Compliance Support from
the Professional at GBS

HIPAA Privacy & Security Compliance Toolkit

GBS
A Leavitt Group Company

Table of Contents

3 **1. Introduction**

5 **2. HHS Resources**

7 **3. Definitions**

9 **4. HIPAA Assessment**

11 **5. HIPAA Compliance Checklists**

15 **6. Basic Concepts**

21 **7. Privacy Requirements**

34 **8. Security Requirements**

41 **9. Breach Notification Requirements**

45 **10. Enforcement**

49 **11. Sample Documents**

This toolkit is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice. Any samples provided in this toolkit are for educational and illustrative purposes only. © GBS Benefits, Inc. All rights reserved.

1. Introduction

Introduction

This toolkit is intended to help employers that sponsor group health plans understand their compliance obligations under the Health Insurance Portability and Accountability Act (HIPAA). It also provides sample resources to help employers comply with HIPAA's documentation requirements for their group health plans.

What this Toolkit Covers

HIPAA is a broad federal law that includes rules for protecting the privacy and security of certain health information, which is called protected health information (PHI). HIPAA also includes notification requirements following a breach of PHI. This toolkit discusses the following rules, which are collectively referred to as the **HIPAA Rules**:

HIPAA Privacy Rule

- Sets national standards for when PHI may be used or disclosed
- Gives individuals certain rights with respect to their PHI

HIPAA Security Rule

- Includes standards that covered entities must implement to protect their electronic PHI (ePHI)

HIPAA Breach Notification Rule

- Requires covered entities to notify affected individuals, the Department of Health and Human Services (HHS) and, in some cases, the media, following a breach of unsecured PHI

While employers are not directly regulated by the HIPAA Rules, most employer-sponsored group health plans are subject to the HIPAA Rules' requirements to some degree. This means that employers that sponsor group health plans for their employees will usually have compliance obligations under the HIPAA Rules with respect to their group health plans. The extent of an employer's compliance obligations under the HIPAA Rules mainly **depends on two factors**:

- Whether the employer's health plan is **self-funded or fully insured**; and
- If the health plan is fully insured, whether the employer has **access to PHI or Substance Use Disorder (SUD) records** from the health insurance issuer (other than certain limited types of PHI).

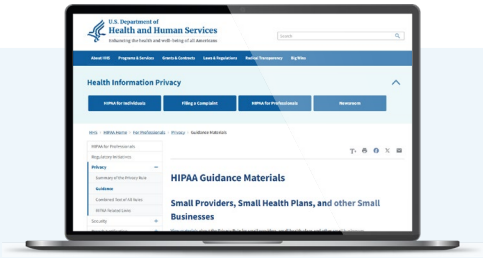
Key Points

- If an employer receives PHI from its health plan (for example, from the issuer or benefits administrator), the employer takes on ***significant responsibilities*** with respect to that PHI.
- Employers that sponsor **fully insured health plans** and **do not have access to PHI** (other than certain limited types) from their issuers have ***minimal compliance obligations*** under the HIPAA Rules.

2. HHS Resources

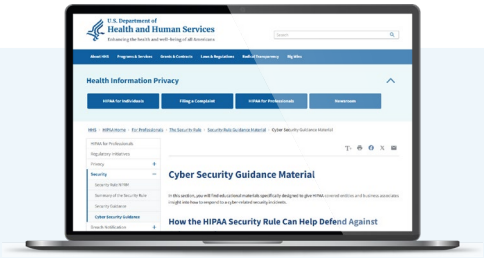
HHS Resources

In addition to this toolkit, there are resources available from the U.S. Department of Health & Human Services (HHS) to help covered entities comply with the HIPAA Rules. These resources are available through HHS' website on the following topic pages:



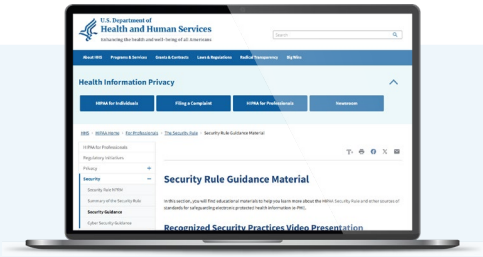
Guidance on the HIPAA Privacy Rules ›

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html



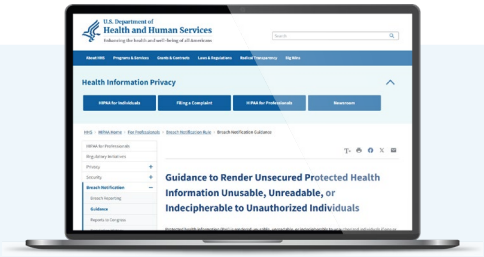
Cyber Security Guidance ›

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html



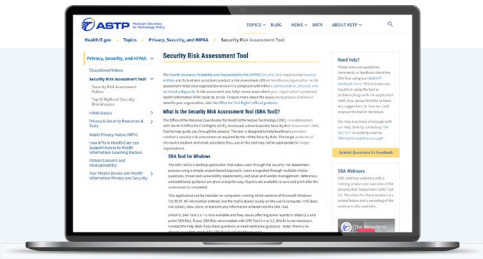
HIPAA Security Rule Guidance ›

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html



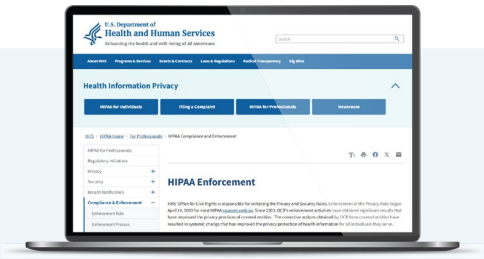
Breach Notification Guidance ›

https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html



Security Risk Assessment Tool ›

https://www.healthit.gov/providers-professionals/security-risk-assessment-tool



Compliance & Enforcement ›

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

3. Definitions

Definitions

The HIPAA Rules include many terms that have specific meanings. To understand the HIPAA Rules, refer back to these key definitions as you use the toolkit.

Availability – The ePHI is accessible and useable upon demand by an authorized person.

Business associate – A person or organization that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. This could include, for example, a third-party administrator or broker/consultant for a health plan. Prior to disclosing any PHI, the covered entity and business associate must enter into a written business associate agreement.

Confidentiality – The ePHI is not made available or disclosed to unauthorized people or processes.

Covered entity – A health plan, health care clearinghouse or health care provider that transmits PHI electronically. A self-funded health plan with fewer than 50 participants that is administered by the sponsoring employer is exempt from the HIPAA Rules.

Designated record set – A group of records maintained by or for a covered entity that includes the:

- Medical records and billing records about individuals maintained by or for a covered health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.

Electronic PHI (ePHI) – PHI that a covered entity (or business associate) creates, receives, maintains or transmits in electronic media.

HHS – The Department of Health and Human Services (HHS), the federal agency that is responsible for implementing and enforcing the HIPAA Rules.

"Hands-off" PHI – A fully insured health plan is hands-off PHI if the PHI it creates or receives from the health insurance issuer is limited to enrollment information, summary health information and information that is released pursuant to a HIPAA authorization. In this situation, most of the HIPAA compliance obligations fall on the health insurance issuer, and not on the employer-sponsored group health plan.

"Hands-on" PHI – A fully insured health plan is hands-on PHI if it creates or receives PHI from the issuer other than enrollment information, summary health information and information that is released pursuant to a HIPAA authorization. Health plans that are hands-on PHI will have significant responsibilities under the HIPAA Rules with respect to the PHI.

Integrity – The ePHI has not been altered or destroyed in an unauthorized manner.

Protected health information (PHI) – Individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity (or a business associate) and relates to the past, present, or future physical or mental health condition of an identified individual. Employment records are not considered PHI.

