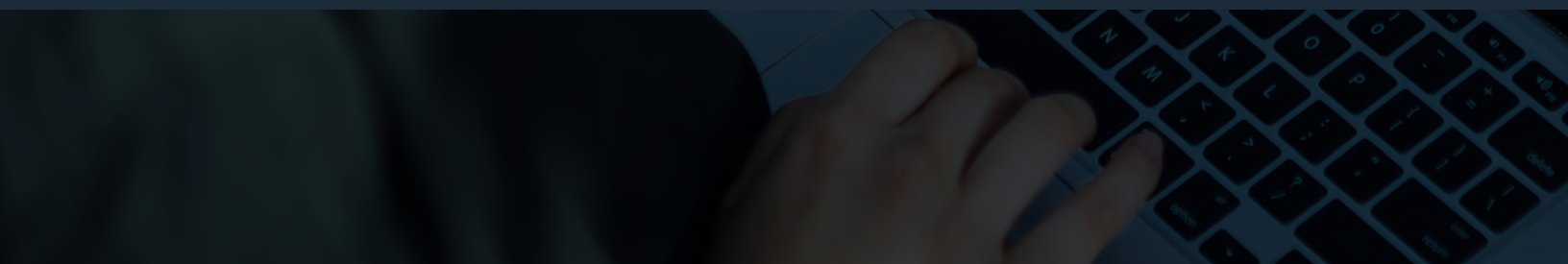
PPi BENEFIT SOLUTIONS

Corporate Benefits
Compliance

HIPAA Privacy and Security for Group Health Plans:

A Guide for Employers



HIPAA's requirements vary significantly in their impact on self-insured versus fully insured plans, with greater responsibilities and administrative burdens placed on self-insured group health plan sponsors. Fully insured group health plans must comply with certain provisions as well, though the scope of those requirements will depend on whether the plan handles participant health data.

This guide focuses on HIPAA's Administrative Simplification provisions, which were implemented to streamline healthcare operations and enhance the privacy and security of health data. The Privacy, Security, and Breach Notification Rules (herein the Privacy and Security Rules collectively for ease of reference) establish standards for safeguarding protected health information (PHI) in both paper and electronic forms and for responding to data breaches.

This publication provides a high-level overview of the Privacy and Security Rules for employers sponsoring group health plans to understand the scope of their responsibilities. It includes a **HIPAA Privacy and Security Compliance Overview for Self-Insured vs. Fully Insured Group Health Plans** (Appendix A). The publication is not meant to serve as a comprehensive guide to HIPAA compliance. Plan sponsors often rely on HIPAA compliance vendors and legal counsel to satisfy many requirements of the Privacy and Security Rules. In addition, note that state privacy laws vary and fall outside the scope of this publication (see Other Group Health Plan Privacy Laws below).

At a Glance:

with each of its business associates assuring that health information will be used, disclosed, and safeguarded in compliance with HIPAA.

II. The Privacy Rule

HIPAA regulates the ways in which group health plans may use or disclose participant health information. Self-insured and hands-on fully insured group health plans must implement certain administrative requirements to ensure that participant health data is protected.

5. Protected Health Information

HIPAA applies to PHI, which is individually identifiable health information that is held or transmitted by a group health plan. Plans must be able to identify, appropriately use, and safeguard this information in the course of their operations.

Certain types of employee health information – such as that collected for disability benefits, life insurance, FMLA, ADA accommodations, or sick leave – are considered employment records rather than PHI. Thus, they are not subject to HIPAA, even though they may contain sensitive health details. Plans may use and disclose de-identified information and summary health information with greater flexibility, and doing so will not compromise an insured plan's hands-off PHI status.

6. Permitted Uses and Disclosures for Plan Sponsors

Plans are permitted under the Privacy Rule to use and disclose PHI in order to carry out their own administrative functions — specifically, for treatment, payment, and healthcare operations. This provision allows plans to facilitate the healthcare coverage of their participants. Plans are also permitted to use and disclose PHI for certain public health, law enforcement, and other national priority purposes. At all times, plans must adhere to the minimum necessary standard, which stipulates that only the minimum amount of information that is necessary for any given purpose is used or disclosed.

7. Required Disclosures

The Privacy Rule requires plans to disclose PHI to a participant upon request or to HHS as part of an investigation or enforcement action.

8. Individual Authorization

Any use or disclosure of PHI by a plan that is not for one of the expressly permitted or required purposes will require a signed, written authorization from the affected participants. HIPAA describes the content that must be included in the authorization, but there is no official model form. Psychotherapy PHI is subject to even stricter specifications.

9. Individuals' Rights Under HIPAA

The Privacy Rule gives participants five rights with respect to their own PHI: the right to access it upon request, the right to receive an accounting of disclosures by the plan (subject to certain limitations), the right to amend incorrect information, the right to restrict certain uses or disclosures, and the right to request confidential communications of PHI.

10. Administrative Requirements

Self-insured and hands-on fully insured group health plan sponsors must comply with seven Privacy Rule administrative requirements: written policies and procedures, Notice of Privacy Practices, workforce training and management, a privacy official, a participant complaints process, retaliation and waiver prohibition, and documentation and record retention. Plans often engage an outside vendor to assist with many of these responsibilities.

III. The Security Rule

All group health plans are subject to the Security Rule. Self-insured and hands-on fully insured group health sponsors must undertake certain measures to protect the confidentiality, integrity, and availability of their electronically maintained or transmitted PHI.

11. Administrative Safeguards

The Security Rule requires plans to undertake nine administrative safeguards: risk analysis and management, a security official, workforce management, information access management, security awareness and training, security incident procedures, a contingency plan, evaluation protocols, and BAAs.

12. Physical Safeguards

The Security Rule requires plans to implement three physical safeguards: facility access and controls, workstation use and security, and device and medical controls.

13. Technical Safeguards

The Security Rule requires plans to consider and implement four technical safeguards: access controls, audit controls, authentication, and transmission security.

IV. The Breach Notification Rule

In the event that participants' PHI is used or disclosed in a way that is not permitted by the Privacy and Security Rules, group health plans must respond immediately with certain risk assessment and notification procedures.

14. Definition of Breach

A breach is any access, use, or disclosure of unsecured PHI in a manner not permitted by HIPAA. Upon discovery of a suspected breach, the plan must undertake a thorough risk assessment to determine the appropriate course of action. Plan sponsors can prevent breaches by ensuring that all PHI in use or transit has been encrypted and all PHI no longer in use has been properly destroyed.

15. Notification Requirements

The plan will be required to provide notification of any breach to the affected individuals, to HHS, and (depending on the number of people affected) the local media within strict timeframes. Business associates are subject to the notification requirements for breaches they cause.

V. Enforcement, Penalties, and Other Privacy Laws

16. Enforcement of Privacy, Security, and Breach Notification Rules

These rules are enforced by the HHS Office for Civil Rights, which takes an active enforcement role through investigation of complaints and audits. HHS is currently focusing on compliance with cybersecurity rules. Additionally, the Department of Justice (DOJ) undertakes criminal investigations into HIPAA violations.

17. Penalties

HHS can levy civil monetary penalties against plan sponsors that violate HIPAA. The amounts are indexed for inflation and increase based on severity. In certain cases, the DOJ can assess criminal penalties and imprisonment.

I. Overview

1. Scope of HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to improve access to health coverage and strengthen protections for personal health information. HIPAA touches nearly every part of the U.S. healthcare system — from how individuals maintain health coverage to how health information is managed, protected, and exchanged. Its portability provisions (found in Title I) focus on ensuring continuity of coverage and protecting individuals from discrimination based on health status, while its Administrative Simplification provisions (found in Title II) set national standards for electronic healthcare transactions and the safeguarding of protected health information.

HIPAA's portability provisions are designed to ensure that individuals can maintain health coverage when they change or lose employment. These protections include special enrollment rights and prohibitions against discrimination based on health status. The accountability provisions focus on protecting health information by establishing national standards for how that information is used, disclosed, and secured — particularly in electronic form. These provisions include the Privacy Rule, which governs how PHI is used and disclosed; the Security Rule, which sets standards for safeguarding electronic PHI (ePHI); and the Breach Notification Rule, which requires notification when unsecured PHI is compromised.

2. Employer's Role

The privacy and security provisions do not apply to employers in their capacity as employers. Instead, they apply to "covered entities," which include healthcare providers, healthcare clearinghouses, and health plans — such as group health plans sponsored by employers (including corporations, partnerships, governmental entities, religious organizations, schools, and other public or private institutions). While church-sponsored and governmental health plans may be exempt from certain federal laws (such as ERISA), they are not exempt from HIPAA's privacy and security provisions and must comply if they meet the definition of a covered entity. See Covered Entities below. An exception exists for group health plans with fewer than 50 participants that are self-administered by the employer.

