “plan sponsor” and “employer” are generally used interchangeably. For simplicity’s sake, the term “employer” is used most often. Readers should keep in mind that any references to “employer” means the employer in its capacity as plan sponsor of a health plan subject to HIPAA.

© 2023 Benefit Comply, LLC

HIPAA Privacy

Overview of Requirements for Employers

Employers sponsoring health plans for their employees must make sure those health plans, as covered entities, operate in compliance with HIPAA privacy requirements. Specifically, employers should:

1. Conduct an inventory of all PHI used to administer the health plan, documenting where the information is stored, how it is transmitted, and who has access to it.
2. Develop a set of written policies and procedures that addresses the plan's use and disclosure rules; handling of individual rights requests including complaints; and documentation of compliance with specific administrative requirements, such as a sanctions process and employee training.
3. Name a Privacy Official.
4. Develop and distribute a Notice of Privacy Practices.
5. Develop and implement safeguards for protecting PHI from improper use and disclosure.
6. Ensure the health plan document (typically an ERISA wrap document) contains language permitting the plan to share PHI with the employer/plan sponsor; and
7. Identify business associates and ensure proper agreements are in place.

Inventory of PHI

A critical component of HIPAA compliance is the process of thoroughly accounting for the PHI that the employer interacts with for purposes of administering the health plan. This is important for several reasons, but at a fundamental level an employer cannot appropriately implement safeguards to protect PHI without having a full understanding of exactly where PHI exists and who has access to it. Therefore, the first step an employer should take for purposes of HIPAA compliance is to conduct a thorough inventory of PHI, including how it flows through the organization, where it is stored, who has access to it, and who it is shared with. For this purpose, an employer must consider:

Definition of Protected Health Information ("PHI")

PHI refers to "individually identifiable health information" that is received, maintained, or transmitted by a covered entity (i.e., a health plan).

"Health information" relates to the past, present, or future treatment of an individual. Coverage by a health plan is considered health information. Therefore, once any piece of individually identifiable information related to an

© 2023 Benefit Comply, LLC

individual's enrollment in a health plan "touches" (i.e., is received by) the health plan (TPA or carrier), that information becomes PHI.

Examples of PHI include data related to enrollment, eligibility, premiums, claims, utilization, and underwriting. It is important to note that PHI does not just refer to claims, treatment, or diagnostic information. Any piece of individually identifiable information, once it has been transmitted to the health plan for processing, is considered PHI. Therefore, when employers are interacting with a piece of individually-identifiable information, they should consider: 1) whether it is coming from health plan records; and/or 2) whether it is being used in some way related to plan administration.

FAQ: Does every piece of individually identifiable medical information an employer interacts with constitute PHI?

No. Only information that has been transmitted to (i.e., has "touched") the health plan is considered PHI. Information collected for other purposes (e.g., employment) and/or outside the scope of the health plan is not considered PHI, even if it looks identical to PHI. Examples of information that may look like PHI but really is not include:

- Drug testing results an employer may collect at the point of hire.
- Vaccine information an employee submits as part of worksite opening/closing decisions.
- Medical information an employee submits along with a disability or FMLA claim; and
- Information an employee voluntarily shares with a co-worker (e.g., pregnancy, upcoming surgery, etc.).

It is important to keep in mind that even when information is not considered PHI, it may still be subject to other confidentiality requirements – e.g., Human Resources law or the Americans with Disabilities Act. Therefore, employers should still treat the information carefully. However, HIPAA's specific privacy and security protections would not apply.

Example 1: An employee tells their manager that they are going in for surgery. Although the information being provided is health information and is individually identifiable, it does not constitute PHI because it is not connected to the health plan (i.e., is not coming from health plan records or being used for some purposes related to plan administration). Therefore, in this context, it is not PHI and HIPAA does not apply (although other confidentiality laws, such as the Americans with Disabilities Act, may protect that information in other ways).

Example 2: Several employees are responsible for coordinating leave of absence requests, including handling the medical information that is submitted along with such requests. The Human Resources Manager is trying to decide if these employees should receive HIPAA privacy training. Although these

employees may encounter individually identifiable health information, this information is likely being provided directly by the employee or by a provider (not from health plan records), and because leave benefits are not considered health plans subject to HIPAA, the information would not be considered PHI in this context. (Note also that these employees should not be gathering substantiation information from health plan records without first getting written authorization in place, as individually identifiable health information coming from health plan records would be considered PHI and using PHI for purposes other than health plan administration is generally not permitted.)

FAQ: Does HIPAA prevent an employer from asking about vaccination status?

No, generally, HIPAA will not stand in the way of an employer collecting vaccine information from employees; it will simply impact how an employer may use that information. The HHS Office for Civil Rights (OCR) has issued a set of FAQs to address questions about when and how the HIPAA Rules apply to uses and disclosures of COVID-19 vaccination-related information. However, the information in the FAQs concerning the HIPAA Rules is applicable to all vaccinations, regardless of the disease or condition being addressed or whether the vaccine has been fully approved or authorized via an emergency use authorization

Special Considerations for Enrollment Information

Enrollment information becomes PHI once it has "touched" the health plan (e.g., been transmitted to the TPA or insurance carrier via a file transfer). At the point when an employer collects enrollment data from its employees, that information has not yet become PHI because it hasn't connected with the health plan. Remember that PHI refers to individually identifiable information that is "received, maintained, or transmitted" by a covered entity (i.e., health plan). There needs to be that point of connection for individually identifiable health information to become PHI.