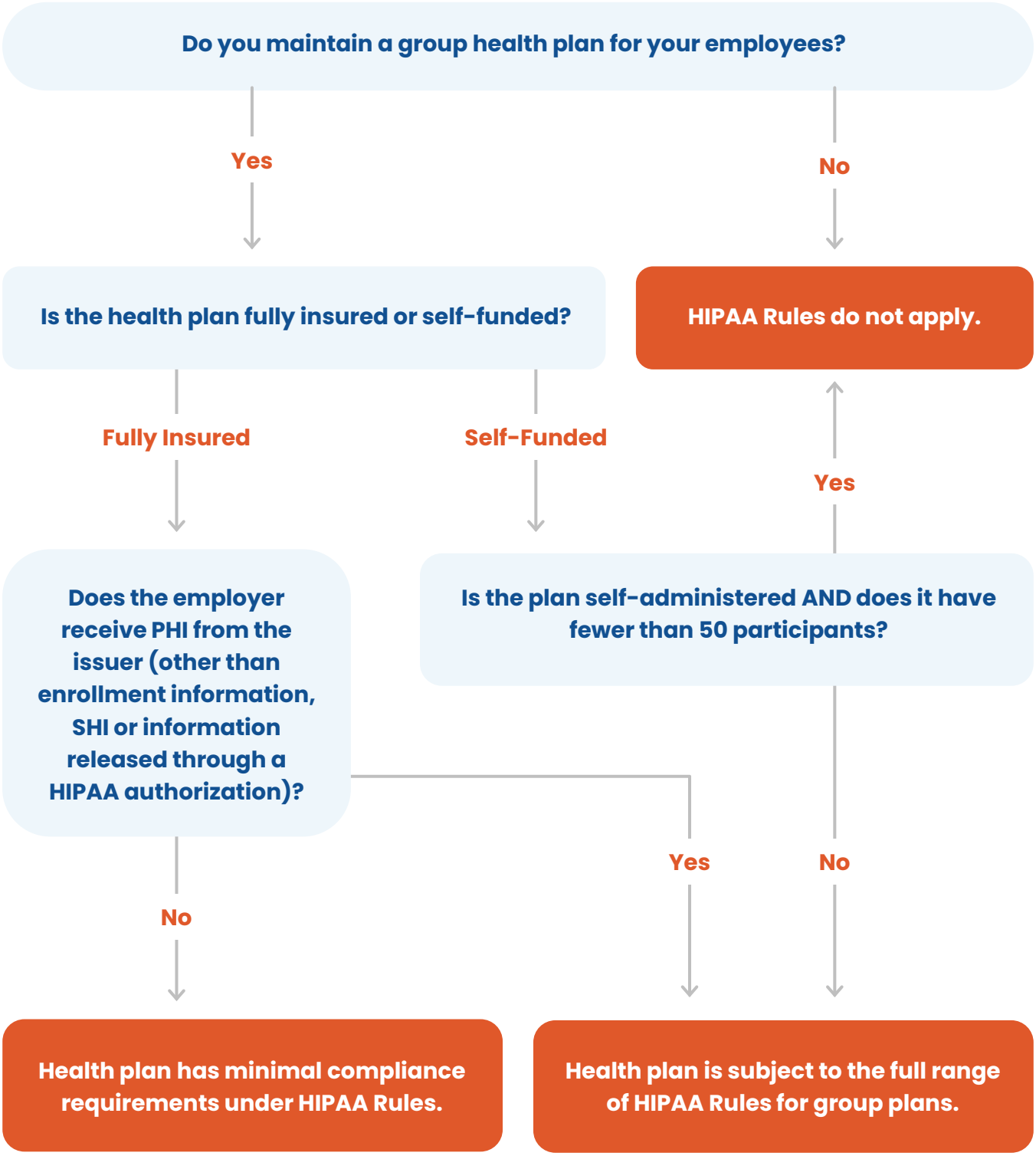
Summary health information (SHI) – Information that summarizes claims history, claims expenses or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five-digit ZIP codes.

Substance Use Disorder (SUD) Rule 2024 – Treats SUD records similarly to HIPAA mental health PHI.

4. HIPAA Assessment

HIPAA Assessment

To assess how the HIPAA Rules may apply to an employer-sponsored group health plan, employers should review their group health plans and their access to PHI. The following flowchart depicts these steps.



5. HIPAA Compliance Checklists

HIPAA Compliance Checklists

An employer is generally not subject to the HIPAA Rules when it performs employment-related functions, such as administering employee leaves of absence or fitness-for-duty requirements. However, the HIPAA Rules indirectly regulate employers in their role as health plan sponsors. When an employer receives PHI from its group health plan for plan administrative functions, the employer must agree to comply with certain requirements of the HIPAA Rules.

Employers should assess their group health plans to determine if the HIPAA Rules apply and, if so, to what extent. A HIPAA assessment flowchart is provided as part of this toolkit to help employers with this process. Also, key concepts and action items are explained throughout this toolkit. After performing a HIPAA assessment, employers should refer to the HIPAA checklist below that is applicable to them.

Fully Insured Health Plan – "Hands-off" PHI

- [ ] Establish a privacy policy prohibiting retaliation and waiver of rights.
- [ ] Perform a risk analysis regarding any ePHI that the group health plan creates or receives.
- [ ] Adopt appropriate administrative, technical and physical safeguards for the ePHI (these requirements are scalable).
- [ ] Designate a security official.
- [ ] Adopt a breach notification policy.

See the sample HIPAA policies for fully insured health plans that are hands-off PHI.

HIPAA Compliance Checklists

Fully Insured Health Plan – "Hands-on" PHI

- [ ] Implement policies and procedures that address the Privacy Rule's requirements, taking into account the health plan's size and types of activities involving PHI.
- [ ] Designate a privacy officer and a security official.
- [ ] Train workforce members on HIPAA policies and procedures.
- [ ] Adopt a sanctions policy for employees who fail to comply with applicable HIPAA requirements.
- [ ] Implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI and Substance Use Disorder (SUD) records.
- [ ] Amend the health plan documents to impose restrictions on the employer's use and disclosure of PHI and Substance Use Disorder (SUD) records.
- [ ] Maintain a Privacy Notice (must be provided upon request).
- [ ] Do not use PHI from the health plan in any employment-related action or decision or in connection with any other benefit plan.
- [ ] Comply with individual rights' requirements.
- [ ] Enter into business associate agreements, as necessary.
- [ ] Perform a risk analysis regarding any ePHI that the group health plan creates or receives.
- [ ] Adopt appropriate administrative, technical and physical safeguards for ePHI (these requirements are scalable).
- [ ] Adopt a breach notification policy.
- [ ] Maintain HIPAA documentation for at least six years.

See the sample HIPAA policies for fully insured health plans that are hands-on PHI and self-insured health plans.

HIPAA Compliance Checklists

Self-insured Health Plan

Self-insured health plans with fewer than 50 participants are exempt from the HIPAA Rules if they are self-administered.

- [ ] Implement policies and procedures that address the Privacy Rule's requirements, taking into account the health plan's size and types of activities involving PHI.
- [ ] Designate a privacy officer and a security official.
- [ ] Train workforce members on HIPAA policies and procedures.
- [ ] Adopt a sanctions policy for employees who fail to comply with applicable HIPAA requirements.
- [ ] Implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI and Substance Use Disorder (SUD) records.
- [ ] Amend the health plan documents to impose restrictions on the employer's use and disclosure of PHI and Substance Use Disorder (SUD) records.
- [ ] Provide a Privacy Notice.
- [ ] Do not use PHI from the health plan in any employment-related action or decision or in connection with any other benefit plan.
- [ ] Comply with individual rights' requirements.
- [ ] Enter into business associate agreements, as necessary.
- [ ] Perform a risk analysis regarding any ePHI that the group health plan creates or receives.
- [ ] Adopt appropriate administrative, technical and physical safeguards for ePHI (these requirements are scalable).
- [ ] Adopt a breach notification policy.
- [ ] Maintain HIPAA documentation for at least six years.

See the sample HIPAA policies for self-insured health plans and fully insured health plans that are hands-on PHI.

6. Basic Concepts

Basic Concepts

Who is Subject to the HIPAA Rules?

The HIPAA Rules apply to **covered entities**. Covered entities include:

Health Plans	Health Care Clearing Houses	Most Health Care Providers

The HIPAA Rules also apply to other entities that perform functions or activities on behalf of a covered entity when those services involve access to, or the use or disclosure of, PHI. These entities are called **business associates**.

Impact on Employers

An employer is not a covered entity under the HIPAA Rules. This means that an employer is generally not subject to the HIPAA Rules when it performs employment-related functions, such as administering employee leaves of absence or fitness-for-duty requirements. However, the HIPAA Rules **indirectly regulate employers in their role as health plan sponsors**. Although an employer and its health plan are separate legal entities, the HIPAA Rules recognize that employers often perform administrative functions on behalf of their health plans that involve PHI. When an employer receives PHI from its group health plan for plan administrative functions, the employer must agree to comply with certain requirements of the HIPAA Rules.

The impact of the HIPAA Rules on employers mainly depends on whether the health plan is insured or self-funded and, if the health plan is insured, whether the employer has access to PHI for plan administration purposes.

Covered Entities

Health Plans

In general, **any individual or group plan that provides or pays the cost of health care** is a covered entity subject to the HIPAA Rules. Health insurance issuers are also considered health plans subject to the HIPAA Rules.

There is a **special exemption for certain small, self-funded health plans**. Under this exemption, a self-funded health plan with **fewer than 50 eligible employees** that is administered by the employer that sponsors the plan is exempt from the HIPAA Rules. This exemption may apply to group medical plans, health reimbursement arrangements (HRAs) or health flexible spending accounts (FSAs) that satisfy the requirements for the exemption.

Basic Concepts

The following chart provides examples of common employee benefits provided by employers and indicates whether the benefits are health plans that are generally subject to the HIPAA Rules. If an employee benefit is not subject to the HIPAA Rules (for example, a disability insurance program), this means that information received in connection with the benefit is not PHI and is not subject to the HIPAA Rules' requirements.

Type of Employee Benefit	Subject to HIPAA Rules?
Group medical plans (fully insured or self-funded)	Yes
Dental and vision plans	Yes
Prescription drug plans	Yes
FSAs	Yes
Dependent care FSA	No
Adoption assistance FSA	No
HRAs	Yes
Health savings accounts (HSAs)	No, but the high deductible health plans (HDHPs) offered with HSAs are subject to the HIPAA Rules
Disease-specific policies, such as cancer policies	Yes, if they provide coverage for medical care
Employee assistance programs (EAPs)	Depends on the EAP's benefits—EAPs that provide medical care (for example, counseling services) are subject to the HIPAA Rules
Wellness plans	Depends on wellness plan's benefits—wellness plans that provide medical care (for example, biometric testing) are likely subject to the HIPAA Rules
Life insurance	No
Disability insurance	No
Section 125 premium-only plans	No
Workers' compensation insurance	No
Retirement plans	No

Basic Concepts

Health Care Clearinghouse

A health care clearinghouse is a public or private entity that processes another entity's health care transactions from a standard format to a nonstandard format (or vice versa). In many cases, health care clearinghouses will receive individually identifiable health information when they provide services to a health plan or health care provider as a business associate. Health care clearinghouses may include, for example, repricing companies, value-added networks, billing services or community health management information systems.

Health Care Providers

Every health care provider, regardless of size, that electronically transmits any health information in connection with a HIPAA-covered transaction is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests and other transactions for which HHS has established standards under HIPAA. Covered health care providers may include, for example, chiropractors, medical clinics, dentists, doctors, nursing homes, pharmacies and hospitals.