When an employer sponsors a group health plan, these rules apply to the plan, whether insured or self-insured, and not to the employer. But in some instances, especially with respect to a self-insured plan, it can be difficult to distinguish between the employer and the plan, especially where the same personnel perform both employment and health plan functions. See Hands-Off Fully Insured Plans below. The privacy and security provisions require strict safeguards to ensure that PHI accessed through the plan is not used for employment-related purposes. Notably, HIPAA does not cover employment records, even if they contain health-related information, though such records may be protected under other laws like the ADA or FMLA. (See Employment Records below.)

3. Covered Entities

HIPAA's privacy and security provisions apply to covered entities, which are comprised of healthcare providers, healthcare clearinghouses, and health plans.

- Healthcare providers include doctors, hospital systems, clinics, pharmacies, dentists, and other entities that provide care and transmit health information electronically.
- Healthcare clearinghouses are public or private intermediaries that process health data between providers and payors, including billing services and community health information systems.

- Health plans encompass private insurers, government programs like Medicare and Medicaid, and employer-sponsored group health plans. A group health plan is defined as an employee welfare benefit plan that provides medical care to two or more employees (and their dependents) through insurance or self-insurance. These plans are subject to HIPAA's privacy and security provisions if they transmit health information electronically in connection with standard transactions, such as claims, eligibility inquiries, or payment authorizations. This includes a broad range of health plans, including major medical coverage, dental coverage, vision coverage, health FSAs, HRAs, EAPs, and other point solutions programs that provide or reimburse medical care expenses.

Group welfare plans and employee benefit programs that do not provide healthcare – including disability benefits, life insurance, accident-only insurance, sick leave, or family and medical leave – are outside of the scope of the privacy and security provisions.

PPI Observation	**Disability Benefits and FMLA.** Given the involvement of sensitive health information, some employers may assume that programs like disability benefits or FMLA are subject to HIPAA's privacy and security provisions, but they are not. These programs fall outside of the scope of Privacy and Security Rules. However, they are often subject to separate confidentiality, security, and recordkeeping requirements. Employers should understand these distinctions and consult legal counsel or other trusted experts to ensure compliance with applicable laws.

Voluntary, supplemental, or fixed indemnity insurance – including accident, critical illness, cancer, or hospital indemnity insurance – might be subject to the privacy and security provisions, depending on how the coverage is structured. Because these arrangements may not provide payments tied to actual medical expenses and instead pay a set amount based on a particular event (e.g., hospital admission or diagnosis of a specific condition or injury), the key question is whether the coverage qualifies as a health plan that provides or pays for "medical care" as defined under federal law. Historically, regulators have avoided taking a definitive position on these types of benefits, acknowledging the complexity in the variability of how they operate.

PPI Observation	**Voluntary Benefits and Health Coverage.** While it's possible for some voluntary, supplemental, or fixed indemnity policies to be subject to the Privacy and Security Rules – if they meet the definition of a covered health plan – the insurer offering the policy would generally be responsible for compliance with those rules as a covered entity, as with any hands-off fully insured plan. That said, employers should consider consulting legal counsel to evaluate the structure and administration of these benefits to ensure they are properly classified and comply with applicable laws, including ERISA and the ACA.

The rules are also unclear about the applicability of HIPAA to expatriate health plans. While such plans would seem to fall within the scope of the Privacy and Security Rules as health plans, regulations do not specifically discuss expatriate plans.

PPI Observation	**Expatriate Health Plans.** A cautious approach would be to treat expatriate health plans as subject to the Privacy and Security Rules and to protect all individually identifiable health information that originates from those plans.

Exception for Small, Self-Administered Plans. The Privacy and Security Rules apply to group health plans (see Covered Entities above) that transmit health information electronically in connection with standard transactions (e.g., payment of claims). A narrow exception applies to a group health plan that satisfies all of the following criteria:

- Is self-administered
- Has fewer than 50 employees
- Does not transmit health information electronically

Plans meeting all three criteria are not subject to the Privacy and Security Rules. However, this exception is extremely limited in scope. Most major medical, dental, and vision plans – even those offered by small employers – do not qualify for the exception, as

they typically involve third-party administrators (TPAs) and are not self-administered. As a result, the exception generally applies only to certain small employers that manage health FSAs or HRAs entirely in-house, without electronic transactions or external support.

Hands-Off Fully Insured Plans. Although the privacy and security provisions apply to both self-insured and fully insured group health plans, the level of compliance required for plan sponsors will depend on how the plan sponsor handles PHI. (Under HIPAA, the plan sponsor, typically the employer that establishes and maintains the group health plan, is distinct from the plan itself.) In particular, some insured group health plans are structured so that the plan sponsor does not access or manage PHI beyond enrollment, disenrollment, or summary health data. This plan is often referred to as hands-off with respect to PHI. In such arrangements, the health insurer, not the plan sponsor, assumes primary responsibility for complying with most of the Privacy and Security Rule requirements.

PPI Observation	**Health FSAs and HRAs.** Employers that sponsor hands-off fully insured medical, dental, and/or vision plans and also sponsor a health FSA or HRA are no longer considered hands-off with respect to PHI. With the exception of small, self-administered plans, these organizations are subject to all the same rules that apply to self-insured plans as outlined below. This may come as a surprise to many employers that sponsor health FSAs or HRAs but have never undertaken HIPAA Privacy and Security Rule compliance. In many cases, sponsors of health FSAs and HRAs find themselves accessing a substantial amount of PHI (for example, while reconciling unsubstantiated claims or approving reimbursements). Before implementing a health FSA or HRA employers should ensure they are able to comply with all applicable HIPAA Privacy and Security Rules.

Hands-On Fully Insured Plans. Fully insured group health plans that receive PHI from their health insurer or other service providers are considered hands-on. Hands-on fully insured plans and their employer sponsors (in addition to the health insurer) must fully comply with the privacy and security requirements.

PPI Observation	**Employee Support and Hands-Off Challenges.** As a practical matter, employers can be drawn into participants' claim issues. Sometimes employees turn to the employer plan sponsor – the human resources department or managers – for help navigating healthcare claim denials, pre-authorizations, or medical bills. While the desire to support employees is understandable, sponsors of fully insured group health plans that want to maintain a hands-off approach must avoid accessing or handling PHI without securing written authorization from the individual. PHI generally refers to individually identifiable health information that is created or received by a covered entity (such as a health plan or provider) and relates to an individual's health condition, care, or payment for care. (See Protected Health Information below.) An employer's active involvement in plan benefits on behalf of employees, for example by contacting the insurer or provider as a claims advocate, may be viewed as evidence that the plan sponsor is actually hands-on, potentially triggering additional obligations under the Privacy and Security Rules. An employee's voluntary disclosure of their own health information to the employer does not, by itself, constitute PHI under the privacy and security provisions. However, once that same information is created or received by a covered entity such as the insurer, it becomes PHI and is subject to protections, regardless of whether it is independently shared by the employee with the employer. (Note: The key distinction is that personal health information becomes PHI only when it is held or transmitted by a covered entity or business associate.) Thus, while human resources or managers from a hands-off plan sponsor may attempt to reach out on behalf of employees, the covered entity (like the insurer or provider) cannot share any information that it considers PHI without written authorization from the individual. To preserve a hands-off approach, fully insured plan sponsors should avoid involvement in PHI-related matters and guide employees to contact the insurer directly with any plan or claims issues.

Self-Insured Plans. Self-insured group health plans – including health FSAs and HRAs – are, by definition, hands-on with respect to PHI and therefore must comply with all HIPAA privacy administrative and breach notification requirements as well as security safeguards.

PPI Observation	As employer plan sponsors consider transitioning from a fully insured to a level-funded or other self-insured arrangement, they should carefully evaluate the additional compliance responsibilities that come with that shift. In particular, implementing safeguards required under the Privacy and Security Rules can introduce new administrative and operational demands. Plan sponsors should assess their internal capacity to meet these requirements and confer with legal counsel to ensure they are prepared to satisfy the obligations associated with a self-insured arrangement.

All covered entities – even hands-off fully insured plans – are subject to the Breach Notification Rule's requirements. (See Definition of Breach and Notification Requirements below.) Operationally, however, a plan sponsor that truly does not access, use, disclose, or transmit PHI significantly reduces its risk of experiencing a breach or triggering breach notification obligations.

4. Business Associates

Frequently, group health plans engage third-party service providers – known as business associates – to perform administrative or operational functions on behalf of the plan that extend beyond the roles of the employer and, if applicable, the insurer. The regulations define a business associate as a person or organization other than a member of the covered entity's own workforce that creates, receives, maintains, or transmits PHI for a plan. It specifically includes claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; and repricing activities. It also includes any legal, actuarial, accounting, consulting, management, administrative, or financial services provided to or for a covered entity that involves the disclosure of PHI.