This distinction is both straightforward and confusing. If employers maintain enrollment information that they have gathered at the point of enrollment in their own benefits administration systems, and also transmit that enrollment information to their health plan, then how is it possible to distinguish between the enrollment data that is not PHI and enrollment data that is?

There are no perfect answers to this question, but the conservative approach is for employers to simply assume that all enrollment data is PHI and apply appropriate safeguards accordingly. This is much easier than trying to parse out a point in time with respect to a particular piece of data and when exactly it becomes PHI. But it is equally important to keep this technical distinction in mind – for example, if a benefits administration system is breached, there may be an argument that no HIPAA violation occurred if that system only contains enrollment information gathered from the employer at the point of enrollment.

© 2023 Benefit Comply, LLC

Health Plans Sponsored

As noted above, the health plan (not the employer) is the covered entity. Many types of group health plans that employers sponsor for their employees are subject to HIPAA. Typically, the following plans are considered health plans for purposes of HIPAA's privacy and security requirements, because they provide and/or pay for the cost of medical care:

- Medical
- Dental
- Health FSA
- HRA
- Vision
- EAP (if it provides counseling services beyond just referrals)
- Hospital Indemnity/Critical Illness policies that pay on a "per service" basis
- On-site medical clinics (exemptions may apply; should be reviewed with legal counsel)
- Wellness Programs (to the extent they are part of major medical plan or otherwise provide or pay for the cost of medical care)
- Prescription Drug
- Long-Term Care other than nursing home fixed indemnity policies
- Retiree Plans

The following types of plans are generally not considered health plans subject to HIPAA's privacy and security requirements because they are not considered to provide or pay for medical care:

- Long-Term Disability
- Short-Term Disability
- Accident-only policies
- Workers' Compensation
- HSAs (unless they are treated as ERISA plans, which is uncommon)
- Critical Illness/Hospital Indemnity policies that pay on a "per period" or "per diem" basis
- Life Insurance
- Nursing home fixed indemnity policies

FAQ: "What about our fully-insured plans? Isn't there an exemption?"

Generally, both fully-insured and self-funded plans are considered "health plans" subject to HIPAA. However, depending on the level of access an employer has to a fully-insured plan's PHI, there may be some leniency with respect to the employer's obligations under HIPAA as plan sponsor.

It may be helpful to think about employers as falling into one of two categories with respect to fully-insured plans:

- "Hands-off" – the employer only accesses Summary Health Information[1] and enrollment/disenrollment information
- "Hands-on" – the employer accesses PHI beyond Summary Health Information and/or enrollment/disenrollment information (e.g., claims data, etc.)

"Hands-on" employers have the same HIPAA privacy and security obligations that apply with respect to self-funded health plans.

The privacy rule is clear that employers taking a "hands-off" approach with respect to fully-insured health plans are exempt from most of the administrative requirements of the privacy rule. "Hands-off" employers are only responsible for ensuring that they don't retaliate against employees who make good-faith complaints, and they can't require employees to waive their right to complain as a condition of enrollment. But note that they may have additional security responsibilities, as discussed more below.

A Note on Level-Funded Plans

While sponsors of level-funded plans will typically have similarly limited access to PHI in connection with their plan, the ability to disregard certain HIPAA rules is specifically limited to fully-insured plans. Since a level-funded plan is usually treated as self-insured for compliance purposes, this means a level-funded plan must technically comply with the full set of HIPAA Privacy and Security rules.