Business Associates

A business associate is a person or organization (other than an employee of a covered entity) that performs certain functions on behalf of, or provides certain services to, a covered entity that involves access to PHI. In general, a business associate means a third party (including a subcontractor) that:

- Creates, receives, maintains or transmits PHI on behalf of the covered entity for a HIPAA-regulated activity or function, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing; or
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services for the covered entity where the provision of the service involves the disclosure of PHI from the covered entity (or from another business associate of the covered entity) to the service provider.

Examples of Business Associates:

- Third-party administrators (TPAs)
- Pharmacy benefit managers (PBMs)
- Attorneys or auditors who use PHI in performing their services
- Health plan consultants or brokers

If a covered entity uses a business associate, there must be a written agreement between the parties, called a business associate agreement, that requires the business associate to comply with certain requirements under the HIPAA Rules. A sample business associate agreement is provided in this toolkit.

Basic Concepts

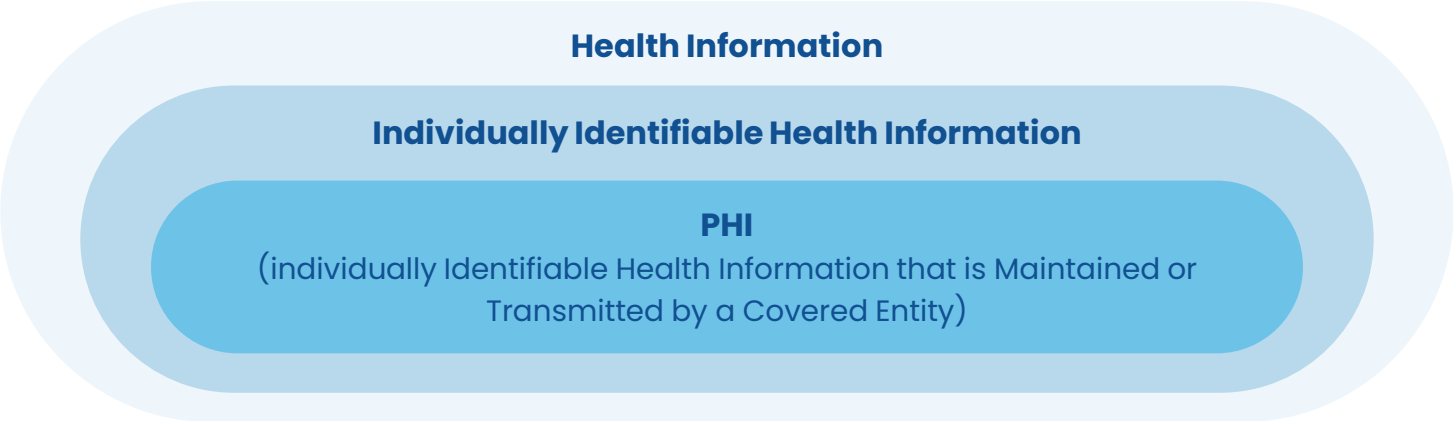
What Information is Protected?

PHI

The HIPAA Rules protect individually identifiable health information, called PHI, that is held or transmitted by a covered entity or its business associate. PHI includes information that relates to any of the following:

- The past, present, or future physical or mental health or condition;
- The provision of health care to an individual; or
- The past, present or future payment for the provision of health care to the individual.

The HIPAA Privacy Rule applies to PHI in any form or media—written, verbal, electronic or in any other medium. The Security Rule's requirements, however, only apply to ePHI.



PHI does not include employment records held by an employer. These records may include, for example, files or records related to occupational injury, disability insurance eligibility, leave requests, drug screenings, workplace medical surveillance and fitness-for-duty tests. Other laws, such as the federal Americans with Disabilities Act or state privacy laws, may impose confidentiality or privacy requirements on the information.

De-identified Health Information

De-identified health information is not governed by the HIPAA Rules because it is no longer individually identifiable. Covered entities may freely use and disclose de-identified information without taking into account the HIPAA Rules. There are two different methods that may be used to de-identify health information.

Statistical Method

Under the statistical method, a person with appropriate knowledge and experience applying generally applicable statistical and scientific principles and methods for rendering information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify the subject of the information. The covered entity must document the analysis and results that justify the determination.

Basic Concepts

Safe Harbor Method

Under the safe harbor method, information is presumed to be de-identified if a covered entity:

- Has no actual knowledge that the information could be used to identify the subject of the information (alone or in combination with other information); and
- Removes 18 specific identifiers from the information. **The 18 identifiers that must be removed are:**

1. Names
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and their equivalent geocodes, except for the initial three digits of a ZIP code if, according to the current publicly available data from the Bureau of Census, (1) the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people, and (2) the initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web URLs
15. IP addresses
16. Biometric identifiers, including finger and voice prints
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code

7. Privacy Requirements

Privacy Requirements

The HIPAA Privacy Rule requires covered entities to comply with national standards for the protection of PHI. The Privacy Rule includes the following three main protections for PHI:

Use and Disclosure Rules	The Privacy Rule limits when an individual's PHI may be used or disclosed by covered entities. As a general rule, a covered entity may not use or disclose an individual's PHI except: (1) as required or permitted by the Privacy Rule; or (2) subject to the individual's written authorization.
Individual Rights	Covered health care providers and health plans must provide individuals with detailed written information that explains their privacy rights and how their information will be used. Individuals also have the right to: › Access their own health records and request corrections; › Request restrictions on the uses and disclosures of their PHI, including that communications containing PHI be sent to an alternate location; and › Obtain documentation of certain disclosures of their PHI.
Administrative Safeguards	Covered entities must develop written privacy procedures and implement appropriate safeguards. For example, covered entities must designate a privacy officer, train employees on privacy requirements and establish a system for receiving complaints. Covered entities must also refrain from intimidating or retaliatory acts, and they cannot require a waiver of HIPAA privacy rights.

Special Exception for Fully Insured Health Plans

Employers that sponsor fully insured health plans and are hands-off PHI have minimal compliance obligations under the HIPAA Privacy Rules.

Use and Disclosure Rules

The Privacy Rule restricts when covered entities may use or disclose an individual's PHI. As a general rule, covered entities may only use or disclose an individual's PHI when:

- ☑ The disclosure is required or permitted by the Privacy Rule; or
- ☑ The individual authorizes the disclosure in writing.

Employes that sponsor group health plans are also subject to these use and disclosure rules if they have access to PHI.

Privacy Requirements

Required Disclosures

A covered entity must disclose PHI in only two situations:

- To individuals (or their personal representatives) when they request access to their PHI in a designated record set or when they request an accounting of disclosures of their PHI; and
- To HHS when it is investigating the covered entity's compliance with the HIPAA Rules.

Permitted Disclosures

A covered entity is permitted, but not required, to use and disclose PHI, without an individual's authorization, in certain situations, including the following:

- **To the individual** – A covered entity may disclose PHI to the individual who is the subject of the information.
- **Public policy purposes** – A covered entity may use or disclose PHI for specific public policy purposes, such as uses and disclosures that are required by law; for public health activities; about victims of abuse, neglect or domestic violence; for health care oversight activities; for judicial or administrative proceedings; for law enforcement purposes; necessary to avert a serious threat to health or safety; and for work-related injuries or illnesses.
- **Treatment, payment and health care operations** – A covered entity may use and disclose PHI or SUD for:
  - Its own treatment, payment and health care operations activities;
  - The treatment activities of any health care provider;
  - The payment activities of another covered entity or any health care provider; or
  - The health care operations of another covered entity if both covered entities has (or had) a relationship with the individual, the PHI pertains to the relationship and the disclosure involves quality or competency assessment activities or fraud and abuse detection and compliance activities.

Authorized Disclosures

A covered entity **must obtain the individual's written authorization for any use or disclosure of PHI or SUD that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule or Part 2**. In general, a health plan may not condition payment, enrollment or benefits eligibility on an individual granting an authorization, except in limited circumstances.

An authorization must be written in specific terms. It may allow use and disclosure of PHI or SUD records by the covered entity seeking the authorization or by a third party. The following information must be contained—in plain language—in HIPAA authorizations or Part 2 consents:

- A description of the information to be used or disclosed;
- The name or other specific identification of the person who is authorized to release the PHI;
- The name or other specific identification of the person who is authorized to receive the PHI;

Privacy Requirements

- A description of the purpose of the requested use or disclosure (for example, at the request of the individual);
- An expiration date or event;
- A statement that the individual has a right to revoke an authorization in writing and an explanation of the procedures for revocation;
- An explanation of the covered entity's ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the receipt of an authorization;
- A statement that informs the individual that the information used or disclosed pursuant to the authorization is subject to re-disclosure by the recipient and may no longer be protected by the HIPAA Privacy Rule or Part 2 Confidentiality rule; and
- The individual's signature and date of signature.

Compliance Tip for Employers

Some common employer functions that involve employees' medical information may require HIPAA authorizations, such as obtaining drug testing results and fitness-for-duty information from health care providers. Such information already in an employer's employment records is not subject to the HIPAA Privacy Rule, but obtaining the information in the first place from covered entities is subject to HIPAA and may require HIPAA authorizations. A HIPAA authorization is also required in order for an employer to help an employee with a claim dispute involving the health insurance issuer. Medical information that is directly provided by the employee to the employer is generally not subject to the HIPAA Rules. However, a valid HIPAA authorization is needed to obtain employees' medical or claim information directly from covered entities (such as health care providers or health insurance issuers).