For purposes of employer-sponsored group health plans, common business associates include TPAs, insurance brokers, benefits consultants, attorneys, actuaries, wellness vendors, health FSA administrators, and IT professionals with access to electronically stored PHI. Less obvious relationships that may trigger business associate responsibilities include document retention, printing/mailing, and shredding services.

PPI Observation	Health insurers are designated covered entities under HIPAA and therefore are not considered business associates of a fully insured group health plan. Similarly, stop-loss insurers are not considered business associates of a self-insured group health plan. These entities are already directly required to comply with HIPAA's Administrative Simplification Rule. However, a health insurer that provides claims processing services or otherwise acts as a TPA for a self-insured plan is considered a business associate of that plan.

Although the Privacy Rule originally applied only to covered entities, business associates are now directly responsible for complying with many of the privacy and security requirements. Chief among those responsibilities is the obligation to enter into an agreement with the covered entity. A BAA is a written contract that requires the business associate to safeguard any PHI it receives or creates on behalf of the covered entity. Covered entities may disclose PHI to a business associate only to support the plan's healthcare operations and as permitted by the BAA — not for the business associate's independent use or purposes.

BAAs must include specific provisions as outlined in the regulations, including a description of the permitted uses and disclosures of PHI by the business associate, a statement that the business associate will not use or disclose PHI beyond what is allowed under the agreement or required by law, and a requirement that the business associate will implement appropriate safeguards to prevent unauthorized use or disclosure of PHI.

A BAA is not required in certain limited situations that may involve PHI, such as those where access to PHI is incidental or where a person or organization acts merely as a conduit for PHI. Examples within a group health plan context include office janitorial staff or delivery services such as the postal service or private courier.

Business associates may delegate certain functions, activities, or services to subcontractors. If a subcontractor will have access to PHI, the business associate must enter into a written agreement with the subcontractor that binds the subcontractor to the same restrictions and conditions that apply to the business associate, including compliance with the Privacy and Security Rules. Business associates are directly subject to the Privacy and Security Rules and are independently liable for violations. As a result, covered entities are not required to actively monitor their business associates. However, under ERISA, group health plans have a fiduciary duty to evaluate their service providers. Accordingly, BAAs should include provisions granting the covered entity the right to audit the business associate and investigate any indications or patterns of noncompliance.

II. The Privacy Rule

The Privacy Rule sets national standards for how covered entities and business associates may use and disclose certain health information. It also gives individuals specific rights regarding access and control over their health data. Designed to balance privacy and protection with the flow of information needed for care and public health, the rule is flexible and comprehensive.

The information below provides a high-level overview of the Privacy Rule for plan sponsors to understand the scope of their responsibilities. It is not meant to serve as a comprehensive guide to compliance. Unless they have privacy experts on staff, plan sponsors often rely on HIPAA compliance vendors and legal counsel to satisfy the Privacy Rule's requirements.

5. Protected Health Information

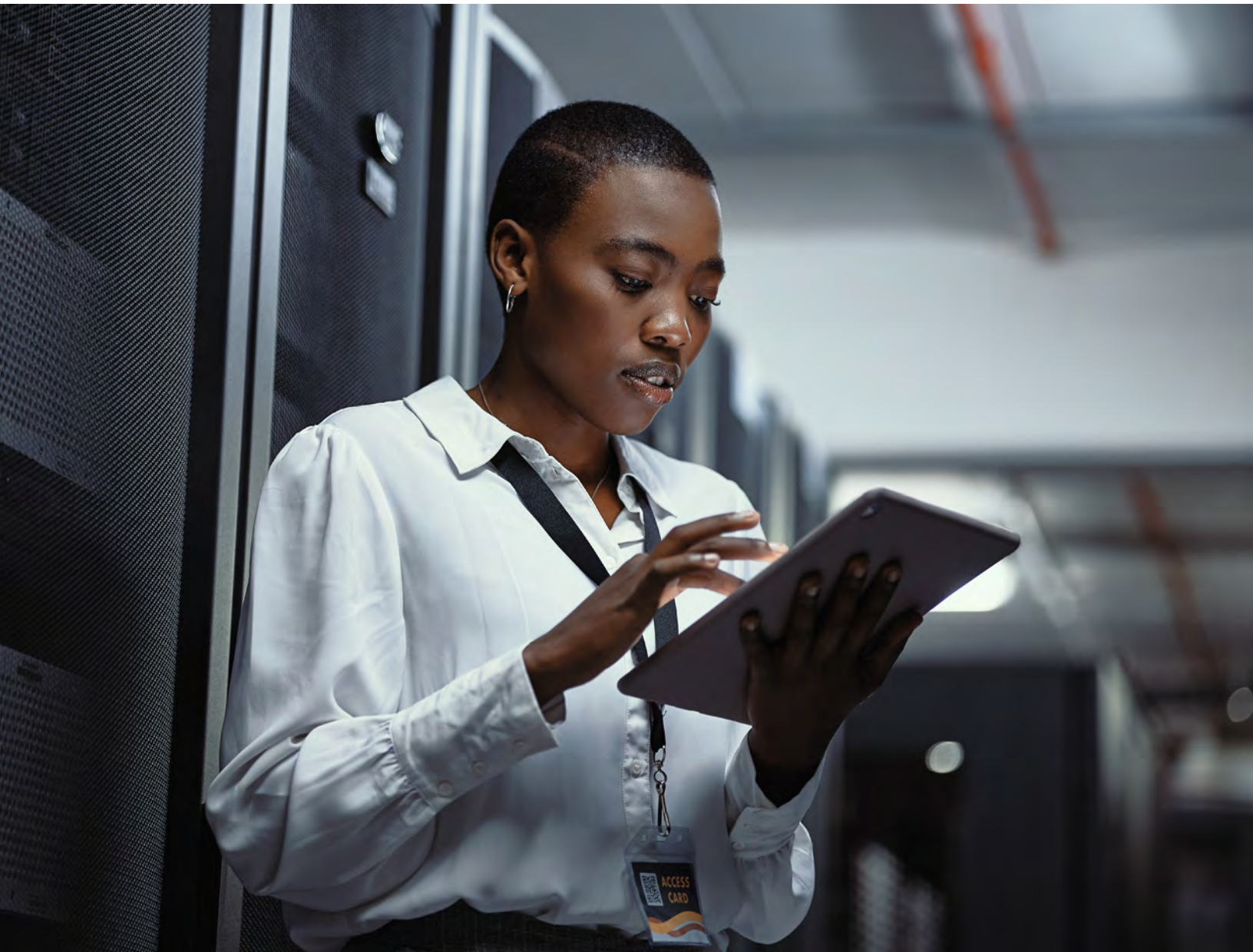
The Privacy Rule applies to PHI, which is defined as "individually identifiable health information" created, received, or transmitted by a covered entity or its business associate(s), in any form — electronic, paper, or oral. (See Covered Entities and Business Associates above.) This includes information related to an individual's past, present, and future physical or mental health condition; the provision of healthcare to an individual; or payment for the provision of healthcare to an individual. In a group

health plan context, PHI can include items such as participant diagnoses, claim amounts, dates of service, provider names, and claim disputes. Electronic PHI (ePHI) is subject to additional standards under the Security Rule. (See Security Rule below.)

PHI is considered "individually identifiable" if it either directly identifies the individual or if there is a reasonable basis to believe it can be used to identify the individual. The regulations list 18 types of identifiers that make health information individually identifiable. These include common data points such as names, addresses, birth dates, Social Security numbers, and full-face photographic images, as well as less obvious ones like IP addresses, biometric identifiers, and other unique identifying numbers or characteristics. If any of these identifiers are present in connection with health information, the data is considered PHI and is subject to the Privacy Rule.

The Privacy Rule provides that a covered entity may not use or disclose PHI except 1) as permitted under HIPAA, 2) as authorized in writing by the individual it pertains to, or 3) as required by the law. (See Permitted Uses and Disclosures for Plan Sponsors below.)

De-Identified Health Information. There are no restrictions on the use or disclosure of health information that has been de-identified. The rules establish two ways to de-identify information: either as formally determined by a qualified statistician or (as a safe harbor) by formally removing any or all 18 identifiers as they pertain to an individual, their family, their household members, and their employer.



Employment Records. The Privacy Rule excludes from the definition of PHI employment records maintained by a covered entity in its capacity as an employer rather than as a health plan. (See Employer's Role above.) This means that even if the same information exists in both employment and health plan records, it is only considered PHI when it is created, received, maintained, or transmitted by the group health plan (or its business associate) for plan-related purposes. For example, an employee's diagnosis may be PHI when used to process a health plan claim, but not PHI when included in response to a request for medical leave or workplace accommodation. The context in which the information is held determines whether HIPAA applies.