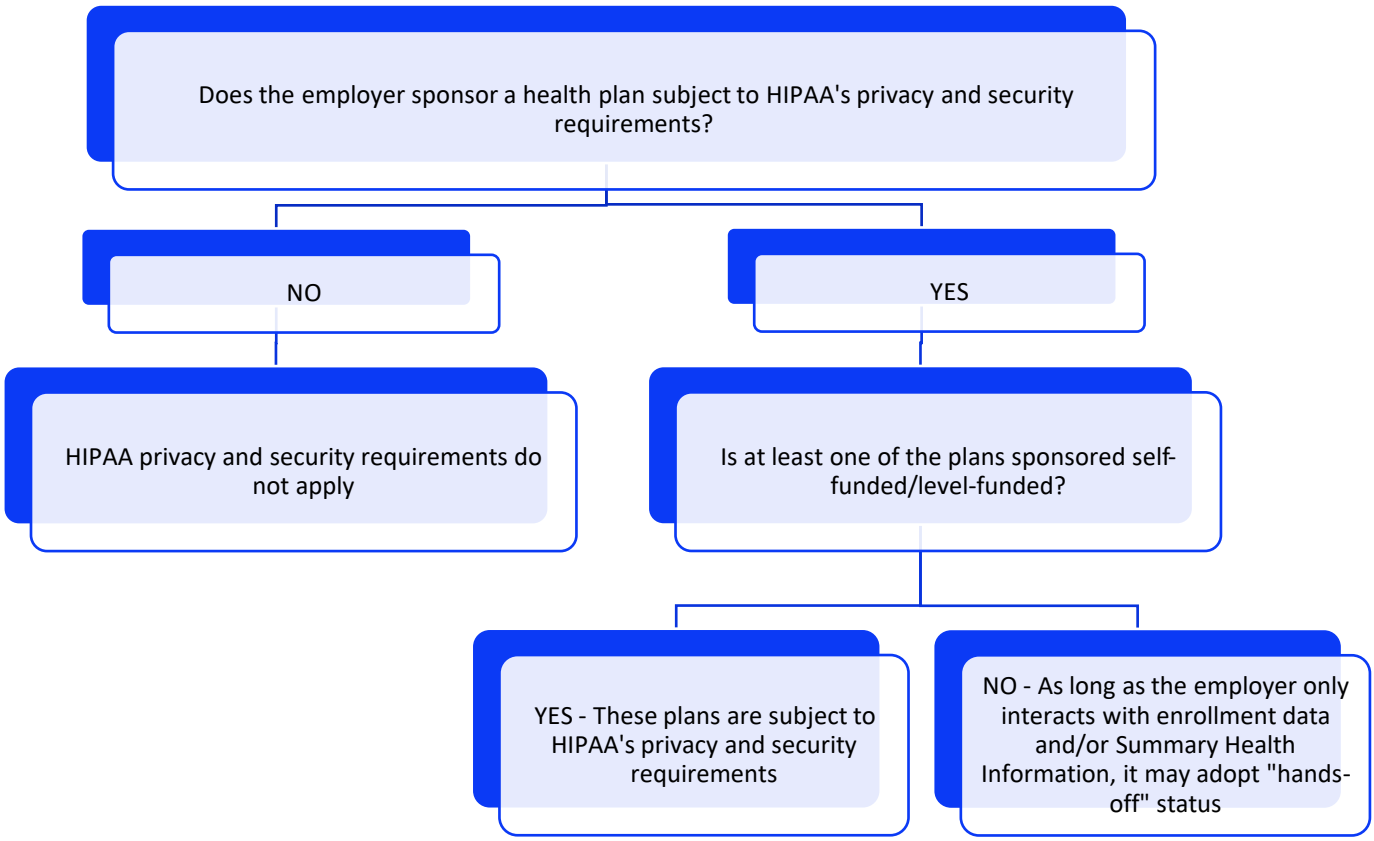
FAQ: "What if an employer sponsors some plans that are fully-insured and others that are self-funded?"

If an employer sponsors any self-funded plans, it must comply with all HIPAA's privacy and security requirements for those plans. Therefore, if an employer has a mix of self-funded and fully-insured plans, it is generally simplest to apply a common compliance approach to all plans. HIPAA allows plan sponsors to designate what is called an "Organized Health Care Arrangement," or "OHCA" to different plans. This allows employers to treat separate plans as a single plan for purposes of HIPAA privacy and security compliance, and adopt a single set of policies and procedures, a single Notice of Privacy Practices, designate a single Privacy Official, etc., for all plans. An employer will typically designate its intent to treat various plans as a single "OHCA" as part of its written HIPAA policies and procedures.

[1] "Summary Health Information" is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five-digit zip code.

© 2023 Benefit Comply, LLC

Fig. 1: Decision Tree for Determining HIPAA Compliance Obligations



FAQ: "All our ePHI is maintained by third parties. Why do we need to comply?"

If an employer sponsors a self-funded group health plan (e.g., a medical plan, dental plan, FSA or HRA), then it is required to comply with HIPAA's privacy and security requirements even if it primarily uses third party vendors (e.g., a TPA) for plan administration. There are a few reasons for this:

- Third party vendors who assist with plan administration are business associates and must mirror the compliance measures that the plan has in place.
- An employer may not have a lot of PHI on its systems, but chances are it has at least *some* PHI (i.e., enrollment files, email correspondences, information downloaded from third party sites and stored in shared network folders). This information must be protected according to the requirements of the Security Rule.
- Even if the employer truly has no PHI on its systems, it should still address the various security controls in anticipation of the possibility that it *might* encounter its health plans' PHI at some point in time. For example – if a vendor sends an employee an unsecured email containing PHI, it's important that the employer have appropriate controls in place (e.g., access controls, encryption, anti-virus processes, etc.) to ensure that that information remains secure.

© 2023 Benefit Comply, LLC

Identifying Employees Needing Access to PHI

HIPAA has a concept informally known as the "firewall," which requires ensuring that only employees who are responsible for plan administration have access to PHI. Other employees within a company should not interact with or have access to PHI, and an employer should be able to demonstrate how it manages access and ensures this "firewall" remains in place. Employees who interact with PHI should be identified (by name, department, role, or title) in the employer's written policies and procedures, in the HIPAA security risk analysis, and in the health plan document (each of these items is discussed in more detail below). To determine who needs access to PHI, the employer should consider who internally is responsible for things like working with carriers and third-party administrators for billing/claims payment, answering questions about benefits/claims, working with external auditors, and other related activities. Typical roles for plan administration include employees in Human Resources, Benefits, Finance/Payroll, and IT (since IT has systems administration oversight that will involve internal systems containing ePHI).

Use and Disclosure Rules

In general, a plan must only use and disclose PHI for reasons that are permitted under HIPAA.

Plan Administration

First, assuming that there are policies and procedures in place and that the plan document permits it, a plan sponsor may use and disclose PHI for purposes of administering its health plan. In other words, plan sponsors may use and disclose PHI for things like claims payment, working with TPAs or carriers, assisting with enrollment/benefits related questions, etc.