Other Disclosures

Disclosures to Plan Sponsors

A group health plan (and the health insurance issuer for a fully insured plan) may disclose the following PHI to the employer sponsoring the plan, without first obtaining HIPAA authorizations from individuals:

- ☑ Plan enrollment or disenrollment information;
- ☑ If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend or terminate the group health plan; and
- ☑ PHI of the group health plan's enrollees for the plan sponsor to perform plan administration functions.

Reminder

An employer that is hands-on PHI (that is, it has access to PHI from the issuer for plan administration functions) takes on significant compliance responsibilities under the HIPAA Rules with respect to that PHI.

Privacy Requirements

If a plan sponsor has access to PHI other than summary health information and enrollment and disenrollment information, the plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the PHI. These restrictions must include the representation that the plan sponsor will not use or disclose the PHI for any employment-related action or decision or in connection with any other benefit plan.

A sample plan amendment and a sample certification are provided in this toolkit.

Disclosures to Business Associates

The HIPAA Rules allow a covered entity to share PHI with a business associate if the covered entity receives satisfactory assurances from the business associate—through a business associate agreement—that it will appropriately handle and safeguard PHI. A business associate may use or disclose PHI only as permitted or required by its business associate agreement or as required by law. In general, a business associate is prohibited from using or disclosing PHI in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. The same applies to SUD records. (F*or more information on SUD requirements, see "Updates" section on page 30.)*

The business associate agreement must establish the permitted and required uses and disclosures of PHI by the business associate. The business associate agreement must also require the business associate to:

- Not use or further disclose the PHI or SUD records other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards to prevent improper use or disclosure of the PHI or SUD records;
- Report to the covered entity any known use or disclosure of PHI or SUD records not permitted by the contract or any breach of unsecured PHI or SUD records;
- Ensure that any subcontractors that create, receive, maintain or transmit PHI or SUD records on behalf of the business associate agree to the same restrictions that apply to the business associate;
- Make PHI and SUD records available, including for amendment, to individuals as required by the HIPAA Rules;
- Maintain an accounting of disclosures, made during the last six years, and make the accounting available upon request; and
- Make its internal practices, books and records relating to use and disclosure of PHI and SUD records available to HHS.

The business associate contract must also allow the covered entity to terminate the contract in the event of a material breach. At termination, the business associate must be required to destroy or return all PHI, if feasible, or extend the limitations on use and disclosure beyond termination of the contract.

A sample business associate agreement is provided in this toolkit.

Enforcement Example:
No Business Associate Agreement

In April 2017, HHS entered into a HIPAA settlement with a small health care provider following an investigation of a business associate. Neither the health care provider nor the business associate could produce a signed business associate agreement. Based on this HIPAA violation, the health care provider agreed to pay HHS **$31,000** to settle the investigation.

Privacy Requirements

Individual Rights

Notice of Privacy Practices

The HIPAA Privacy Rule requires covered entities to provide a Notice of Privacy Practices to each individual who is the subject of PHI. The Privacy Notice for a health plan must be written in plain language and must:

- Explain how the health plan may use and disclose an individual's PHI;
- Describe the individual's rights with respect to his or her PHI; and
- Summarize the health plan's legal duties with respect to the PHI.

There are a number of specific provisions that must be incorporated into the Privacy Notice, such as details regarding how individuals may exercise their rights with respect to PHI. A typical Privacy Notice is multiple pages long due to the numerous content requirements. HHS had developed model Privacy Notices. See details on the following page.

The Privacy Notice requirements for a health plan vary depending on whether the plan is self-insured or fully insured, and, if the plan is fully insured, whether the plan sponsor has access to PHI for plan administration purposes. A self-insured plan must always issue its own Privacy Notice, while a fully insured plan is only required to maintain its own Privacy Notice if the employer has access to PHI for plan administration functions.

Special Rules for Fully Insured Health Plans

The plan sponsor of a fully insured health plan has limited responsibilities with respect to the Privacy Notices. The extent of its limited responsibilities depends on whether the plan sponsor has access to PHI for plan administration functions.

- ☑ If the sponsor of a fully insured plan is hands-on PHI, it is required to maintain a Privacy Notice and to provide the notice upon request.
- ☑ If the sponsor of a fully insured plan is hands-off PHI, it is not required to maintain or provide a Privacy Notice.

Delivery Requirements

At least once every three years, self-insured health plans must provide the Privacy Notice, or notify participants that the notice is available with instructions for how to obtain a copy. In addition, self-insured health plans must provide the Privacy Notice in the following circumstances:

- To new enrollees at the time of enrollment;
- Within 60 days of a material change to the notice; and
- Any time upon a participant's request.

Privacy Requirements

If a health plan sends out a revised notice (for example, following a material change to the notice), it will reset the three-year notice requirement.

A health plan must provide the Privacy Notice to individuals covered by the plan. If the health plan provides the Privacy Notice to a covered employee, the plan is not required to provide a separate notice for dependents (for example, a spouse or child) covered through the employee.

The Privacy Notice must actually be delivered to participants. Merely posting the Privacy Notice on a website or on a bulletin board in the workplace is not sufficient. The Privacy Notice may be provided electronically via email to participants who have agreed to receive an electronic notice. The health plan must provide a participant with a paper copy of the Privacy Notice if it discovers that the electronic delivery has failed.

In general, the Privacy Notice may be provided with other plan documents. It does not need to be provided as a stand-alone document. For example, a health plan could provide the Privacy Notice with the plan's enrollment materials or with the summary plan description (SPD). However, the Privacy Notice may not be combined in the same document as a HIPAA authorization.

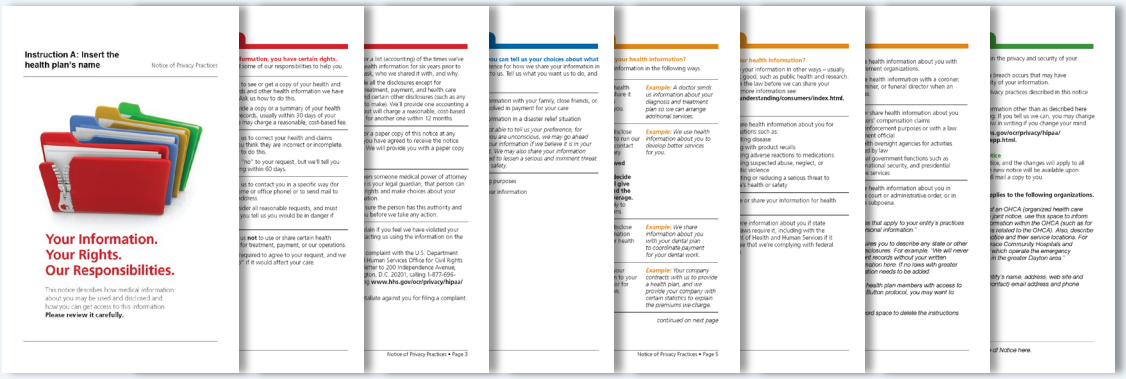
If a health plan maintains a website about the plan's services or benefits, the Privacy Notice must be posted on the website and must be electronically available through the website.

Model Privacy Notices

HHS has developed model Privacy Notices that health plans may customize and use. There are three designs for the model Privacy Notice for health plans—a booklet version, a full-page version and a layered version. Every design has the same language, although the layered notice includes an additional first page that summarizes key privacy rights, choices, uses and disclosures.

Each design is in a fillable Adobe PDF format and has some areas that can be customized for each health plan. More information on customizing the notice and best practices is available in the Health Plan Instructions and Questions and Instructions for using the Model Notices. For additional flexibility, HHS also maintains a text-only version of the model Privacy Notice.

HHS Model Privacy Notice
Booklet Version



Privacy Requirements

Other Individual Rights

The Privacy Rule requires covered entities to provide individuals with the following rights with respect to their PHI:

Individual Right	Description
Right to access PHI	Individuals have the right to inspect and obtain a copy of their PHI in a designated record set that is maintained by or for a covered entity, except that they do not have the right to access psychotherapy notes of mental health professionals. Additionally, they do not have the right to access PHI that is not in a designated record set. For example, a health plan's quality control records, or a hospital's provider performance evaluations, even if those include PHI about an individual.
Right to amend or correct PHI	Individuals have the right to request that covered entities amend or correct their PHI in a designated record set when that information is inaccurate or incomplete. Covered entities must comply with these requests, subject to certain limitations.
Right to obtain an accounting of disclosures	Individuals have a right to an accounting of certain disclosures of their PHI by a covered entity. Many common group health plan disclosures (such as disclosures for payment and health care operations) are exempted from this accounting requirement.
Right to request restrictions on uses and disclosures	Individuals have the right to request that a covered entity restrict its use or disclosure of PHI with respect to: (1) treatment, payment or health care operations; or (2) other people involved in the individual's care. In general, a covered entity is not required to agree to requests for restrictions.
Right to request alternative communications	A health plan must permit individuals to request to receive communications of PHI by alternative means or at alternative locations. A health plan must accommodate reasonable requests if the individual clearly indicates that the disclosure of all or part of the PHI could endanger the individual.

Special Rules for Fully Insured Health Plans

Fully insured health plans that are hands-off PHI are not subject to these individual rights requirements. Rather, individuals who are enrolled in these health plans would exercise their privacy rights through the health insurance issuer.

Administrative Requirements

In general, the HIPAA Privacy Rule requires a health plan to comply with numerous administrative requirements. These are listed on the following page.

