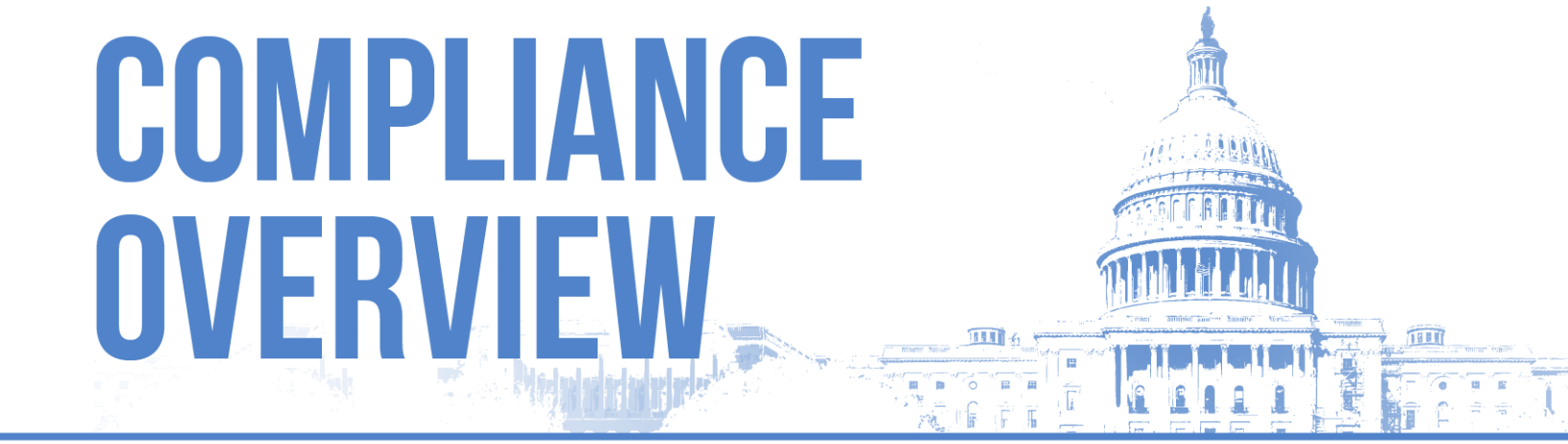
# COMPLIANCE OVERVIEW



## HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. The Privacy Rule applies to covered entities—health plans, health care clearinghouses and most health care providers—and their business associates.

The HIPAA Privacy Rule:

- ☑ Sets limits and conditions on the uses and disclosures of protected health information (PHI) that can be made without an individual's authorization;
- ☑ Gives individuals rights over their PHI, including the right to receive a notice from covered entities about their privacy practices; and
- ☑ Requires appropriate safeguards to protect the privacy of PHI.

The Privacy Rule applies to both self-funded and fully insured health plans. However, 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 Privacy Rule.

### LINKS AND RESOURCES

The Department of Health and Human Services' (HHS) website includes a brief summary of the HIPAA Privacy Rule and links to the official regulation text.

## Affected Entities

- The HIPAA Privacy Rule applies to covered entities and business associates.
- A covered entity is a health plan, a health care clearinghouse or a health care provider that conducts certain transactions electronically.
- In general, a business associate is an entity that performs a function, activity or specific service for a covered entity that involves PHI.

## Impact on Employers

- The extent of a plan sponsor's obligations under the Privacy Rule depends on whether the employer has access to PHI for plan administration.
- Sponsors of fully insured plans that do not have access to PHI have minimal obligations under the Privacy Rule.

## Affected Entities

The HIPAA Privacy Rule directly regulates these covered entities:

- ☑ Health plans;
- ☑ Health care clearinghouses; and
- ☑ Health care providers that conduct certain transactions electronically.

> ***Exception for Small, Self-funded Health Plans***
>
> 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 Privacy Rule. 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.

### *Business Associates*

Business associates also must comply with the Privacy Rule. In general, a business associate is 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 (TPA) or broker consultant for a health plan. Before the business associate may create or receive any PHI on behalf of the covered entity, the two parties must enter into a written business associate agreement.

If a business associate delegates any of its functions to a subcontractor that creates, receives, maintains or transmits PHI on its behalf, the business associate must enter into a written contract with the subcontractor to ensure that the subcontractor will agree to comply with the HIPAA Privacy and Security Rules.

### *Plan Sponsors*

The Privacy Rule indirectly regulates employers as plan sponsors. If an employer performs administrative functions for its group health plan (for example, reviewing health FSA claims), the employer will usually need to access PHI from the plan. 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 Privacy Rule.

Employers with fully insured health plans have minimal compliance obligations under the HIPAA Privacy Rule if they do not create PHI or receive it from the health insurance issuer. In this situation, most of the HIPAA compliance obligations fall on the health insurance issuer, and not on the employer-sponsored group health plan.

In order for a plan sponsor or other third party to discuss a pending claim on behalf of the plan participant with an insurance carrier or third-party administrator, the HIPAA Privacy Rule requires that the insurance carrier or third-party administrator be provided with the plan participant's written authorization.

# COMPLIANCE OVERVIEW

## Protected Information

The HIPAA Privacy Rule governs PHI.