Public Policy Purposes

Second, a plan may use and disclose PHI for certain public policy related purposes – for example, disclosures of PHI might be necessary in the event of certain public health emergencies, or in the case of victims of abuse or neglect, or for judicial proceedings. In addition, plans might be required by law to release PHI in some cases – for example, to comply with public records laws or Medicare Secondary Payer requirements.

To the Individual Who is the Subject of the PHI

Third, a plan can release an individual's PHI to that individual if requested by the individual (or their personal representative).

To Third Parties in Certain Instances

Fourth, plans can disclose an individual's PHI to a friend, relative, or other person in certain instances and certain requirements are met. First, a disclosure is permitted if the individual is available and agrees to the disclosure. For individuals who are incapacitated, a plan may disclose PHI to a third party if the plan determines in its professional judgment that the disclosure is in the individual's best interest.

© 2023 Benefit Comply, LLC

For Underwriting

Finally, plans can use PHI for purposes of underwriting – but it is important to note here that genetic information may not be used for this purpose, and plans may only disclose Summary Health Information to entities that are outside of the organized health care arrangement unless they are business associates.

Employers should review the types of activities they engage in on behalf of their health plans and be sure that they clearly articulate in their policies and in their Notice of Privacy Practices which types of uses and disclosures of PHI they make.

If a use or disclosure doesn't fall into one of the above buckets, it will be necessary to obtain written authorization from the individual who is the subject of the PHI before making that disclosure. Examples of situations where a written authorization would be necessary include situations where a spouse calls in asking for information about an employee's claim. Or perhaps a plan wants to use PHI for marketing purposes (which do not fall under plan administration). Or maybe a parent wants to access PHI about an adult child who is on their plan. Or perhaps an employer wants to substantiate an employee's request for FMLA by looking in its health plan records to see if there are related claims. Employers may also be tempted to review claims information for purposes of making decisions about hiring or firing an employee. These are all examples of uses and disclosures of PHI that are not required or otherwise permitted by law and would not be allowed without the written permission of the individual who is the subject of the PHI.

Common Use and Disclosure Issues – Some Examples

Example 1: An employee contacts Human Resources to ask a question about a spouse's claim. Because one adult is requesting another adult's PHI, the employer must either: 1) get verbal authorization from the spouse for a single conversation with the employee, or 2) get written authorization from the spouse for ongoing communications with the employee. Without authorization, the employer is not permitted to share the spouse's PHI with the employee.

Example 2: A spouse contacts the plan sponsor with questions about their own claim. In this situation, the spouse is requesting their own PHI, and as long as the employer verifies the spouse's identity (if not already known), it can discuss the spouse's PHI with the spouse.

© 2023 Benefit Comply, LLC

Written Privacy Policies and Procedures

It is not enough for employers to informally address HIPAA privacy requirements. To be fully compliant, they must also have a set of written policies and procedures in place that describe exactly how they comply with the requirements of the Privacy Rule. A good set of policies and procedures will address:

1. Who is authorized to interact with PHI;
2. Rules for using and disclosing PHI, including how to verify identities and obtain written authorization for special uses and disclosures of PHI.
3. Internal standards for safeguarding PHI.
4. Training for employees and sanctions for employee violation of the Privacy Rule or the plan's written policies and procedures.
5. Process for handling individual rights requests and complaints.
6. Process for obtaining/reviewing written authorizations for disclosing PHI to third parties.
7. Requirements for disseminating the Notice of Privacy Practices.
8. Administrative and documentation requirements.
9. Standards for training staff on the Privacy Rule.
10. Contact information for the Privacy Official; and
11. Identifying and handling breaches of PHI.

Finding a good starting template is key – thorough templates will address the above items and provide an employer with a helpful roadmap to ensure that they are addressing all required elements of the Privacy Rule.

HIPAA Privacy Official

The role of the HIPAA Privacy Official is to oversee all elements of HIPAA privacy compliance within an organization. The Privacy Official may delegate duties to others within the organization but maintains ultimate responsibility for ensuring that the plan operates in compliance with HIPAA's requirements. The Privacy Official will often serve as an internal resource for questions about privacy requirements, including appropriate uses and disclosures of PHI, and will be responsible for investigating any suspected breaches of PHI to determine whether or not a breach occurred – and if it has, making sure the appropriate notification and reporting is completed.

There are no specific requirements surrounding who should assume the role of Privacy other than that the designated Privacy Official maintains ultimate responsibility for ensuring that adequate privacy policies and procedures are developed, implemented, and enforced. So, the named Privacy Official should have authority within the organization to enforce HIPAA's privacy requirements. Often, organizations will designate a person within their Human Resources or Benefits Departments as Privacy Official. Sometimes, the Privacy Official will be a figurehead (e.g., Senior Vice President or General Counsel) with actual responsibilities delegated to others within the organization. At other times, the Privacy Official will be the person who is responsible for the day-to-day responsibilities of plan administration.

© 2023 Benefit Comply, LLC

Notice of Privacy Practices

The HIPAA Notice of Privacy Practices (NPP) is an important communication piece that informs participants how the plan uses and discloses their PHI and what their rights are with respect to that PHI.