Privacy Requirements

Administrative Requirements

In general, the HIPAA Privacy Rule requires a health plan to comply with the following administrative requirements:

- **Implement reasonably designed policies and procedures** that address the Privacy Rule's requirements and are designed to ensure compliance with those requirements, taking into account the health plan's size and types of activities that involve PHI;
- Designate a **privacy officer** responsible for the development and implementation of the health plan's privacy policies and procedures;
- Designate a **contact person** (who may also be the privacy official) responsible for receiving privacy complaints and providing information about privacy practices;
- **Train** all members of its workforce on its policies and procedures with respect to PHI, as necessary and appropriate for those individuals to carry out their job functions;
- Put in place appropriate **administrative, technical and physical safeguards** to protect the privacy of PHI;
- Provide a **complaint process** for individuals regarding the health plan's privacy policies and procedures and **document any privacy complaints** that it receives;
- Establish and apply **appropriate sanctions** against members of its workforce who fail to comply with the health plan's privacy policies and procedures and **document any sanctions** that are applied;
- **Mitigate, to the extent possible, the harmful effect** of any violation of its privacy policies or procedures;
- **Refrain from intimidating or taking retaliatory action** against any individual who exercises his or her individual privacy rights or files a privacy complaint;
- Do not require individuals to **waive their privacy rights** as a condition of enrollment in the plan, eligibility for benefits or payment;
- Provide a **Privacy Notice** to plan participants (special exception applies for fully insured health plans);
- Require all business associates to enter into **business associate agreements** with the health plan;
- Confirm that the **plan document has been amended**, as required by the Privacy Rule;
- Do not use PHI from the health plan in any **employment-related action or decision** or in connection with any **other benefit plan**; and
- Maintain the plan's privacy policies and documentation required by the Privacy Rule for **at least six years**.

Exception for Fully Insured Health Plans

Fully insured group health plans that are "hands off" PHI are not subject to most of the Privacy Rule's administrative requirements. These health plans are only required to comply with the ban on retaliatory acts and waiver of individual rights.

An employer that is hands-on PHI (that is, it has access to PHI from the issuer for plan administration functions) takes on significant compliance responsibilities under the HIPAA Rules with respect to that PHI.

Updates

Privacy Requirements

Update 1

2024 Rule Aligning Confidentiality of Substance Use Disorder (SUD) Records with HIPAA Privacy

In April 2024, HHS issued a final rule (42 CFR Part 2 Final Rule) modifying the Confidentiality of Substance Use Disorder (SUD) Patient Records Act to align with HIPAA and HITECH regulations. Like HIPAA, Part 2 protects patient privacy but relates to records of treatment for substance use disorder (SUD) when federally funded or assisted, whereas HIPAA applies to protected health information generally, regardless of whether federal funds are involved. SUD records are most similar to PHI mental health records under HIPAA, and they may also include separate SUD clinician notes, which cannot be used or disclosed without specific consent from the individual. This is analogous to HIPAA protections for psychotherapy notes. The Part 2 rule (for SUD records) does NOT specifically incorporate the HIPAA Risk Assessment requirement, but it does incorporate the HIPAA Breach Notification requirements.

Full compliance with the 2024 Final Rule is required by February 16, 2026, but covered entities are encouraged to update their Privacy Policies, Notices of Privacy Practices, and BAAs by the end of 2025. HHS plans to finalize changes to the HIPAA Privacy Notice to address uses and disclosures of PHI that is also subject to Part 2. In this Toolkit we have updated references to PHI to also include SUD records, where applicable. Additionally, the Sample NPP and BAA at the end of this Toolkit have been updated to include references to SUD as well as to PHI. However, the Part 2 rule on Confidentiality of SUD Records does not specifically incorporate the HIPAA Security risk assessment requirement.

The 2024 Final Rule is intended to ease the complexity of compliance for entities required to comply with both HIPAA and Part 2, facilitate information sharing and improved care coordination, continue patient privacy protections, and also expand patient rights regarding the uses and disclosures of the SUD records. The key changes in the 2024 Final Rule are:

- Except in an emergency or other special situations, a patient may provide a single consent (to providers, health plans, third-party payers and others) for all future uses or disclosures of SUD records for the purposes of treatment, payment, and/or health care operations pursuant to Part 2. Thus, the HIPAA Authorization form should be updated to reference SUD records as well as PHI.
- HIPAA-regulated entities are permitted to redisclose SUD records received under that single consent in accordance with the HIPAA Privacy Rule.
- Disclosure of patient records to public health authorities is permitted, if they have been unidentified in accordance with HIPAA standards.
- Patients will be able to obtain an accounting of disclosures of their SUD records and request restrictions on certain disclosures.
- The HIPAA Breach Notification Rule requirements will also apply to Part 2 SUD records.

Updates

Privacy Requirements

Update 1 (continued)

- The Part 2 Patient Notice requirements now align with the HIPAA Notice of Privacy Practices (NPP) requirements, so the NPP can be amended to also reference SUD records as well as PHI.
- HHS will be able to impose civil monetary penalties for violations of Part 2, in line with HIPAA and the HITECH Act.
- SUD records and testimony cannot be used in civil, criminal, administrative, and legislative proceedings against patients, unless the patient consents or there is a valid court order.
- Part 2 SUD records no longer need to be segregated from a patient's other records.
- Part 2 programs must establish a complaints process about Part 2 violations and must not require patients to waive the right to file a complaint as a condition of providing treatment, enrollment, payment, or eligibility for services.

Updates

Privacy Requirements

Update 2

Reproductive Health Care Privacy: 2024 HIPAA Privacy Rule Changes to Strengthen Privacy Rights, and Texas District Court Ruling Vacating Privacy Rule

This section: 1) explains the HIPAA Privacy Rules changes that were required by the 2024 HIPAA Privacy Rule to Support Reproductive Health Care, and 2) the Texas District Court ruling (Purl v HHS) that vacated this rule in June 2025. It is expected that the US Supreme Court will eventually rule on whether or to what extent these 2024 Privacy Rule provisions apply. The details below are informative only, and the privacy provisions listed for reproductive health care information do not apply at this time, but some or all of them might apply in the future.

Background

In June 2022 the Supreme Court decision in Dobbs v. Jackson Women's Health Organization overturned Roe v Wade. This removed the federal right to an abortion, thus allowing each state to enact laws regulating the legality of abortion in that state. Many states implemented restrictions on abortions, and some states implemented near-total bans, which also applied to pregnancy terminations due to medical complications. One result of such restrictions was that some pregnant women traveled across state lines to have pregnancies terminated in states that had not adopted such restrictive laws.

OCR originally issued guidance confirming how the HIPAA Privacy Rule applies to disclosures of reproductive health information. Section §164.512(e) of the HIPAA Privacy Rule permits but does not require disclosures of PHI in extraterritorial civil, criminal, or administrative investigations or proceedings. In April 2023, OCR published an NPRM to strengthen reproductive health information privacy, and it issued a final rule in April 2024. The final rule was effective on June 25, 2024, with enforcement starting on December 23, 2024.

Requirements (Now Vacated) under the 2024 HIPAA Privacy Rule

The 2024 HIPAA Privacy Rule made the following changes, which are now vacated:

1. added a new definition for reproductive health information;
2. prohibited disclosures of an individual's PHI for the purpose of conducting a criminal, civil, or administrative investigation into or imposing criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care that is lawful under the circumstances in which it is provided;
3. prohibited the identification of any person for the purpose of conducting such an investigation or imposing such liability;
4. required HIPAA-regulated entities to obtain a signed attestation from the requester of the PHI that it will not be used for a prohibited purpose.

Updates

Privacy Requirements

Update 2 (continued)

Several lawsuits were filed over the 2024 final rule. Some of these requested that the final rule be vacated in its entirety, and some sought to prevent HHS from enforcing compliance in certain states. In June 2025, one of those challenges was successful (Purl v HHS). A Texas District Court judge vacated the final rule, and his decision applies nationally, not just in Texas. Therefore, the requirements listed above no longer apply.

For additional information, see HHS Fact Sheet on HIPAA Privacy Rule to Support Reproductive Health Care Privacy and provisions vacated by Purl v HHS.

8. Security Requirements

Security Requirements

The HIPAA Security Rule establishes national standards for securing individuals' ePHI. These standards require covered entities to analyze the risks and vulnerabilities of the confidentiality, integrity and availability of their ePHI. The risk assessment process helps covered entities implement reasonable and appropriate administrative, physical and technical safeguards to protect their ePHI.

Impact on Health Plans

In general, sponsors of self-insured and fully insured group health plans should conduct risk assessments and implement appropriate safeguards to protect their ePHI. Unlike the Privacy Rule, the Security Rule does not contain a special exception for fully insured plans that do not have access to PHI for plan administration purposes. However, fully insured health plans that do not handle ePHI will have fewer obligations under the Security Rule due to their hands-off approach to PHI.

Electronic PHI

The Security Rule only applies to ePHI—it does not apply to PHI that is in paper or written form, and it does not apply to electronic personal information that is not PHI.

Electronic PHI is PHI that is transmitted by, or maintained in, electronic media. This includes PHI in computers, devices that are used with computers (such as disks and drives), and smartphones. It also includes PHI that is sent via email or in any manner using the internet.

The Security Rule's requirements apply even when the ePHI is located on a device that is not owned by the covered entity (for example, an employee's smartphone) or is accessed outside of the covered entity's physical location (for example, on a home computer or on a laptop outside of work). HHS has cautioned that covered entities should be extremely careful about allowing off-site use of, or access to, ePHI due to security risks involved.

Security Requirements

The HIPAA Security Rule requires covered entities to maintain **reasonable and appropriate administrative, technical and physical safeguards** for protecting ePHI. Each covered entity must analyze the risks to ePHI in its environment and create solutions appropriate for its own situation. What is reasonable and appropriate depends on the nature of the entity's business, as well as its size, complexity and resources. Specifically, a covered entity must:

- Ensure the confidentiality, integrity and availability of all ePHI it creates, receives, maintains or transmits;
- Identify and protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- Protect against reasonably anticipated use or disclosure of ePHI that is not permitted or required under the HIPAA Privacy Rule; and
- Ensure its workforce complies with the procedures implemented to comply with the HIPAA Security Rule.