Employment-related records that are not PHI include sick leave documentation, ADA reasonable accommodation requests, disability claims, FMLA medical certifications, life insurance evidence of insurability, drug test results, vaccination status, and pre-employment physicals. These records are not subject to the Privacy and/or Security Rules but may be subject to other laws such as the ADA or FMLA. For example, covered employers are required to treat as strictly confidential all records and documents relating to FMLA medical certifications of employees or their family members and must segregate these from general personnel files. (See the DOL's FMLA Employer Guide for more information on this topic.)

PPI Observation	**Dual Roles.** Employers that sponsor group health plans should be mindful of their dual roles as both employers and sponsors of group health plans. Under privacy provisions, the group health plan is considered a separate legal entity from the employer (even if the employer administers the plan). While the Privacy Rule does not directly regulate employers, it does govern how and under what conditions a group health plan may disclose PHI to the plan sponsor. Specifically, a plan may share PHI with the employer only to support plan administration functions — and only if the employer certifies that it will safeguard the information in accordance with HIPAA and will not use it for employment-related purposes. For example, an employer may receive PHI to audit claims processing but may not use that same information to make employment decisions. Self-insured and hands-on fully insured plan sponsors should ensure that their plan documents include this required certification language.

There may be limited situations where the administrative needs of an employment-related matter and the group health plan overlap. For example, if an employee is unable to respond to a disability claim, an employer might try to obtain medical information from the group health plan to substantiate the claim. In such cases, any information disclosed by the plan is considered PHI, subject to privacy and security provisions. The plan may only release information to the employer if the individual provides a valid authorization (see the discussion below on Permitted Uses and Disclosure of PHI for Plan Sponsors). Without a valid authorization, the disclosure is impermissible.

Enrollment Information. Enrollment and disenrollment information that is created or received by the group health plan is considered PHI. However, this type of information is afforded some relief from the use and disclosure restrictions under the Privacy Rule. A group health plan or health insurer may disclose enrollment or disenrollment information to the plan sponsor without jeopardizing a plan's hands-off PHI status. For example, the health insurer for a fully insured high deductible health plan may provide a list of enrolled employees along with coverage tier to the plan sponsor to facilitate health savings account contributions. This is true even for plans where the enrollment function is performed by a TPA or another business associate. Furthermore, enrollment information collected by an employer for administrative functions – such as facilitating payroll deductions – is not considered PHI, provided it has not been received from the group health plan or a business associate.

Summary Health Information. Summary health information is information that summarizes claims history, claims expenses, or types of claims experience of group health plan participants. It is stripped of most individual identifiers (although it can include a zip code). Plan sponsors of fully insured group health plans may request and use summary health information for the limited purposes of obtaining premium bids (i.e., "marketing" the insurance) or of modifying the plan. These limited uses do not impact the plan's hands-off PHI status, provided the information is used solely for these purposes.

6. Permitted Uses and Disclosures for Plan Sponsors

A covered entity (such as a group health plan) may use and disclose PHI for treatment, payment, and healthcare operations without an individual's authorization. These permitted uses enable the plan and its workforce to carry out essential functions without creating unnecessary barriers to the delivery of and payment for healthcare. Essential functions include coordinating care, processing claims, managing benefits, and ensuring payment for services.

- **Treatment** is defined by HIPAA as the provision, coordination, or management of healthcare and related services among healthcare providers; consultation between healthcare providers regarding a patient; or the referral of a patient from one healthcare provider to another.
- **Payment** includes activities of healthcare providers and health plans to get paid for services. For group health plans, this also covers tasks such as determining eligibility or enrollment, processing claims, reviewing for medical necessity, and handling billing.
- **Healthcare operations** include the administrative, financial, and legal activities necessary for a covered entity to run its business and support treatment and payment. The Privacy Rule lists the following activities as covered healthcare operations: case management, care coordination, performance evaluation, credentialing and accreditation, medical reviews and audits, and other business management and general administrative activities of the entity.

A covered entity may disclose PHI to another covered entity if each entity has or had a relationship with the individual who is the subject of the information and the PHI pertains to that relationship.

PPI Observation	**Medical Emergency and Sharable Information.** Beyond disclosures between covered entities, the Privacy Rule also addresses situations where information may be shared with individuals involved in a participant's care. Plan sponsors may receive inquiries from family or personal representatives during an employee's medical emergency. The Privacy Rule permits covered entities to share PHI directly relevant to a person's involvement in the individual's care. If the participant is present and agrees – or when given the opportunity does not object – the plan may share information. Disclosure is also allowed if the plan reasonably infers, based on professional judgment, that the participant would not object. For example, a family member helping with claims after an accident may be given information about the employee's medical plan enrollment.

National Priority Purposes. The Privacy Rule permits the use and disclosure of PHI for certain specified purposes that are outside of the healthcare context but serve the public interest. This includes uses and disclosures made in the following circumstances:

- For public health activities, including disease tracking and child abuse reporting
- To aid victims of abuse, neglect, or domestic violence
- For health oversight activities such as audits and investigations
- As ordered by a court or judge in a judicial or administrative proceeding
- In response to law enforcement
- To funeral directors, coroners, and medical examiners regarding a deceased person
- For organ/tissue donation and transplant
- For certain research purposes
- In response to a serious threat to health or safety
- For national security, military missions, or other essential government functions
- For workers' compensation

PPI Observation	It is rare that the employer sponsor of a group health plan would be in the position to respond to any of the national priority PHI requests listed above. If such a request is received, it should be promptly forwarded to the insurer or TPA for appropriate handling.

The requested PHI can be provided to public authorities who are legally authorized to receive such reports. The specific rules and conditions around each of these types of purposes vary depending on the unique circumstances.

PPI Observation	**Reproductive Healthcare.** In April 2024, HHS finalized a rule amending the Privacy Rule to prohibit the use or disclosure of PHI for investigations or legal actions related to legal reproductive healthcare. This included restrictions on identifying individuals for such purposes. However, in June 2025, a federal court vacated the rule. As a result, the special protections for reproductive health information are no longer in effect. Group health plans should now comply with the standard Privacy Rule, which does not include specific limitations on disclosing PHI for reproductive care beyond the general privacy requirements.

Minimum Necessary Standard. In most cases, permitted uses or disclosures of PHI are subject to a minimum necessary standard. This means a covered entity must make reasonable efforts to use, disclose, or request only the minimum amount of PHI needed to accomplish the intended purpose.

This requirement does not apply to the following circumstances:

- Disclosures to or a request by a healthcare provider for treatment
- Disclosures to an individual who is the subject of the information or to the individual's personal representative
- Uses or disclosures made pursuant to an authorization
- Disclosures to HHS for complaint investigation, compliance review, or enforcement
- Uses or disclosures required by law
- Uses or disclosures required for compliance with other Privacy and Security Rules

Each covered entity must create and implement policies and procedures that apply the minimum necessary standard in practice to its own organization. Those policies should reflect who at the organization should have access to which types of PHI and in what situations. For example, individuals in one department may need access to some, but not all, levels of PHI that would be available to members of the workforce in another department.

A plan sponsor may rely on the judgment of other covered entities, their business associates, and public officials that any request for PHI is limited to the minimum amount of information that is needed. A disclosure of PHI that exceeds the minimum necessary standard is itself a violation of the Privacy Rule. (See Penalties below.)

7. Required Disclosures

A covered entity is required to disclose PHI in two situations: 1) to individuals or their personal representatives when specifically requested and 2) to HHS as part of an investigation or enforcement action. (See Individuals' Rights Under HIPAA for an overview of a participant's right to request access to their own PHI.) HHS's enforcement protocols and the penalties associated with violations of the Privacy and Security Rules are discussed in greater detail below.

8. Individual Authorization

If a plan or its employer sponsor wishes to use or disclose a participant's PHI for purposes other than treatment, payment, healthcare operations, or national priority purposes, a valid, signed authorization from the participant is required. A valid authorization must be written in plain language and include certain core elements to ensure that individuals understand and consent to the use or disclosure of their protected health information, including:

- A description of the information to be disclosed.
- The name of the disclosing entity.
- The recipient of the information.
- The purpose of the disclosure.
- An expiration date or event.
- A statement of the individual's right to revoke the authorization.
- The individual's (or personal representative's) signature and date.

HHS has not provided a model authorization; thus, any form that contains these elements will satisfy the requirement.

A covered entity generally may not condition treatment or payment on receiving authorization from an individual, except in certain circumstances. A group health plan may, for example, condition enrollment on a participant's providing authorization for the use of PHI for underwriting purposes.

Psychotherapy notes are subject to extra protection under the Privacy Rule. A covered entity (including a group health plan) may not use or disclose psychotherapy notes without authorization – even for treatment, payment, or healthcare operations – except in limited circumstances. HIPAA defines psychotherapy notes as the notes recorded in any medium by a mental health professional during or as a result of a counseling session. Crucially, they must be separated from the rest of the medical record to be afforded this heightened level of protection. They do not include supplementary data such as prescribed medications, counseling times or frequency, clinical test results, or summary information.