Content of the NPP

A compliant NPP contains all the elements required by the regulations. These elements are detailed and complex – to review them in their entirety, please review the regulatory language found at 45 CFR 164.520(b). But at a high level, the notice should contain:

1. The following header prominently displayed: THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.
2. A description of how the plan uses and discloses PHI, including examples.
3. A list of the rights an individual has under HIPAA (right to access PHI, amend PHI, request confidential communications, etc.).
4. A list of the duties of the Covered Entity for protecting PHI and maintaining/revising the notice.
5. A process for submitting complaints, including contact information.
6. Contact information for other questions about the notice; and
7. An effective date.

HHS makes a model notice for health plans available, which contains instructions for proper completion of the notice. The model notice is located here: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html.

Delivery of the NPP – Timing & Methods

In general, the NPP must be provided at enrollment (in new hire enrollment materials) and within 60 days of any revision. In addition, the NPP must be provided to any individual (including non-participants) who requests it. Finally, a reminder of the availability (or redistribution) of the NPP must be issued every 3 years.

The HIPAA regulations contain specific instructions for distribution of the NPP. First, if there is a website (e.g., an intranet site) that contains information about the health plan's customer service or benefits, then the NPP must be posted on and made available electronically through the website. (Note – this is not saying that the company needs to post the NPP on its corporate website; only that if there is a website, such as an intranet site, specific to the *health plan* that describes the health plan's customer service or benefits, that the NPP be posted there.)

In addition, the NPP must be individually delivered to the individual entitled to the notice. So, posting *only* on a website or otherwise making the notice available to individuals (e.g., posting at the workplace) won't substitute for the required actual delivery. The NPP can be provided by email, if the recipient has agreed to receive an electronic notice and that agreement hasn't been withdrawn. However, if the employer knows that the email

© 2023 Benefit Comply, LLC

transmission to an individual has failed, it must provide a paper copy of the notice to the individual. While it's best to get some type of up-front consent for electronic delivery of the NPP, it is probably low risk to rely on the ERISA electronic delivery safe harbor for electronic delivery of the NPP. So, if the NPP is being provided along with other ERISA documents (e.g., the SPD), and if the DOL electronic delivery safe harbor rules are being followed for those materials, it's likely OK to rely on those same rules for the NPP.

Business Associates – Identifying and Contracting

In general, a business associate is any third party that performs plan administration functions on behalf of a covered entity when those functions involve the use and/or disclosure of PHI. Such services may involve third-party administration services; coordination with third-party administrators and/or carriers to resolve employee benefits and claims issues; data analytics and other activities related to the creation, renewal, or replacement of a health insurance contract; care and disease management; provision of software platforms that store PHI; and even shredding services for paper PHI. Ultimately, it is important for employers to review its vendor relationships considering two questions:

1. Does the vendor perform some type of plan administration service on behalf of the health plan? (In other words, is the service being provided related in some way to administration of the employer's health plan?)
2. In performing such service, does the vendor interact with PHI in any way?

If the answers to both above questions are "yes," then that vendor should be considered a business associate. As a business associate of the plan, HIPAA requires that there be a Business Associate Agreement (BAA) in place with this vendor. Some business associates will be obvious – for example, the third-party administrator who administers one or more of the employer's health plans will be a business associate. (Note – carriers who administer fully insured plans are not considered business associates because they are covered entities and must comply with HIPAA in that capacity.) Brokers will likely act as business associates, as will some attorneys. COBRA vendors may be business associates if they are receiving health plan information in order to administer COBRA benefits. These are some of the more obvious relationships. But there are other, less obvious relationships that must be considered as well. For example:

- The Department of Health and Human Services (HHS) has made it clear in its guidance that **cloud services providers** (e.g., Microsoft) are business associates when they are providing software/applications that are used to store or transmit electronic PHI. Therefore, employers must consider who provides their HRIS/benefits platforms, and if PHI is exchanged via email or stored in network folders, what company provides those services?
- Many phone systems now operate through the internet rather than through landlines. If an **internet phone services provider** is able to store/record information that is transmitted, then it would also be a business associate if PHI is discussed verbally over the phone.

© 2023 Benefit Comply, LLC

- IT Departments may want to consider whether it has **third-party IT vendors** who provide any sort of assistance that involves access to systems that contain PHI. And employers cannot forget about paper PHI! If they discard paper PHI properly by shredding it, then any vendor responsible for collecting that shredding would also be considered a business associate.
- Similarly, paper-based **document storage vendors** (e.g., Iron Mountain) are business associates if they are storing files that may contain PHI (like old enrollment files).
- HHS has recently issued guidance regarding **health application vendors** – i.e., vendors that provide certain wellness/fitness apps that collect and track individual data. If employees are using these applications in connection with a wellness program or the medical plan, then the vendors would be considered business associates and a BAA would be necessary.

Vendors that are not performing a plan administration function should not be accessing PHI, and vendors that are performing a plan administration function should have a BAA in place before they interact with any of the plan's PHI. A BAA essentially passes down the same privacy and security protections that apply to the health plan to the business associate. It is a way for employers to ensure that any PHI they entrust to third parties remains protected and secured. There are specific elements that must be included in a compliant BAA, so employers should review any agreements they are relying on to ensure that they meet all applicable requirements. HHS makes the required provisions available here: https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

Health Plan Document & Plan Sponsor Certification

The employer's health plan document (typically the ERISA plan document) must contain specific language that permits the health plan to share PHI with the employer as plan sponsor. This is necessary because the health plan is the covered entity, and the employer is not. Therefore, an agreement (similar in some ways to a BAA) must exist between the employer as plan sponsor and the health plan. The language in the plan document should specify the terms and conditions of the employer's use and disclosure of PHI and the employer should complete a certification that the plan documents contain the required language, and the employer agrees to abide by it.