Security Requirements

Risk Assessment

According to HHS, performing a risk assessment is a **crucial first step** to comply with the Security Rule. A risk assessment helps an organization establish appropriate administrative, physical and technical safeguards for its ePHI. It directs what reasonable steps a covered entity or business associate should take to protect the ePHI it creates, transmits, receives or maintains.

There are numerous methods of performing a risk assessment (also called a risk analysis), and there is no single method or best practice that guarantees compliance with the Security Rule. HHS has a HIPAA Security Risk Assessment (SRA) Tool that employers can use when the website is active. Most risk analysis processes have common steps. The following are examples of common risk analysis steps:

Elements for Risk Assessment	
Identify the scope of analysis	The scope should include the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that a covered entity creates, receives, maintains or transmits.
Gather data	Gather relevant data on ePHI and identify where ePHI is stored, received, maintained or transmitted.
Identify potential threats and vulnerabilities	Identify and document potential threats and vulnerabilities to the confidentiality, availability and integrity of ePHI.
Assess current security measures	Analyze current security measures implemented to minimize or eliminate risks to ePHI.
Determine the likelihood of threat occurrence	Use information gathered from the previous steps to assess: (1) the likelihood that a threat will trigger or exploit a specific vulnerability; and (2) the resulting impact on the health plan.
Determine the potential impact of threat occurrence	Measure the impact of a threat occurring, such as the unauthorized access to or disclosure of ePHI, permanent loss of corruption of ePHI, or temporary loss or unavailability of ePHI.
Determine risk level	Determine the level of risk to ePHI (based on the likelihood of threat occurrence and the potential impact of threat occurrence).
Identify security measures and finalize documentation	Identify security measures that can be used to reduce risk to a reasonable and appropriate level and document the risk analysis.

Security Requirements

Also, to better understand the risk analysis and management processes, covered entities should be familiar with the following terms:

- **Vulnerability** means a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of security policy.
- **Threat** means the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. Threats may be grouped into the following categories:
  - **Natural threats**, such as floods, earthquakes, tornadoes and landslides;
  - **Human threats**, including intentional actions (for example, network and computer-based attacks, malicious software upload and unauthorized access) and unintentional actions (for example, inadvertent data entry or deletion); and
  - **Environmental threats**, such as power failures, pollution, chemicals and liquid leakage.
- **Risk** means the net impact considering the probability that a particular threat will exercise a particular vulnerability and the resulting impact if this should occur.

Security Standards

The security standards are divided into the following three categories:

Administrative Safeguards	Physical Safeguards	Technical Safeguards

Each type of safeguard has certain standards and implementation specifications associated with it.

- **Administrative safeguards** – These are the administrative actions, policies and procedures to prevent, detect, contain and correct security violations.
- **Physical safeguards** – These are the physical measures, policies and procedures to protect electronic systems and related building and equipment from natural and environmental hazards and unauthorized intrusion.
- **Technical safeguards** – These safeguards are the technology and procedures that protect ePHI and control access to it.

Security Requirements

The standards and implementation specifications for each type of safeguard are listed in the Security Standards Matrix below. The Security Rule allows covered entities some flexibility in determining how to implement the standards and implementation specifications, including choosing which technology it will employ in order to achieve the required security standards. In deciding how to implement security measures, a covered entity is permitted to take into account:

- Its size, complexity and capabilities;
- Its technical infrastructure, hardware and software security capabilities;
- The costs of security measures; and
- The probability and criticality of potential risks to health information.

Enforcement Example

In December 2024, the Office for Civil Rights (OCR) announced a HIPAA settlement with a covered entity (medical provider) regarding a former contractor's impermissible access to the provider's electronic medical record system to retrieve PHI of 34,310 individuals for use in filing fraudulent Medicare claims. HHS found that the medical provider failed to: conduct an accurate and thorough risk analysis, regularly review records of activity in its information systems, and implement procedures to terminate former workforce members' access to ePHI. Pursuant to the settlement, the medical provider paid **$1.19 million** and implemented a corrective action plan.

However, HHS has stated that cost alone is not a justification for failing to implement a procedure.

In an effort to provide covered entities with additional flexibility, the Security Rule categorizes implementation specifications as "required" or "addressable." The "required" implementation specifications must be implemented.

The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.

Policies and Procedures

Covered entities are required to implement **reasonable and appropriate policies and procedures** to comply with the Security Rule's standards and implementation specifications. These policies and procedures must be documented in written form, which may be electronic. In addition, a covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI. Documentation supporting its security policies must be retained **for at least six years** from the date of its creation or the date when it was last in effect, whichever is later.

Security Requirements

Security Standards Matrix		
Standards	Implementation Specifications (R) = Required and (A) = Addressable	
Administrative Safeguards		
Security Management Process	Risk Analysis	(R)
	Risk Management	(R)
	Sanction Policy	(R)
	Information System Activity Review	(R)
Assigned Security Responsibility		(R)
Workforce Security	Authorization and/or Supervision	(A)
	Workforce Clearance Procedure	(A)
	Termination Procedures	(A)
Information Access Management	Isolating Health Care Clearinghouse Functions	(R)
	Access Authorization	(A)
	Access Establishment and Modification	(A)
Security Awareness and Training	Security Reminders	(A)
	Protection from Malicious Software	(A)
	Login Monitoring	(A)
	Password Management	(A)
Security Incident Procedures	Response and Reporting	(R)
Contingency Plan	Data Backup Plan	(R)
	Disaster Recovery Plan	(R)
	Emergency Mode Operation Plan	(R)
	Testing and Revision Procedures	(A)
	Applications and Data Criticality Analysis	(A)
Evaluation		(R)
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	(R)

Security Requirements

Security Standards Matrix		
Standards	Implementation Specifications (R) = Required and (A) = Addressable	
Physical Safeguards		
Facility Access Controls	Contingency Operations	(A)
	Facility Security Plan	(A)
	Access Control and Validation Procedures	(A)
	Maintenance Records	(A)
Workstation Use		(R)
Workstation Security		(R)
Device and Media Controls	Disposal	(R)
	Media Reuse	(R)
	Accountability	(A)
	Data Backup and Storage	(A)
Technical Safeguards		
Access Control	Unique User Identification	(R)
	Emergency Access Procedure	(R)
	Automatic Logoff	(A)
	Encryption and Destruction	(A)
Audit Controls		(R)
Integrity	Mechanism to Authenticate Electronic PHI	(A)
Person or Entity Authentication		(R)
Transmission Security	Integrity Controls	(A)
	Encryption	(A)

9. Breach Notification Requirements

Breach Notification Requirements

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) amended HIPAA to add breach notification requirements for unsecured PHI. The HITECH Act, and its underlying HIPAA breach notification rules, require covered entities to notify affected individuals following the discovery of a breach of unsecured PHI. Notification must also be provided to HHS and, in some cases, to the media.

Breach of Unsecured PHI

The HIPAA Rules define a "breach" as the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the information. There are three exceptions to this definition.

1. Disclosures where the recipient of the information would not reasonably have been able to retain the information;
2. Certain unintentional acquisition, access, or use of information by employees or others acting under the authority of a covered entity or business associate; and
3. Certain inadvertent disclosures among people similarly authorized to access PHI at a business associate or covered entity.

Unsecured PHI

The breach notification requirements only apply to **unsecured PHI or SUD records**. PHI or SUD records are unsecured if they are not rendered unusable, unreadable or indecipherable to unauthorized individuals by a methodology specified by HHS. HHS has specified **encryption and destruction** as the methodologies for securing PHI.

An impermissible use or disclosure of PHI or SUD records is **presumed to be a breach** unless the covered entity or business associate demonstrates through a **risk assessment** that there is a **low probability** that the PHI or SUD records have been compromised (or one of the three exceptions to the definition of breach applies). The risk assessment must, at a minimum, take into account these factors:

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

If an evaluation of the factors fails to demonstrate that there is a low probability that PHI or SUD records have been compromised, breach notification is required.

Breach Notification Requirements

Breach Notification

Notice to Individuals

If a covered entity discovers that it has experienced a breach of unsecured PHI or SUD, it must notify each individual whose unsecured PHI or SUD has been (or is reasonably believed by the covered entity to have been) accessed, acquired, used or disclosed as a result of the breach. The notice must be provided without unreasonable delay and in no case later than **60 calendar days** after the breach is discovered.

Enforcement Example

In January 2017, OCR announced a HIPAA settlement with a health care provider based on the untimely reporting of a breach of unsecured PHI. After receiving a breach notification report from the health care provider, OCR investigated and found that the provider failed to notify affected patients, media outlets and OCR within 60 days of the discovery. Pursuant to the settlement, the provider paid **$475,000** to OCR and implemented a corrective action plan.

The notice must be written in plain language and must contain the following information:

- A brief description of what happened, including the dates the breach occurred and was discovered, if known;
- A description of the types of unsecured PHI or SUD records that were involved, such as names, Social Security numbers or other types of information;
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, mitigate harm to individuals and protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, an email address, website or postal address.

In general, notice must be provided in writing, by first-class mail to the individual's last known address. Notice can be sent electronically if the individual has agreed to electronic notice. In a case that requires urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide notice by telephone or other means.

Notice to HHS

Covered entities must notify HHS of a breach of unsecured PHI or SUD records. However, the notification required depends on the size of the group affected.