9. Individuals' Rights Under HIPAA

The HIPAA Privacy Rule grants five core rights to individuals with respect to their own PHI: access, accounting, amendment, restriction, and confidential communication.

Access. Individuals have the right to access and obtain a copy of their PHI maintained by a covered entity, upon request. This includes records used to make decisions about them, such as enrollment, payment, claims, and case management. Certain types of information – like psychotherapy notes, information related to legal proceedings, and certain laboratory and research results – are excluded. Covered entities may charge a reasonable fee for copies and mailing.

PPI Observation	**Parental and Spousal Rights.** The Privacy Rule gives a parent the right to access the medical records of their minor child, unless state law or specific circumstances limit that right. These limits (as permitted by state or federal law) include when the minor consents to care without parental involvement, receives care by court order, or has a confidential agreement with the provider. Access may also be denied if disclosure could endanger the child. For adult dependents, including spouses, PHI cannot be shared without written authorization, except in limited emergency situations. Note that the group health plan is responsible for ensuring that disclosures are permitted and appropriately authorized, particularly with respect to minors or adult dependents, even if the request for the information comes from the parent or spouse in an official or routine capacity. Requests for PHI may sometimes be directed to the plan sponsor (i.e., the employer), especially if the requester is seeking a workaround to obtain information from the group health plan. Because the plan sponsor is not a covered entity and generally does not have access to PHI, it must be especially cautious not to respond to such requests unless the disclosure is explicitly permitted under HIPAA — for example, when performing limited plan administration functions under a compliant plan document. See Permitted Uses and Disclosure of PHI for Plan Sponsors above and Restriction below. Furthermore, self-insured group health plans and hands-on plan sponsors should implement safeguards to prevent inadvertent disclosures. An unauthorized disclosure of PHI could constitute a breach under the Privacy Rule, triggering notification obligations to affected individuals, HHS, and more. See The Breach Notification Rule below.

Accounting. Individuals may request an accounting of the disclosures of their PHI made by the covered entity or its business associates, excluding treatment, payment, healthcare operations, or those authorized by the individual. This right applies to disclosures for purposes such as legal proceedings or health oversight or in response to subpoenas. The accounting must cover disclosures made within the six years prior to the request.

Amendment. Individuals may request that covered entities amend the PHI in their designated record set if it is inaccurate or incomplete. If granted, the covered entity must share the amended PHI with others who rely on it. If denied, the individual must receive a written explanation and be allowed to add a statement of disagreement to their record.

Restriction. Individuals have the right to request that a covered entity restrict the use or disclosure of their PHI for treatment, payment, and healthcare operations, as well as to family members or other persons involved in their care. Healthcare providers must agree to such a restriction if the individual pays in full out-of-pocket for a service and requests that the related PHI not be shared with the group health plan. However, group health plans are not subject to this restriction. While individuals may request restrictions from a group health plan, the plan is not required to agree to the request.

Confidential Communications. Individuals are permitted to request an alternative means of communication of their PHI from the covered entity. For example, a participant may request that claims information be sent to a separate address or be communicated by email instead of post. The covered entity is required to accommodate the request if the individual indicates that they could otherwise be endangered.

10. Administrative Requirements

Employer-sponsored group health plans are also responsible for implementing a series of administrative protocols that form the backbone of their privacy compliance program. These requirements are not one-size-fits-all. The Privacy Rule acknowledges the range of covered entities, which vary by size, complexity, and exposure to PHI, and allows for flexibility in how these standards are met.

As mentioned above, fully insured hands-off plans are largely exempt from these administrative obligations. All self-insured group health plans and hands-on fully insured plans must implement the following items. For a discussion of hands-on and hands-off fully insured plans, see Hands-Off Fully Insured Plans above.

Privacy Policies and Procedures. Group health plans must establish and maintain written policies and procedures (typically a policies and procedures document) that outline how they will comply with the Privacy Rule. These protocols form the foundation of the plan's broader privacy compliance efforts. A key component of these procedures is adherence to the minimum necessary standard, which requires covered entities to limit the use, disclosure, and request of PHI to the minimum amount necessary to accomplish the intended purpose. Policies should clearly define how this standard is applied across various operational areas, including workforce access controls, data sharing practices, and business associate relationships. See Minimum Necessary Standard above.

PPI Observation	HHS has not provided a model policies and procedures document. While plan sponsors often rely on HIPAA compliance vendors for templates or model documents, it must be specifically customized to reflect the covered entity's structure, operations, and privacy practices. It is essential that the procedures described in the document accurately match those carried out in practice. As a result, policies and procedures documents can differ significantly from one plan to another, depending on the organization's size, complexity, and level of involvement with PHI.

Policies and procedures documentation should be updated as needed to reflect changes in the organization or its handling of PHI. A general best practice is to review this documentation annually in connection with other routine reviews of organizational policies.

Notice of Privacy Practices. Group health plans must provide participants with a Notice of Privacy Practices describing how the plan may use and disclose PHI, along with a statement of its obligation to protect that information. The notice must also outline individuals' rights under HIPAA as well as contact information for submitting complaints and inquiries.

HHS maintains a Model Notice of Privacy Practices, which must be customized to the covered entity's specific structure and practices. Versions of the notice in multiple formats, with text in English or Spanish and instructions for completion, can be found at Model Notices of Privacy Practices | HHS.gov.

The notice must be provided upon enrollment and posted online with other benefits materials, and participants must be reminded of the notice's availability at least once every three years. For more information on group health plan notification responsibilities, see the PPI publications **Required Group Health Plan Notices Overview** and **Required Group Health Plan Notices Chart**.

PPI Observation	Self-insured group health plans are directly responsible for maintaining and distributing the Notice of Privacy Practices. Hands-on fully insured health plans must maintain a notice but only provide a copy to participants upon request. They will also receive a notice from the health insurer. For hands-off fully insured plans, the insurer typically distributes the notice, but the plan sponsor must still ensure that participants are informed about its availability.

Workforce Training and Management. Employer-sponsored group health plans must ensure that any workforce members who access PHI are trained in the organization's policies and procedures, to the extent necessary for them to perform their job functions. Training must be provided:

- Within a reasonable period after a new workforce member is hired.
- Whenever there is a material change to the plan's policies and procedures that affects their responsibilities.

Plans must also implement and enforce a sanctions policy for workforce members who fail to comply with privacy requirements. Training expectations and disciplinary procedures should be documented in the plan's HIPAA policies and procedures.

PPI Observation	Although HIPAA does not specify how often training must occur, as a best practice, many plan sponsors choose to conduct regular refresher sessions annually to reinforce compliance and reduce risk. Following a policy violation, some plans require retraining as part of the corrective action to reinforce accountability and a culture of compliance.

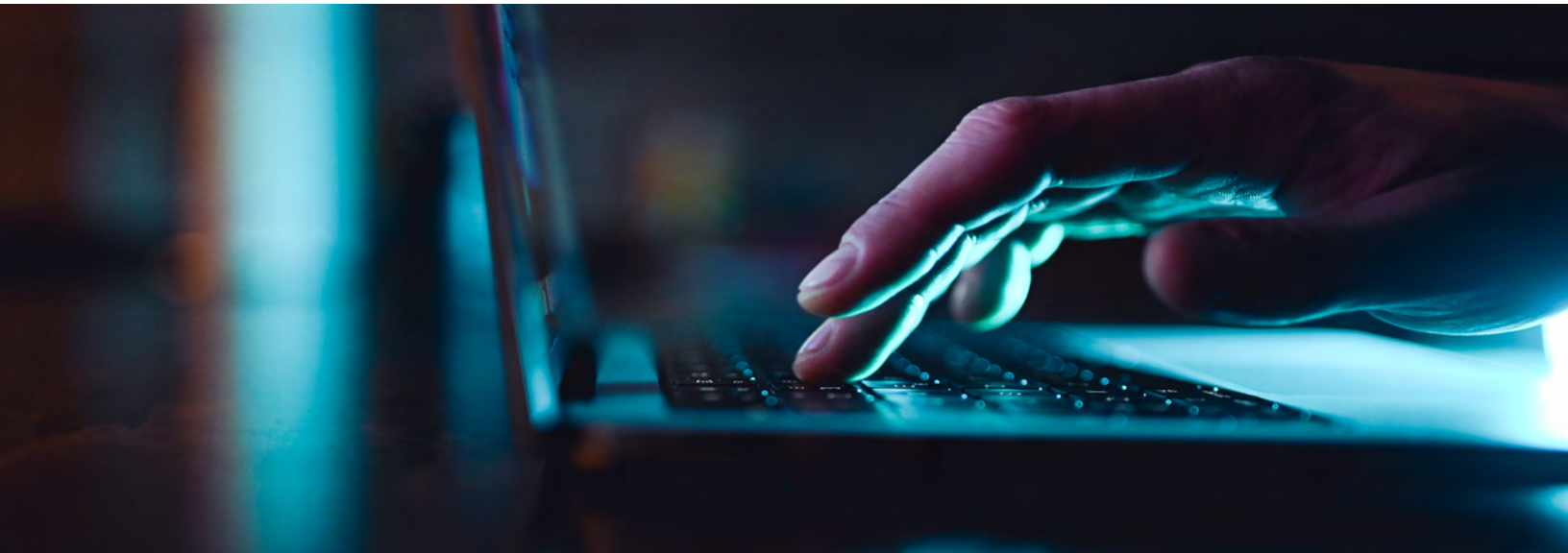
Privacy Official. The plan sponsor must designate a Privacy Official (also known as a Privacy Officer) responsible for developing, implementing, and overseeing the plan's privacy policies and procedures. Generally, the individual serves as the primary contact for privacy-related inquiries and complaints, coordinates workforce training, and ensures the plan's ongoing compliance with the Privacy Rule.