To receive PHI, employers must amend their group health plan documents to contain the following provisions:

1. The permitted and required uses and disclosures of PHI by the plan sponsor (i.e., for legitimate plan administration purposes or as otherwise permitted or required by law).
2. That the health plan will only release PHI to the plan sponsor upon receipt of certification by the plan sponsor that its health plan document contains provisions outlining the requirements of the Privacy Rule and that the plan sponsor agrees to abide by those provisions. These provisions require that the plan sponsor:
    - not use or further disclose PHI other than as permitted by the plan documents or as required by law.

- ensure that any agents or subcontractors to whom the sponsor provides PHI received from the health plan agree to the same restrictions and conditions that apply to the plan sponsor.
- not use or disclose PHI for employment-related actions or in connection with any other benefit or employee benefit plan of the plan sponsor.
- report to the health plan any use or disclosure of the information that is inconsistent with the permitted uses or disclosures.
- make PHI available for purposes of the access, amendment, and accounting of disclosures provisions in the privacy rule, and incorporate any amendments.
- make its internal practices, books, and records relating to the use and disclosure of PHI received from the health plan available to the Department of Health and Human Services for the purpose of determining the plan's compliance with the privacy rule.
- if feasible, return or destroy all PHI received from the health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
- ensure that there is adequate separation between the group health plan and the plan sponsor.

3. Implement the “firewall” referenced above by:
    - Describing (by name title, role, or department) the employees or other persons under the control of the plan sponsor who will be given access to PHI, including any employees who receive PHI in the ordinary course of business.
    - Restricting the access of these employees/persons to PHI to plan administration functions; and
    - Providing an effective mechanism to resolve issues of noncompliance by such persons.

In addition, the health plan document must require the plan sponsor to:

1. Implement administrative, physical, and technical safeguards that reasonable and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the sponsor creates, receives, maintains, or transmits on behalf of the group health plan.
2. Ensure that the firewall required by the privacy amendment is supported by reasonable and appropriate security measures.
3. Ensure that any agent or subcontractor to whom the plan sponsor provides ePHI agrees to implement reasonable and appropriate security measures to protect the information; and
4. Require the plan sponsor to report to the plan any security incident of which the plan sponsor becomes aware.

© 2023 Benefit Comply, LLC

HIPAA Security

General Security Overview

Whereas HIPAA privacy is concerned with appropriate safeguarding of PHI in all forms (electronic, verbal, written, etc.), HIPAA security is uniquely concerned with the confidentiality, integrity, and availability of PHI in its electronic form. Electronic PHI is also called "ePHI." The security rule contains a set of standards that all covered entities and business associates must address, although the Security Rule provides significant flexibility for organizations to address the standards and implement security measures in a way that makes sense for their environment, size, budget, and overall mission.

HIPAA Security Risk Analysis

Employers must complete a Risk Analysis to identify potential vulnerabilities with their current controls, to evaluate risk with respect to vulnerabilities, and to work to mitigate this risk in its risk management program. The risk analysis is foundational to an employer's HIPAA security efforts. It will usually be completed primarily by somebody in the IT department, with some input provided by Human Resources and/or Benefits.

There are many variables to consider, including a company's computer systems, how ePHI flows through the organization, and even physical controls with respect to the office building. It is possible (even likely) that an employer has already conducted this type of analysis for other purposes. If so, completing a HIPAA-specific analysis should be fairly straightforward, but note that it will be important to ensure that the analysis includes a complete analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of any ePHI the organization maintains.

While there are no hard and fast rules about how a risk analysis must be conducted, we recommend the following steps for completing a thorough risk analysis:

1. Identify all areas where ePHI is stored/located, who has access to that information, and how/where it is transmitted. (See the Inventory of PHI section for more detail.)
2. Evaluate current security controls as compared to HIPAA's standards.
3. Consider how well the existing security controls protect the ePHI and assign final risk scores to these controls, specifically considering:
    - The likelihood that some type of threat (malware, a misdirected email, a lost laptop, a natural disaster, etc.) could exploit an existing vulnerability.
    - The impact to the organization if a threat were successfully exploited.
    - The total risk to the organization taking account of the existing controls in place, potential threats, and the likelihood and impact analyses described above.
4. Use the final risk scores to help prioritize any needed mitigation efforts or additional security efforts.

© 2023 Benefit Comply, LLC

5. Review the risk analysis from time to time (both periodically and when there are major operational, legal, or infrastructure changes to the organization) and make updates as needed.

Each of these items is discussed in more detail below.

Identification of ePHI

The organization should begin its risk analysis by conducting a detailed inventory of their ePHI, documenting where ePHI is stored and maintained, and how ePHI flows, both inside and outside of the organization (e.g., where ePHI is sent, and from whom it is received). They should also identify the systems and applications (e.g., email, cloud providers, internal networks) used to accomplish the transmission of ePHI. You should maintain this inventory and update it regularly to ensure that the risk analysis remains current. Please see the Inventory of PHI section for more details on this analysis.