Breaches involving fewer than 500 individuals	The covered entity must maintain a log or other documentation of the breaches. Within 60 days after the end of each calendar year, the covered entity must notify HHS of the breaches that occurred during the year.
Breaches involving 500 or more individuals	The notice must be provided at the same time as the notice to the individuals and in the manner specified on the HHS website.

Breach Notification Requirements

Notice to Media

If the breach of unsecured PHI or SUD records involves **more than 500 residents of a state or jurisdiction**, the covered entity must notify prominent media outlets that serve that area. The notice must include the same information as a notice to an individual. It must be provided without unreasonable delay and no later than **60 calendar days** after the breach is discovered.

Business Associate Role

If a business associate discovers a breach of unsecured PHI or SUD records, it must notify the covered entity of the breach. Notification must be provided without unreasonable delay and no later than 60 calendar days after the breach is discovered. The notice must include, to the extent possible, the identification of each individual whose unsecured PHI or SUD records have been affected. The business associate must also give the covered entity any information necessary to notify the individual of the breach.

Administrative Requirements

Covered entities must incorporate compliance with the breach notification requirements into their HIPAA privacy policies and procedures. Covered entities and business associates have the burden of demonstrating that all notifications were provided or that an impermissible use or disclosure did not constitute a breach, and must maintain documentation to meet the burden of proof.

10. Enforcement

Enforcement

HHS' OCR (Office for Civil Rights) is responsible for enforcing the HIPAA Privacy and Security Rules. OCR investigates complaints that individuals file, conducts compliance reviews, and performs education and outreach to encourage compliance. OCR also works with the Department of Justice regarding possible criminal violations of HIPAA.

Enforcement Data

Since the compliance date of the Privacy Rule in April 2003 through October 2024, OCR has received over 374,321 HIPAA complaints and has initiated over 1,193 compliance reviews. The OCR has resolved 99% of these cases (370,578). In many cases involving HIPAA violations, OCR worked with the entities involved to apply corrective measures instead of imposing penalties. However, as of October 31, 2024, OCR has settled or imposed a civil money penalty in 152 of these cases, resulting in a total dollar amount of **$144,878,972**. More information regarding HIPAA enforcement is available through OCR's website.

Most of OCR's investigations are **trigged by individuals' complaints** regarding HIPAA violations or a **covered entity's breach notification reports**. OCR has investigated many different types of entities, including national pharmacy chains, major medical centers, group health plans, hospital chains and small provider offices. Since Feb. 2024, most HHS investigations and settlements have involved Security violations.

OCR's most investigated compliance issues (2024, in order of frequency):

- Security Rule Violations, particularly Risk Analysis and Ransomware Cybersecurity investigations;
- Impermissible Uses and Disclosures of PHI;
- Lack of safeguards on PHI;
- Lack of patient access to PHI;
- Lack of administrative safeguards to protect ePHI; and
- Breach notification to individual.

HIPAA Audits

OCR has audited covered entities and business associates to ensure their compliance with the HIPAA Rules. According to OCR, these HIPAA audits are primarily a compliance improvement activity. However, if an audit reveals a serious compliance issue, OCR may initiate a review to investigate.

- In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by covered entities to comply with HIPAA's requirements.
- In March 2016, OCR launched the second phase of its HIPAA audit program. This second phase of HIPAA audits included both desk audits and onsite audits of covered entities and their business associates. OCR conducted audits of 166 covered entities and 41 business associates.
- On December 17, 2020, OCR released its 2016-2017 HIPAA Audits Industry Report that reviewed selected health care entities and business associates for compliance with certain provisions of the HIPAA Privacy, Security, and Breach Notification Rules.

Enforcement

The OCR website says: "The 2024-2025 HIPAA Audits will review 50 covered entities' and business associates' compliance with selected provisions of the HIPAA Security Rule most relevant to hacking and ransomware attacks. These Audits will give OCR an opportunity to examine mechanisms for compliance, identify promising practices for protecting the privacy and security of health information, and discover risks and vulnerabilities that may not have been revealed by OCR's enforcement activities."

Civil Penalties

OCR has the authority to assess civil penalties for violations of the HIPAA Privacy or Security Rules. The amount of the penalty depends on the type of violation involved. These penalties may not apply if the violation is corrected within 30 days of the date the person knew, or should have known, of the violation. HHS is also required to assess penalties for violations involving willful neglect and to formally investigate complaints of such violations. The 2024 Part 2 final rule on Confidentiality of SUD Records incorporates the HIPAA penalties, so civil and criminal penalties for HIPAA violations now also apply to violations of the Part 2 regulations. This includes the four culpability tiers for civil monetary penalties.

These civil penalty amounts are subject to annual inflation-related increases. The penalty amounts that apply to civil penalties that are assessed on or after Aug. 8, 2024, and relate to violations occurring after Nov. 2, 2015, are as follows:

Category of Violation	Minimum Penalty Per Violation	Maximum Penalty Per Violation
Did not know	$141	
Reasonable cause	$1,424	$71,162
Willful neglect, corrected	$14,232	
Willful neglect, not corrected	$71,162	$2,134,831

Criminal Penalties

Criminal penalties may be assessed for violations of the HIPAA Privacy and Security Rules. These penalties are $50,000 and one year in prison for knowing violations, $100,000 and five years in prison for violations committed under false pretenses, and $250,000 and 10 years in prison for offenses committed for commercial or personal gain.

Amount of Penalties – Important Factors

The Enforcement Rule provides some guidance on the actions that constitute a single violation, but gives HHS the authority to determine the number of violations based on the nature of the covered entity's obligation to act or not act under the provision that is violated. Where a violation is continuing, a separate violation occurs each day that the covered entity is in violation of the requirements. Also, HHS must consider certain aggravating or mitigating factors when imposing civil penalties. These factors include the following:

Enforcement

- The nature and extent of the violation, including (but not limited to) the number of individuals affected and the time period during which the violation occurred;
- The nature and extent of the harm resulting from the violation, including whether the violation resulted in physical harm, financial harm, harm to an individual's reputation or hindered an individual's ability to obtain health care;
- The history of prior compliance with HIPAA's administrative simplification requirements, including whether the current violation is the same or similar to previous instances of noncompliance, whether and to what extent the covered entity has attempt to correct prior instances of noncompliance, how the covered entity has responded to technical compliance assistance from OCR and how the covered entity has responded to prior complaints;
- The financial condition and size of the covered entity; and
- Any other matters as justice may require.

Civil money penalties may not be imposed if HHS determines that the violation was not due to willful neglect and it is corrected within a time frame specified by HHS (that is, within 30 days). Willful neglect is defined as a conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provisions. HHS has discretion to expand the 30-day time period depending on the nature and extent of the covered entity's compliance failure.

For violations due to reasonable cause and not to willful neglect that are not corrected in a timely manner, HHS may waive civil money penalties, in whole or in part, to the extent that payment of the penalty would be excessive relative to the violation. In addition, HHS must initiate civil money penalty actions within six years from the date the alleged violation occurred.

Resolution Agreements vs. Civil Penalties

Rather than imposing civil penalties, OCR almost always resolves HIPAA violations informally with covered entities (or business associates) through resolution agreements. These agreements typically include a monetary settlement amount that is a fraction of the potential civil monetary penalties and a corrective action plan that requires the covered entity (or business associate) to fix remaining compliance issues.

Highest Penalty Paid: In October 2018 Anthem, Inc. agreed to pay $16 million to HHS OCR and take substantial corrective action to settle potential violations of HIPAA Privacy and Security Rules after a series of cyberattacks led to the largest U.S. health data breach in history and exposed the electronic protected health information of almost 79 million people. Previously, the highest HIPAA penalty paid to OCR was $5.55 million, paid in 2016.

More Information

More information on OCR's enforcement process is available on its website.

11. Sample Documents

Sample Documents

Fully Insured Health Plans that are Hands-off PHI

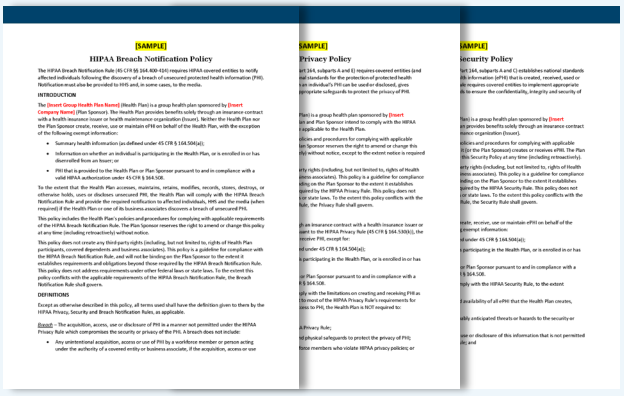
These sample HIPAA policies and related documents are based on hypothetical employers and health plan designs and are provided for educational and illustrative purposes only. They will not apply to every employer's situation, and they must be customized for a specific employer's circumstances. These sample policies are not exhaustive—depending on an employer's situation, additional policies may be required. Nothing in this toolkit should be considered as legal advice, including these sample documents. Employers should work with knowledgeable benefits counsel to obtain legal advice on HIPAA compliance.

Important - Customization Required

Nothing in this toolkit should be considered as legal advice, including these sample documents. These sample documents are provided for educational and illustrative purposes only.

The following are **sample HIPAA policies for fully insured health plans that are "hands-off" PHI**. These samples cannot be used "as is"—they must be customized for specific plan and employer information. Also, if the sample policies do not accurately reflect an employer's implementation of the HIPAA Rules, they should be customized for the employer's specific approach. We encourage all customization to take place in coordination with knowledgeable benefits counsel. Note that the Sample Policies require a "Hands-off" plan sponsor to designate a HIPAA Security Official but not a HIPAA Privacy Official.