Complaints. The plan must have a process for participants to lodge complaints about its compliance with its policies and procedures or the Privacy Rule. The complaint process must be explained in the Notice of Privacy Practices. Participants may also bring complaints directly to HHS.

Retaliation and Waiver. The plan may not retaliate against participants for filing complaints or exercising their rights under the Privacy Rule, nor may it condition eligibility or coverage on a participant's waiver of those rights. Even though fully insured hands-off plans have no access to PHI, they are nonetheless prohibited from engaging in retaliation or seeking a waiver with respect to participant rights under HIPAA.

Documentation and Record Retention. The plan must maintain its policies and procedures, Notice of Privacy Practices, complaints documentation, and other HIPAA activities for at least six years from the date of their creation or last effective date.

PPI Observation	Many of the Privacy Rule obligations can more easily be managed with the support of a reputable vendor specializing in privacy compliance. Vendors often provide policies and procedures templates and training programs, though the plan sponsor must take an active role in customizing those resources and monitoring the vendor's performance. Importantly, even when using a vendor, the covered entity retains full responsibility for compliance.



III. The Security Rule

Under the HIPAA Security Rule, plan sponsors must implement certain administrative, physical, and technical safeguards to protect PHI that is maintained or transmitted in an electronic format, known as electronic PHI or ePHI. Specifically, these safeguards aim to accomplish four goals: 1) ensure the confidentiality, integrity, and availability of ePHI; 2) protect against reasonably anticipated threats to the security of ePHI; 3) protect against reasonably anticipated unauthorized uses or disclosures of ePHI; and 4) ensure compliance with these provisions by the workforces of covered entities and business associates.

This guide provides a high-level overview of the Security Rule for plan sponsors to understand the scope of their responsibilities. It is not meant to serve as a comprehensive guide to compliance. Like with the Privacy Rule, unless they have privacy experts on staff, plan sponsors often rely on HIPAA compliance vendors and legal counsel to satisfy the Security Rule's requirements. Plan sponsors must also coordinate with information technology experts familiar with how ePHI is created, maintained, and transmitted by the organization.

Also like the Privacy Rule, the Security Rule is designed to be flexible to enable organizations to implement policies, procedures, and technologies that are appropriate for their particular ePHI risks. The administrative, physical, and technical safeguards adopted by a group health plan should be adjusted as the plan, the organization as a whole, and the HIPAA regulations evolve over time. The entity must continually review and update their security measures to stay ahead of emerging cybersecurity threats.

PPI Observation	The increase in remote work provides additional HIPAA security challenges for group health plan sponsors. An entity's administrative, physical, and technical safeguards should be customized to reflect the reality of their employees' needs. While the Security Rule does not define specific solutions (such as multifactor authentication for remote access to ePHI), HIPAA does require covered entities to continually assess whether stronger protocols are necessary. A successful risk analysis will consider whether heightened technical safeguards are warranted to protect a more remote employee population from cyberattacks.

11. Administrative Safeguards

Risk Analysis and Management. The Security Rule's administrative safeguards require a group health plan to perform an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI. The risk analysis is the first step in Security Rule compliance, allowing the plan to identify potential risks and vulnerabilities to be addressed by other Security Rule safeguards. After completing the risk analysis, the group health plan can then determine which security measures are reasonable and appropriate to implement for managing those risks. This includes tracking access to ePHI, reviewing records to detect security incidents, periodically evaluating the effectiveness of security measures put in place (and modifying them as necessary), and regularly reevaluating potential risks to ePHI.

PPI Observation	HHS has created the HIPAA Security Risk Assessment Tool to help small- and medium-size organizations comply with the Security Rule: Security Risk Assessment Tool | HealthIT.gov. Plan sponsors should consider the following steps as they embark on creating the risk analysis: 1) identify all ePHI created, received, or transmitted by the organization; 2) identify the external sources of ePHI, including vendors and consultants; and 3) identify the human, natural, and environmental threats to information systems that contain ePHI.

Other Administrative Safeguards. Other administrative safeguards under the Security Rule include:

- Designating a security official (someone familiar with the plan's IT systems) responsible for developing and implementing the Security Rule policies and procedures.
- Implementing security policies and procedures (e.g., password protection, access logs, system audits) to ensure employees who handle ePHI have authorized and appropriate access.
- Implementing security policies and procedures to ensure access to ePHI is only authorized when necessary (similar to the Privacy Rule's "minimum necessary" standard).
- Implementing security policies and procedures to address security incidents (see The Breach Notification Rule section below for information on incidents that are considered unauthorized access or disclosure of ePHI).
- Training all employees on security policies and procedures and applying sanctions for violations.
- Establishing procedures for responding to emergencies or other damage to information systems that contain ePHI (e.g., backing up ePHI, restoring lost data, protecting ePHI during the emergency).
- Performing periodic assessments of how well security policies and procedures meet the requirements of the Security Rule.
- Confirming BAAs are in place before permitting a business associate to create, receive, maintain, or transmit a plan's ePHI (including a contractual requirement for the business associate to report to the plan any known security incident).

12. Physical Safeguards

The Security Rule requires group health plans to implement certain physical measures to protect the organization's ePHI systems, facilities, and equipment from natural hazards, environmental threats, and unauthorized intrusion. These physical safeguards include policies and procedures that:

- Limit unauthorized physical access to facilities that house electronic information systems (e.g., a locked office door with a key card access record).
- Specify proper use of and physical safeguards for workstations that can access ePHI.
- Govern the receipt, removal, and movement (including final disposal) of hardware and electronic media that contain ePHI.

13. Technical Safeguards

The Security Rule requires group health plans to implement policies for the use of technology that serves to protect and control access to ePHI. These technical safeguards include policies and procedures that:

- Control access of electronic information systems so that only authorized persons may access ePHI.
- Include hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI and ensure that ePHI is not improperly altered or destroyed.
- Verify that a person seeking access to ePHI is who they say they are.
- Guard against unauthorized access to ePHI that is transmitted over an electronic network.

PPI Observation	In December 2024, HHS published proposed regulations modifying the Security Rule to strengthen cybersecurity protections for ePHI. The proposed rule arrived on the heels of HHS's January 2024 Cybersecurity Performance Goals, a set of voluntary guidance published with the goal of helping covered entities strengthen their cyber resiliency practices. Once finalized, the new rules would include mandates such as specific compliance time periods for existing requirements, enhanced risk analysis provisions, the use of multifactor authentication, and annual internal compliance audits. Though the proposed rule was issued at the end of the previous presidential administration, cybersecurity is an issue with bipartisan support. Group health plan sponsors should evaluate their current cybersecurity protections and consider making adjustments in light of the voluntary guidance and proposed rule. For more information, see HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information | HHS.gov.

IV. The Breach Notification Rule

Established by the HITECH Act of 2009, the HIPAA Breach Notification Rule requires covered entities and business associates to follow certain procedures after a breach of unsecured PHI. While the Privacy and Security Rules already require regulated entities to mitigate the harmful effects of any violations, the Breach Notification Rule expands upon those provisions and adds specific notification requirements. This guide provides a high-level overview of the Breach Notification Rule for plan sponsors to understand the scope of their responsibilities. It is not meant to serve as a comprehensive guide to compliance. In the event of a suspected breach, plan sponsors should work with legal counsel to assess the incident and follow through with required breach notifications.

14. Definition of Breach

A breach is defined by the HITECH Act as the acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA that compromises the security or privacy of the information. Any impermissible use or disclosure of PHI is presumed to be a breach unless the plan can demonstrate that there is a low probability that the PHI has been compromised. This determination must be made through the performance of a breach risk assessment that considers four key factors:

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

Given the strict timing requirements of the breach notifications, the risk assessment must be performed quickly and efficiently. The plan may therefore elect to provide notification of the breach before fully completing all four parts of the breach risk assessment.