### *What is PHI?*

PHI is individually identifiable health information (in oral, written or electronic form) that is created or received for a covered entity and relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.

## Privacy Protections

While some states have laws that protect patients' privacy, the HIPAA Privacy Rule establishes a minimum level of privacy protection that must be given to all PHI covered by the Rule. In summary, the Privacy Rule includes three main categories of protection for PHI:

| | |
|---|---|
| **Use and Disclosure Rules** | Covered entities may use and disclose PHI for purposes of treatment, payment and health care operations, subject to a minimum necessary standard. Unless an exception applies, a covered entity must first obtain an individual's written authorization before using or disclosing PHI for any other purpose. |
| **Individual Rights** | Providers and health plans must provide individuals (for example, health plan participants) with detailed written information that explains their privacy rights and how their information will be used (a Privacy Notice). Individuals also have the right to:<br>• Access their own health records and request corrections;<br>• Request restrictions on the uses and disclosures of their PHI, including that communications containing PHI be sent to an alternate location; and<br>• Obtain documentation of certain disclosures made of their health care records. |
| **Administrative Safeguards** | Covered entities must develop written privacy procedures and implement appropriate safeguards. For example, covered entities must designate a privacy officer, train employees and establish a system for receiving complaints. Covered entities must refrain from intimidating or retaliatory acts, and they cannot require a waiver of HIPAA privacy rights. |

## Requirements for Health Plan Sponsors

The compliance requirements indirectly imposed on a plan sponsor by the HIPAA Privacy Rule **vary based on whether the plan sponsor has access to PHI.**

### *Plan Sponsors Offering a Fully Insured Group Health Plan—No Access to PHI*

A plan sponsor that offers a fully insured group health plan will be minimally impacted by the HIPAA Privacy Rule if its access to health information is limited to the following plan sponsor functions:

- ☑ Assisting employees with claim disputes as permitted by the employees' written authorization;
- ☑ Receiving summary health information (SHI) for purposes of obtaining premium bids or modifying, amending or terminating the plan; and
- ☑ Conducting enrollment and disenrollment activities.

SHI summarizes claims history, claims experience or types of claims experienced by individuals from whom a plan sponsor has provided health benefits under a group health plan. The HIPAA Privacy Rule requires that certain identifiers such as name, Social Security number and date of birth be excluded from SHI.

Plan sponsors offering a fully insured group health plan with no access to PHI may not:

- ☒ Require an individual to waive rights provided by the Privacy Rule as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits; or
- ☒ Intimidate, threaten, coerce, discriminate against or take other retaliatory action against an individual for exercising rights provided by the Privacy Rule.

### *Plan Sponsors Offering a Fully Insured or Self-funded Group Health Plan—With Access to PHI*

Sponsors of fully insured group health plans that have access to PHI for plan administration functions are required to comply with the Privacy Rule's requirements. These requirements also apply to sponsors of self-funded group health plans.

Where a plan sponsor has access to PHI in order to perform plan administration functions, the plan sponsor must do all of the following:

- Implement policies and procedures that address the Privacy Rule's requirements, considering the health plan's size and types of activities involving PHI;
- Designate a privacy officer;
- Train workforce members on HIPAA policies and procedures;
- Adopt a sanctions policy for employees who fail to comply with applicable HIPAA requirements;
- Provide a process for individuals to make complaints about the plan's privacy policies and procedures;
- Refrain from taking retaliatory action against an individual who makes a complaint with the plan sponsor, group health plan or HHS alleging a violation of the HIPAA Privacy Rule;
- Implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI;
- Amend the health plan documents to impose restrictions on the employer's use and disclosure of PHI;
- Develop and maintain a Privacy Notice;

- Not use PHI from the health plan in any employment-related action or decision, or in connection with any other benefit plan;
- Not require individuals to waive their privacy rights as a condition of enrollment in the plan or of eligibility for benefits, treatment or payment;
- Comply with individual rights' requirements;
- Enter into business associate agreements, as necessary; and
- Maintain HIPAA documentation for at least six years.

## Enforcement

HHS' Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy Rule. OCR enforces HIPAA's Privacy and Security Rules by investigating complaints, conducting compliance reviews of covered entities and business associates and performing education and outreach to promote compliance with the Rules' requirements. OCR also works in conjunction with the Department of Justice to refer possible criminal violations of HIPAA.

An OCR investigation **may trigger civil penalties** for a covered entity or business associate. The penalty amounts vary based on the type of violation. Also, penalties may not apply if the violation is corrected within 30 days of when the entity knew, or should have known, of the violation.

The civil penalty amounts are subject to annual inflation-related increases. Penalty amounts for civil penalties assessed on or after Jan. 17, 2020 (relating to violations occurring after Nov. 2, 2015), are as follows:

| Type of Violation | Minimum Penalty/Violation | Maximum Penalty/Violation |
|---|---|---|
| Did not know about violation | $119 | $59,522 |
| Violation due to reasonable cause | $1,191 | |
| Corrected violation caused by willful neglect | $11,904 | |
| Violation caused by willful neglect, not corrected | $59,522 | $1,785,651 |

The possible **criminal penalties** for violations of the HIPAA Privacy and Security Rules 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.