Current Security Controls

Review each of the required security standards and compare each to what the employer currently has in place. The security standards are organized into "physical," "technical," "administrative," and "organizational" safeguards. HHS maintains a library of guidance material that describes each safeguard in detail here: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

Threat Identification

After inventorying ePHI and looking at existing security controls in place, employers must identify any potential threats to the plan's ePHI. Threats are typically categorized into the following three (3) types:

- Natural threats (flood, earthquake, fire, tornado, show, ice and hurricane).
- Human threats (intentional or unintentional damage through vandalism, sabotage, terrorism, robbery, vehicle crash, hazardous waste, computer crime, or user error); and
- Technical threats (power failures, hardware/software failures, gas leaks, telecommunications failure).

Vulnerability Identification

Taking into consideration existing safeguards and any identified threats, identify any potential vulnerabilities to the plan's ePHI. A vulnerability is defined as "a flaw, weakness or area of exposure in a system security, procedure, design, product, or implementation that exposes ePHI to a possible threat and could result in the damage, loss or misuse of the electronic data." In other words, vulnerabilities exist where inadequate controls are in place. And a threat (e.g., poor workforce training or simple user error) can exploit a vulnerability.

© 2023 Benefit Comply, LLC

Risk Likelihood

Considering current threats, current controls, and vulnerabilities, employers must assess the *likelihood* that a given threat will exploit an existing vulnerability. For example, if an organization does not currently train staff on the risk of malware/social engineering (or even if it does), what is the likelihood that a user might open an attachment containing a virus that could infiltrate systems containing ePHI?

Impact Analysis

Employers should assess the impact an adverse event would have to the confidentiality, integrity, and/or availability of the plan's ePHI. In other words, what would the impact to the employer be if the successful exploitation of a vulnerability caused ePHI to be used or disclosed in an unauthorized manner (impacting confidentiality); improperly modified (impacting integrity); or become unavailable to those authorized to access it (impacting availability)?

Risk Score

After considering vulnerability and impact, an employer should assign an overarching risk score to help it prioritize with respect to any necessary remediation or mitigation measures.

Decision-Making

Based on the results of the analysis, an organization must determine what controls it wishes to implement (or maintain) with respect to ePHI. The employer should document its decision-making in its risk analysis and describe its controls in the form of written policies and procedures.

Note that the security standards are identified as "required" or "addressable." Controls that are "required" are just that – obligatory. Controls that are "addressable" offer a bit more flexibility. While not optional, they do permit an organization to analyze whether it would be "reasonable and appropriate" to implement a certain control given the organization's environment and security framework with respect to the likely contribution it would make to the protection of ePHI.

Written Security Policies and Procedures

Organizations must have a set of written procedures that describe how they comply with the requirements of the security rule. These procedures are based on the set of safeguards and implementation specifications contained in the Security Rule and should be informed by the organization's risk analysis and the decisions it makes about its security approach in response.

Organizations may rely on an existing set of general security policies that are not specific to HIPAA but should ensure that they address all required HIPAA security standards and should document how the controls apply specifically to ePHI.

© 2023 Benefit Comply, LLC

HIPAA Security Official

Just like designating a Privacy Official to oversee privacy-related compliance issues within, organizations must also designate a Security Official who is responsible for ensuring that the security risk analysis is completed, that any identified areas of concern are mitigated appropriately, and that written policies and procedures are developed and followed internally. The Security Official is also responsible for overseeing implementation of necessary security controls as a result of the organization's risk analysis and conducting ongoing monitoring of the effectiveness of current controls.

The Security Official will also act as a contact for reporting concerns about security, including known or suspected breaches of ePHI and will coordinate with the Privacy Official to ensure that any known or suspected breaches of unsecured ePHI are handled appropriately.

The named Security Official may designate others in the organization to lead, manage, or complete the Security Official's responsibilities, but will maintain ultimate responsibility for compliance.

Security Awareness Training

In addition to training employees who interact with PHI on HIPAA's use and disclosure requirements, organizations should provide broad-based security awareness training to all employees who have electronic access to the employer's systems (whether or not they interact with PHI). This broader training is meant to reduce the likelihood of a general security incident that could impact systems and applications where ePHI is located. The training does not need to be specific to HIPAA but should address the organization's password management expectations; login monitoring protocols; and how to identify/protect against malware. Usually, this training effort is managed by the employer's IT Department.

Security Requirements for "Hands-Off" Plan Sponsors

Unlike with privacy requirements, there is no broad-based exemption for hands-off employers under the Security Rule; therefore, the exact nature of a hands-off plan employer's security requirements are less clear. However, from a practical standpoint, it seems as though the employer (at least in its capacity as an ERISA plan administrator) should take at least the following steps to demonstrate due diligence with respect to its health plan's obligations under the Security Rule:

1. Conduct an analysis (whether or not technically a "risk assessment" under HIPAA) to verify and document that the plan sponsor truly doesn't have access to PHI (beyond summary health or enrollment/disenrollment information).
2. Designate a Security Official to act as a point of contact for any questions or issues that may arise with respect to the health plan's ePHI (even if there is no access to it, questions may still arise, and at least some level of coordination with the carrier will be needed).