Self-insured health plans and fully insured health plans that have access to PHI should not use these sample HIPAA policies. These health plans have additional responsibilities under the HIPAA Rules.


[SAMPLE]

HIPAA Breach Notification Policy

The HIPAA Breach Notification Rule (45 CFR §§ 164.400-414) requires HIPAA-covered entities to notify affected individuals following the discovery of a breach of unsecured protected health information (PHI). Notification must also be provided to HHS and, in some cases, to the media.

INTRODUCTION

The [Insert Group Health Plan Name] (Health Plan) is a group health plan sponsored by [Insert Company Name] (Plan Sponsor). The Health Plan provides benefits solely through an insurance contract with a health insurance issuer or health maintenance organization (Issuer). Neither the Health Plan nor the Plan Sponsor create, receive, use or maintain ePHI on behalf of the Health Plan, with the exception of the following exempt information:

- Summary health information (as defined under 45 CFR § 164.504(a));
- Information on whether an individual is participating in the Health Plan, or is enrolled in or has disenrolled from an Issuer; or
- PHI that is provided to the Health Plan or Plan Sponsor pursuant to and in compliance with a valid HIPAA authorization under 45 CFR § 164.508.

To the extent that the Health Plan accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI, the Health Plan will comply with the HIPAA Breach Notification Rule and provide the required notification to affected individuals, HHS and the media (when required) if the Health Plan or one of its business associates discovers a breach of unsecured PHI.

This policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Breach Notification Rule. The Plan Sponsor reserves the right to amend or change this policy at any time (including retroactively) without notice.

This policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Breach Notification Rule, and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Breach Notification Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Breach Notification Rule, the Breach Notification Rule shall govern.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy, Security and Breach Notification Rules, as applicable.

Breach – The acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. A breach does not include:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if the acquisition, access or use

[Download Now >](#)

Editable Templates

Sample HIPAA Privacy Policy

Sample HIPAA Security Policy

Sample Breach Notification Policy

Sample Documents

Fully Insured Health Plans with Access to PHI & Self-Insured Health Plans

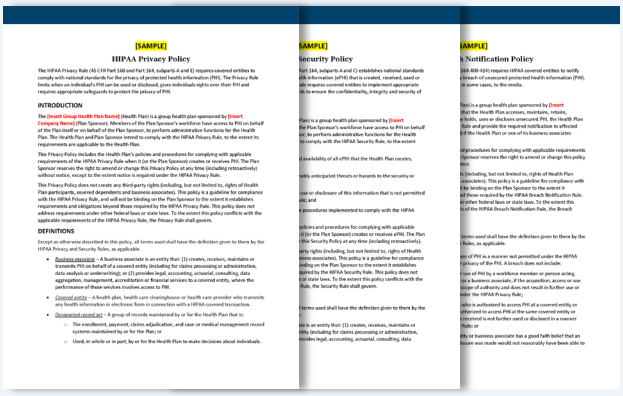
Important - Customization Required

Nothing in this toolkit should be considered as legal advice, including these sample documents. These sample documents are provided for educational and illustrative purposes only.

The following are **sample HIPAA policies** for fully insured health plans that are **"hands-on" PHI** and self-insured health plans. These samples cannot be used "as is"—they must be customized for specific plan and employer information. Also, if the sample policies do not accurately reflect an employer's implementation of the HIPAA Rules, they should be customized for the employer's specific approach.

Because these policies assume that the health plan sponsor has access to PHI for plan administration functions, they incorporate a wide range of HIPAA compliance requirements. If a separate entity (for example, a third-party administrator or issuer) performs almost all of a health plan's administrative functions and the employer's access to PHI (and ePHI) is very limited, these policies can be revised to reflect that limited access. We encourage all customization to take place in coordination with knowledgeable benefits counsel.

Fully insured health plans that are **"hands-off" PHI** should not use these sample HIPAA policies. These health plans have fewer responsibilities under the HIPAA Rules.


[SAMPLE]

HIPAA Privacy Policy

The HIPAA Privacy Rule (45 CFR Part 160 and Part 164, subparts A and E) requires covered entities to comply with national standards for the privacy of protected health information (PHI). The Privacy Rule limits when an individual's PHI can be used or disclosed, gives individuals rights over their PHI and requires appropriate safeguards to protect the privacy of PHI.

INTRODUCTION

The [Insert Group Health Plan Name] (Health Plan) is a group health plan sponsored by [Insert Company Name] (Plan Sponsor). Members of the Plan Sponsor's workforce have access to PHI on behalf of the Plan itself or on behalf of the Plan Sponsor, to perform administrative functions for the Health Plan. The Health Plan and Plan Sponsor intend to comply with the HIPAA Privacy Rule, to the extent its requirements are applicable to the Health Plan.

This Privacy Policy includes the Health Plan's policies and procedures for complying with applicable requirements of the HIPAA Privacy Rule when it (or the Plan Sponsor) creates or receives PHI. The Plan Sponsor reserves the right to amend or change this Privacy Policy at any time (including retroactively) without notice, except to the extent notice is required under the HIPAA Privacy Rule.

This Privacy Policy does not create any third-party rights (including, but not limited to, rights of Health Plan participants, covered dependents and business associates). This policy is a guideline for compliance with the HIPAA Privacy Rule, and will not be binding on the Plan Sponsor to the extent it establishes requirements and obligations beyond those required by the HIPAA Privacy Rule. This policy does not address requirements under other federal laws or state laws. To the extent this policy conflicts with the applicable requirements of the HIPAA Privacy Rule, the Privacy Rule shall govern.

DEFINITIONS

Except as otherwise described in this policy, all terms used shall have the definition given to them by the HIPAA Privacy and Security Rules, as applicable.

- Business associate – A business associate is an entity that: (1) creates, receives, maintains or transmits PHI on behalf of a covered entity (including for claims processing or administration, data analysis or underwriting); or (2) provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation or financial services to a covered entity, where the performance of those services involves access to PHI.
- Covered entity – A health plan, health care clearinghouse or health care provider who transmits any health information in electronic form in connection with a HIPAA-covered transaction.
- Designated record set – A group of records maintained by or for the Health Plan that is:
  - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for the Plan; or
  - Used, in whole or in part, by or for the Health Plan to make decisions about individuals.

[SAMPLE]

Security Policy

[SAMPLE]

Notification Policy

Download Now >

Editable Templates

Sample HIPAA Privacy Policy

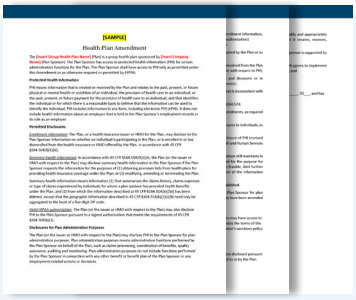
Sample HIPAA Security Policy

Sample Breach Notification Policy

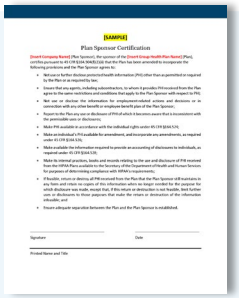
Sample Documents

Other Sample Documents

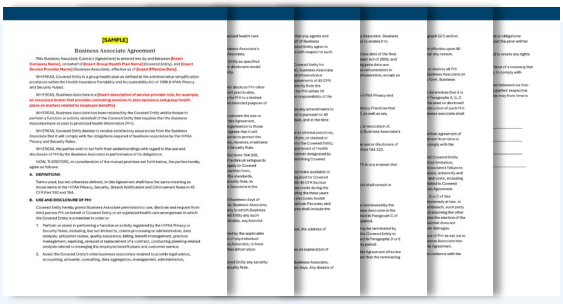
The following are sample documents for various HIPAA documentation requirements, such as the plan amendment and business associate agreement requirements. These samples cannot be used "as is"—they must be customized where indicated for specific plan and employer information. Also, if the sample policies do not accurately reflect an employer's implementation of the HIPAA Rules, they should be customized for the employer's specific approach. We encourage all customization to take place in coordination with knowledgeable benefits counsel. **Nothing in this toolkit should be considered as legal advice, including these sample documents. These sample documents are provided for educational and illustrative purposes only.**



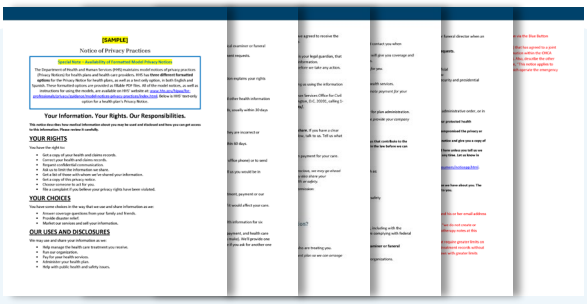
Sample Health Plan Amendment



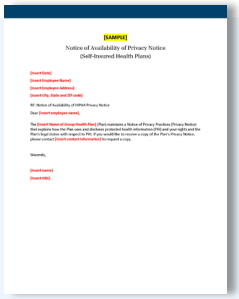
Sample Plan Sponsor Certification



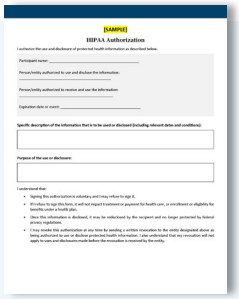
Sample Business Associate Agreement



Sample Notice of Privacy Practices (Privacy Notice)



Sample Notice of Availability of Privacy Notice (Self-Insured Plans)



Sample HIPAA Authorization

Compliance Support from
the Professional at GBS

GBS

A Leavitt Group Company