Breach Exceptions. HIPAA provides an exception for three types of impermissible uses or disclosures of PHI that do not meet the definition of breach and therefore do not require notification. Those exceptions are:

1. Unintentional acquisition, access, or use of PHI by a workforce member or other authorized person that was made in good faith and within the scope of their authority, as long as the information is not further used or disclosed.
2. Inadvertent disclosure of the PHI by one person authorized to access the plan's PHI to another person authorized to access the same plan's PHI, as long as the information is not further used or disclosed.
3. Where the plan has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

Unsecured PHI. Any breach of PHI where the information remains unsecured is subject to HIPAA's breach notification requirements discussed below. PHI is considered unsecured if it has not been rendered unusable, unreadable, or indecipherable to unauthorized persons.

PPI Observation	Any impermissible access, acquisition, use, or disclosure of PHI that has been properly encrypted or destroyed through an HHS-approved technology and methodology, such as by encrypting ePHI and destroying all PHI and ePHI that is no longer in use, is exempt from the breach notification requirements. For example, if a plan workforce member accidentally sends an email with ePHI to the wrong (unauthorized) person, they will not have to follow the breach notification protocols as long as that email was encrypted. For that reason, many plan sponsors consider it a best practice to implement HIPAA-compliant software that analyzes all outgoing emails and automatically encrypts those that may contain ePHI.

A group health plan sponsor that uses and discloses PHI should consider contracting with a shredding company to eliminate their paper PHI and should work with a reputable technology solutions company to securely and effectively store, transmit, and destroy their ePHI.

15. Notification Requirements

If a plan discovers or suspects a breach of PHI, conducts a risk assessment, determines that none of the exceptions outlined above apply, and finds that the information is indeed unsecured, then the plan's next step will be to provide proper notification. Notices must be provided to three different recipients depending on the number of participants involved: the affected individuals, HHS, and (potentially) the media.

Notice to Individuals. The plan must notify all participants whose unsecured PHI was improperly used or disclosed as soon as possible, but in no case later than 60 days following the discovery of the breach. The notice must include the following:

- A brief description of what happened
- The types of information involved
- The steps individuals should take to protect themselves from potential harm
- A brief description of what the plan is doing to investigate, mitigate, and prevent further breaches
- Contact information for additional questions

Plan sponsors will want to ensure that the content of the notification does not itself constitute a breach of PHI. The notice should be provided in writing and sent by first-class mail, unless the participant has previously consented to electronic disclosures, in which case the notification can be emailed. If the plan has insufficient or out-of-date contact information for 10 or more of the affected individuals, then it must also either post the notice on their website for at least 90 days or publish the notice in local major media outlets.

Notice to HHS. The plan must notify HHS of all breaches online by submitting a breach report form at Breach Reporting | HHS.gov. For breaches that affect 500 or more individuals, the plan must submit this notification as soon as possible but in no case later than 60 days following discovery of the breach. For breaches that affect fewer than 500 individuals, the plan must include the breach on an annual log of all breaches that occurred during the calendar year and submit the log to the same website no later than 60 days following the end of the calendar year in which the breaches are discovered.

PPI Observation	HHS publicly maintains the log of all reported breaches that affected 500 or more individuals going back several years. This list can be viewed at U.S. Department of Health & Human Services - Office for Civil Rights.

Notice to the Media. For breaches that affect 500 or more residents of a state, the plan must provide notice of the breach in prominent media outlets that serve location(s) where the affected individuals reside. The notification should contain the same content as the individual notice and must also be provided as soon as possible but in no case later than 60 days following the discovery of the breach.

Business Associates. Upon discovery of a breach, a business associate must notify the plan as soon as possible and no later than 60 days following discovery. As the covered entity, the plan is still ultimately responsible for ensuring that proper notification is provided to participants, HHS, and the media (if applicable). However, the plan may delegate notification responsibilities to the business associate.

PPI Observation	To ensure there is no delay in providing required notices to individuals, HHS, and the media (if applicable), plans typically include a shorter deadline in their BAAs for business associates to notify the plan of possible breaches that occur at or by the business associate.

Group health plans should include risk assessment and breach notification protocols in their written HIPAA policies and procedures and ensure that workforce members are trained on the protocols. Pursuant to HIPAA's general recordkeeping requirements, plans should keep documentation of all risk assessments and breach notifications on file for at least six years. The plan must be able to demonstrate to HHS or a participant that a use or disclosure of unsecured PHI did not constitute a breach or that all required notifications were timely provided following the discovery of a confirmed breach.

V. Enforcement, Penalties, and Other Privacy Laws

16. Enforcement of Privacy, Security, and Breach Notification Rules

HHS's Office for Civil Rights (OCR) is the agency responsible for enforcing HIPAA's Privacy, Security, and Breach Notification Rules. OCR does so by investigating complaints filed by individuals, conducting compliance reviews and audits on covered entities to determine compliance, and providing education and outreach on HIPAA's requirements. OCR works with the DOJ to investigate possible criminal violations under HIPAA.

OCR will investigate complaints about HIPAA violations that occurred within the previous six years if the complaint is submitted within 180 days of when the complainant knew or should have known about the alleged violation. If OCR accepts a complaint for investigation and finds that the covered entity was not in compliance with HIPAA, they will attempt to resolve the case by obtaining voluntary compliance, corrective action, and/or a resolution agreement with the covered entity. The issues most often alleged in complaints are:

- Impermissible uses and disclosures of PHI.
- Lack of Security Rule safeguards of ePHI.
- Lack of patient/participant access to their own PHI.
- Use or disclosure of PHI that exceeded the minimum necessary standard.

The HITECH Act requires HHS to periodically audit covered entities and business associates for their compliance with the Privacy and Security Rules. Organizations are selected for audit by HHS at random. These audits allow HHS to examine mechanisms for compliance, identify best practices, and discover new risks and vulnerabilities with an eye towards breach prevention.

PPI Observation	HHS has initiated their 2024-2025 "Phase 3" HIPAA audits, which will target 50 covered entities and business associates. Specifically, these audits will review organizations' compliance with the Security Rule with respect to the threat posed by hacking, ransomware, and cyberattacks. OCR will publish an industry report summarizing OCR's findings after the 2024-2025 HIPAA audits are completed.

17. Penalties

OCR may impose a civil monetary penalty on a covered entity for failure to comply with the Privacy and Security Rules. Penalty amounts vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect.

	Minimum Penalty*	Maximum Penalty*	Calendar-Year Cap*
Tier 1: Lack of Knowledge	$141	$71,162	$2,134,831
Tier 2: Reasonable Cause and Not Willful Neglect	$1,424	$71,162	$2,134,831
Tier 3: Willful Neglect, Corrected Within 30 Days	$14,232	$71,162	$2,134,831
Tier 4: Willful Neglect, Not Corrected Within 30 Days	$71,162	$2,134,831	$2,134,831

*For penalties assessed on or after August 8, 2024. Penalties are indexed annually for inflation and may not exceed a calendar year cap for multiple violations of the same requirement.

A person who knowingly obtains or discloses PHI in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one year imprisonment. The criminal penalties increase to $100,000 and up to five years' imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years' imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain, or malicious harm.

18. Other Group Health Plan Privacy Laws

There are other privacy and security laws beyond HIPAA that protect the disclosure of individual health information by insurers, TPAs, and other group health plan service providers. On the federal level, these laws include the Gramm-Leach-Bliley Act, which requires financial institutions (including insurers) to safeguard nonpublic personal information (NPI), including PHI protected by HIPAA, and provide privacy notices to customers.

HIPAA is the only federal privacy law that applies directly to employers in their role as group health plan sponsors, but certain employment laws require employers to keep medical information confidential, even if the information is not received in relation to group health plan operations. The ADA prohibits discrimination based on disability, including in the employment context. Under the ADA, employers must treat medical information about employees and applicants (e.g., provided by an employee as part of an ADA accommodation, return to work assessment, or pregnancy or vaccination status disclosure) in a confidential medical record.

Many states have privacy laws that protect personal information generally, including but not limited to PHI, to extents that may be greater or lesser than HIPAA. Generally, HIPAA preempts state laws related to PHI that are less stringent. Conversely, state law supersedes HIPAA to the extent it provides protections or rights beyond what HIPAA requires. State privacy laws vary and fall outside the scope of this publication. Employers should closely review state privacy law requirements – such as individual rights, notifications, risk assessments, and prohibitions on discrimination – with legal counsel.