© 2023 Benefit Comply, LLC

3. Ensure that the carrier has appropriate safeguards in place to ensure the confidentiality and integrity of the plan's ePHI, and document the extent to which the plan sponsor is relying on the carrier's policies and procedures to ensure compliance with the Security Rule.
4. Ensure that there are processes in place to respond to and provide notification for any breaches of unsecured ePHI, in particular any of which the plan sponsor may become aware; and
5. If the plan has any Business Associates, ensure that compliant Business Associate Agreements are in place.

There is little guidance for these "hands-off" situations because the risk under HIPAA for the employer is admittedly low. At the same time, we feel it is important not to overlook the fact that the employer most likely has fiduciary obligations under ERISA to oversee proper plan administration. So being mindful of the various stakeholders and their key HIPAA obligations and ensuring appropriate attention is being given by them to those activities is a good strategy to minimize any exposure under ERISA for the employer.

© 2023 Benefit Comply, LLC

Identifying & Handling Breaches of PHI

In general, a breach occurs any time there is impermissible use or disclosure of PHI – that is, a use or disclosure not permitted by the Privacy Rule. However, there are three exceptions to this general rule:

1. An unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate.
2. An inadvertent disclosure of PHI from one person authorized to access PHI to another person authorized to access PHI; and
3. Unauthorized disclosure in which an unauthorized person would not reasonably have been able to retain the information.

If none of these exceptions apply, then whenever there is an impermissible use or disclosure of PHI, an entity must perform a risk assessment to determine whether or not the use or disclosure constitutes a breach or not. It does this by considering four factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the PHI or to whom the disclosure was made.
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

This assessment should be conducted by the Privacy Official, ideally in conjunction with legal counsel, each time there is any impermissible use or disclosure of PHI. If, after conducting this assessment, the Privacy Official concludes that there is a low probability that the PHI has been compromised, then the incident does not need to be treated as a breach. The results of the assessment should be documented, and the documentation maintained in accordance with HIPAA's record retention requirements.

When a breach has occurred, there are specific notification and reporting requirements that a covered entity must comply with under HIPAA. First, individuals must be notified of the breach "without unreasonable delay" and no later than 60 days after the breach was discovered by the entity. (Note that in this case, "discovered" means the date that the breach is known, or by exercising reasonable due diligence, would have been known, to the entity.)

Second, entities must notify HHS of the breach. For breaches affecting fewer than 500 individuals, this notification must be made annually within 60 days of the end of the calendar year in which the breach occurred. However, for breaches affecting 500 or more individuals, the notification must be made within 60 days after the breach was discovered by the entity, concurrently to the notification to individuals.

Finally, for breaches affecting more than 500 residents of a state or jurisdiction, a covered entity must also notify prominent media outlets in that state or jurisdiction within the same timeframe that notification is due to individuals.

© 2023 Benefit Comply, LLC

The breach notification must be written in plain language and must contain certain information, such as a description of circumstances relating to the breach; the type of PHI disclosed; and steps individuals should take to protect themselves from potential harm.

Oversight and Enforcement

Background

In recent years, regulators have taken a more proactive approach to HIPAA compliance oversight. As a result of HITECH, the Office for Civil Rights (OCR), a division of HHS, was put in charge of oversight and tasked with conducting proactive audits of covered entities and business associates to assess compliance efforts. There have been two rounds of audits undertaken so far, and for the most recent round, OCR has made both its protocol and findings available publicly:

- The protocol used for audits may be found here: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html.
- OCR's audit findings report may be found here: https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf.

Potential Penalties for HIPAA Violations

HHS has established the following penalty structure, which is indexed annually, for different types of violations of the HIPAA Privacy and Security Rules. Note that in 2019, HHS indicated that it would cap all penalties at $1.5 million per year, indexed for inflation. The regulations have not been updated to reflect this guidance, so the table below reflects current law in the Federal Register. Separately, there are potential penalties for criminal violations that range from $50,000 to $250,000 and/or 1 to 10 years' imprisonment.

Penalty Tier	Min Penalty Per Violation	Max Penalty Per Violation	Calendar Year Cap*
Tier 1 (Lack of Knowledge)	$137	$68,928	$2,067,813
Tier 2 (Reasonable Cause)	$1,379	$68,928	$2,067,813
Tier 3 (Willful Neglect)	$13,785	$68,928	$2,067,813
Tier 4 (Willful Neglect not corrected within 30 days)	$68,928	$2,067,813	$2,067,813

© 2023 Benefit Comply, LLC

*In 2019, HHS indicated that it would cap penalties at $1.5 million per year, adjusted for inflation.

While enforcement efforts to date have primarily focused on providers and payers, this does not mean that employers can afford to ignore HIPAA. Many of the drivers of large settlements stem from basic gaps in compliance – failure to enter into compliant BAAs; failure to conduct a security risk analysis; failure to have written policies and procedures in place, etc. The requirements are clear – HIPAA has been around now for almost 30 years. While employers may not be the primary target of enforcement, there is no excuse now for not making a thorough effort at due diligence with respect to HIPAA privacy and security compliance.

Conclusion

The hope for this guide is not that employers have a step-by-step roadmap for putting together a HIPAA compliance program (although we have separate solutions for that!); instead, the goal is to help employers understand the breadth of privacy and security requirements and to address some of the most common questions and misconceptions we tend to see that act as a barrier to achieving full compliance. We hope this serves as a helpful starting point for thinking holistically about HIPAA privacy and security, what obligations apply to employers as plan sponsors, and making important decisions about next steps.

© 2023 Benefit Comply, LLC