19. Summary

Employers sponsoring group health plans should be familiar with the full scope of HIPAA's privacy and security obligations. This is especially important for sponsors of self-insured and hands-on fully insured group health plans, which are subject to a range of administrative requirements, including:

- Identifying PHI and understanding the permitted uses and disclosures for treatment, payment, and healthcare operation under the Privacy Rule.
- Creating and maintaining written policies and procedures that describe the plan's compliance with HIPAA.
- Training workforce members on those policies and procedures, including the minimum necessary standard.
- Implementing the administrative, physical, and technical safeguards for ePHI as required by the Security Rule.
- Recognizing security incidents, performing risk assessments, and providing proper notifications in accordance with the Breach Notification Rule.

In their role as plan sponsors, employers are responsible for protecting and securing the PHI they access or maintain. Sponsors of self-insured and hands-on fully insured group health plans may choose to work with a HIPAA compliance vendor to help manage more complex operational requirements, but the ultimate responsibility remains with the covered entity.

20. Resources

Breach Portal | OCR

FMLA Employer Guide | DOL.gov

Guide to Privacy and Security of Electronic Health Information | HealthIT.gov

HIPAA for Professionals | HHS.gov

HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information | HHS.gov

Model Notices of Privacy Practices | HHS.gov

Security Risk Assessment Tool | HealthIT.gov

Appendix A

HIPAA Privacy and Security Compliance Overview for Self-Insured vs. Fully Insured Group Health Plans

This appendix provides an overview of key compliance distinctions under the HIPAA Privacy, Security, and Breach Notification Rules for self-insured and fully insured hands-off group health plans. The level of involvement with PHI determines the extent of compliance responsibilities under HIPAA. For fully insured group health plans that handle PHI (i.e., "hands-on" plans), generally both the plan and the insurer must comply with the same rules that apply to self-insured plans as outlined below. One notable exception is that distributing the Notice of Privacy Practices remains primarily the responsibility of the insurer.

Self-Insured Group Health Plan Sponsors (including HRAs and Health FSAs)

By definition, self-insured group health plans are hands-on with respect to PHI and therefore must comply with all HIPAA privacy administrative and breach notification requirements as well as security safeguards. In most cases, plan sponsors rely on HIPAA compliance vendors and legal counsel to satisfy the requirements unless they have HIPAA privacy and security experts on staff.

Key compliance considerations for self-insured plan sponsors include:

- **Evaluating how PHI is accessed, used, and disclosed.** This involves determining which workforce members have access to PHI and reviewing how that information is used, disclosed, stored, and transmitted. Plan sponsors must also identify business associates (e.g., vendors that create, receive, maintain, or transmit PHI on behalf of the plan) in order to assess whether BAAs are required. (See Managing Business Associate Agreements (BAAs) below.)
- **Designating a Privacy and Security Officer.** This individual typically oversees the plan's privacy policies and procedures, serves as the primary contact for HIPAA-related inquiries and complaints, coordinates workforce training, and supports ongoing compliance efforts. Depending on the organization's size and scope of PHI access, some plan sponsors establish a HIPAA Privacy and Security committee to assist with these responsibilities.
- **Engaging a HIPAA compliance vendor.** As noted above, plan sponsors often work with HIPAA compliance vendors to support implementation of the Privacy and Security requirements. These vendors may assist with the following requirements:
    - Drafting and adopting written policies and procedures
    - Training workforce members
    - Establishing complaint and anti-retaliation procedures
    - Implementing a sanctions policy for workforce noncompliance
    - Conducting a Security Rule risk analysis and establishing appropriate administrative, physical, and technical safeguards
- **Providing a Notice of Privacy Practices.** Self-insured group health plans are responsible for maintaining and distributing a Notice of Privacy Practices that describes how the plan may use and disclose PHI, outlines participants' rights under HIPAA, and includes contact information for inquiries and complaints. Plan sponsors may use the model notice provided by HHS at Notice of Privacy Practices for Protected Health Information | HHS.gov, customized to reflect the plan's structure and practices. If the sponsor offers both self-insured and fully insured plans, the notice should specify to which it applies. The notice must be provided upon enrollment and posted online with other benefits materials. Additionally, participants must be notified of its availability at least once every three years.
- **Amending the plan document.** To permit disclosures of PHI to the plan sponsor, the plan document must be amended to include language required under the Privacy Rule. The sponsor must also sign a certification agreeing to safeguard PHI and use it only for permitted purposes.
- **Managing Business Associate Agreements (BAAs).** Plan sponsors must review vendor relationships to determine whether a vendor performs functions or services on behalf of the plan that involve PHI (e.g., creating, receiving, maintaining, or transmitting PHI). Business associates are required to enter into a written agreement (a BAA) that outlines their responsibilities under the Privacy and Security Rules. Legal counsel typically assists with these agreements to ensure appropriate safeguards are in place.

- **Developing breach and security incident procedures.** Plan sponsors must establish protocols for identifying potential breaches, conducting risk assessments, and preparing notifications to affected individuals, HHS, and the media (if applicable). Plan sponsors must also confirm that their BAAs contain clear provisions outlining the business associate's responsibilities for breach identification, reporting, and notification. These procedures are generally documented in the plan's HIPAA Privacy and Security policies and procedures and are supported by workforce training.
- **Considering state privacy laws.** In addition to HIPAA's federal requirements, some states impose privacy laws that may be more stringent. Plan sponsors must work with legal counsel, and, where relevant, payroll or data vendors, to evaluate whether any state-specific obligations apply to the plan's handling of personal information.
- **Reviewing and updating policies and workforce training.** HIPAA Privacy and Security policies and procedures should be reassessed on a regular basis to reflect changes in the organization, its handling of PHI, and evolving regulatory or cybersecurity standards. Plan sponsors should conduct refresher training to reinforce compliance and support workforce awareness, especially following identified risks or material changes.

Hands-Off Fully Insured Group Health Plan Sponsors

Fully insured group health plans that are structured so that the plan sponsor does not access or manage PHI beyond enrollment, disenrollment, or summary health data are referred to as "hands-off" with respect to PHI. In such cases, the health insurer, not the plan sponsor, assumes primary responsibility for complying with most of the HIPAA Privacy Rule and all of the Security Rule requirements.

Key considerations for hands-off fully insured plan sponsors include:

- **Limiting PHI access.** The plan sponsor may receive enrollment and disenrollment data as well as summary health information (i.e., stripped of most individual identifiers) without triggering additional HIPAA obligations. To maintain a hands-off status, sponsors must avoid accessing PHI related to participant claims, appeals, or other health plan operations unless the individual has provided specific written authorization.
- **Confirming no ePHI is created, received, or transmitted by the plan sponsor (via the Security Risk Assessment Tool).** This may involve a conversation with the insurer to confirm that the insurer does not share any ePHI with the plan sponsor.
- **Engaging and maintaining HIPAA authorizations.** For any use or disclosure of PHI beyond enrollment, disenrollment, or summary health information, the plan sponsor must obtain a signed authorization from the affected individual. This includes situations where employees request assistance with claims or coverage issues that would otherwise involve PHI access.
- **Educating workforce members.** To preserve a hands-off approach, plan sponsors should educate workforce members who support the group health plan – such as HR professionals, benefits specialists, and finance staff – on the boundaries of permissible PHI access. Training should cover the basic requirements of the Privacy and Security Rules, how to identify PHI, and the potential administrative consequences of inadvertently becoming hands-on.
- **Facilitating awareness of the Notice of Privacy Practices.** Although the insurer is responsible for creating and distributing the Notice of Privacy Practices, the plan sponsor must ensure that participants are reminded of its availability and how to request a copy from the insurer at least once every three years. This reminder is sometimes included in annual enrollment materials or other routine benefits communications.
- **Documenting compliance.** Even though formal HIPAA Privacy and Security policies and procedures are not strictly required for plan sponsors that do not have access to PHI, some plan sponsors may want to memorialize compliance through a limited-scope written policy that confirms: the plan sponsor has no access to PHI or ePHI, the insurer is responsible for the Privacy Notice, the plan will comply with breach notification requirements, and the plan will not take retaliatory action against an individual for exercising their HIPAA privacy rights or require an individual to waive their HIPAA privacy rights.
- **BAAs with plan service providers.** Even though BAAs are not required for plan sponsors that do not have access to PHI, some plan sponsors may want to consider entering BAAs with service providers as a cautious approach in the event the plan sponsor later adds a self-insured benefit, such as an HRA, health FSA, or level-funded product (which is also generally considered a self-insured plan).

PPI BENEFIT SOLUTIONS

About PPI: PPI Benefit Solutions combines seasoned expertise with cutting-edge technology to deliver comprehensive, cost-effective solutions that simplify benefits administration for small and mid-sized employers. Our commitment to excellence is reflected in innovative services and collaborative partnerships with carriers and brokers. Together, we foster a dynamic benefits ecosystem that reduces administrative burden, drives business growth, and supports long-term organizational resilience.

For more information, visit **ppibenefits.com**.