
Lexis Practice Advisor®

# HIPAA Privacy and Security Presentation

# Overview

This training discusses:

- The HIPAA Privacy Rule
- The HIPAA Security Rule
- How to handle and safeguard protected health information, or PHI

# What is HIPAA?

# HIPAA Training Requirements

HIPAA regulations require a covered entity or business associate (in short, the group health plan and its vendors) to implement a security awareness and training program for all members of its workforce, including management.

This presentation is designed to meet this regulatory training requirement.

# Privacy Rule and Security Rule

HIPAA's Privacy Rule provides the framework for protecting PHI from unauthorized access and disclosure.

HIPAA's Security Rule safeguards electronic PHI.

# The Privacy Rule

# What is HIPAA's Privacy Rule?

HIPAA's Privacy Rule provides the framework for protecting certain health information of health plan participants (employees/former employees, their spouses and dependents) from unauthorized access or disclosure by:

- Covered Entities (group health plans, physicians and hospitals)
- Their Business Associates (their vendors)

# What Does the HIPAA Privacy Rule Require?

To comply with the Privacy Rule, a group health plan (like any other covered entity) must comply with the following:

- Provide **notice** of privacy practices.
- Adopt appropriate administrative, technical, and physical **safeguards** to protect participant PHI privacy and implement Privacy Rule policies and procedures.
- Designate a **privacy officer**.
- **Train** workforce members on HIPAA compliance.
- Enter into **business associate agreements** with applicable vendors.
- Grant participants the right to access, amend, and receive an accounting of their **PHI disclosures**.

# What Does the HIPAA Privacy Rule Require? (continued)

HIPAA protects against unauthorized access and disclosure. Here, disclosure is defined to mean (1) releasing, (2) transferring, (3) providing access to, or (4) divulging in any manner information outside the entity holding the information. 45 C.F.R. § 160.103. When explaining HIPAA, recognize that:

- Health information held by a Covered Entity is usually protected, subject to exceptions for processing claims and other administrative necessities
- Health information held by an employer in its role as employer is not protected
- Health information held by an employer that is HIPAA-protected must be handled confidentially and never used to make employment decisions
- Employers and their employees must act reasonably and within the scope of HIPAA when handling PHI created or collected by the plan

# Who is Subject to HIPAA?

- Health plans (like group health plans)
  - Excludes self-administered plans with fewer than 50 participants
  - Excludes plans offering only certain types of coverage (like limited scope dental-only or vision-only care)
- Health Care Clearinghouses –and–
- Health Care Providers (physicians, hospitals)

# Employer Group Health Plan Covered Entities

A group health plan that is a covered entity may be:

- An insured health plan (and its issuer) –or–
- A self-insured group health plan

# Who Has the Responsibility?

- **Fully insured health plans maintained by an employer without access to PHI:** If an employer sponsors a group health plan that does not create or receive PHI (other than summary health or enrollment information) the employer need not comply with the HIPAA Privacy Rule and the HIPAA Security Rule. However, the insurer is subject to the rules.

- **Self-funded and Fully-insured plans health plans having PHI access:** These plans will need to comply with the HIPAA Privacy Rule and the HIPAA Security Rule, even if the self-funded plan uses a third-party administrator for all plan administration functions.

# Who are Business Associates?

A Covered Entity may need to permit a contractor, subcontractor, or other outside persons or entities to access PHI to provide services to the Covered Entity. These services may include the handling, processing, or reviewing of health claims.

These third parties are the Business Associates of the Covered Entity.

# Need for Business Associate Agreements

**Contracts Required:** Covered entities are required to obtain satisfactory assurances from the business associate in the form of a written contract or other arrangement that the business associate will appropriately handle and safeguard the covered entity's PHI.

# What Does Protected Health Information Include?

PHI is individually identifiable health information, including demographic data, that relates to:

- An individual's 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 an individual

# Protected Health Information Examples

PHI includes:

- Information your doctors, nurses, and other health care providers put in a participant's medical record
- Conversations a health plan participant's doctor has about the participant's care or treatment with nurses and others
- Information about a health plan participant's condition residing in a health insurer's (or other covered entity's) computer system
- Billing information about a participant – and –
- Most other health information about a participant held by the covered entity or its business associate

# What Does PHI Exclude?

PHI does not include individually identifiable health information that is:

- In education records covered by the Family Educational Rights and Privacy Act
- In records on a student who is 18 years or older, or attending an institution of post-secondary education, which were made by certain medical professionals when providing treatment to the student
- In employment records held by a covered entity in its role as employer
–or–
- Regarding a person who has been deceased for more than 50 years

# Permitted Uses and Disclosures of PHI

Although HIPAA aims to prevent the unauthorized disclosure of an individual's PHI, certain disclosures are permitted, or required, for example, for claims processing and plan administration.

The following are permitted PHI uses and disclosures:

- Disclosures to the individual of their own PHI
- Uses or disclosures for treatment, payment, or health care operations
- Uses or disclosures incidental to a permitted or required use or disclosure
- Uses or disclosures specifically authorized or consented to by the individual
- Certain disclosures for public purposes (e.g., as required by law, to address public health matters, to report on victims of abuse, neglect, or domestic violence, to facilitate authorized health oversight activities, for research, to facilitate military and other specialized government functions, among others)
- Uses or disclosures of limited data sets (PHI that has been stripped of certain identifying information) for research, public health, or health care operations activities
- Uses and disclosures related to certain underwriting activities

# The Privacy Notice

Individuals have a right under HIPAA to receive a written notice describing:

- The uses and disclosures of their PHI that may be made by a group health plan or other covered entity
- The individuals' rights regarding PHI –and–
- The covered entity's legal duties regarding PHI

# Contents of Privacy Notice

- Header
- Uses and Disclosures
- Separate statement for certain uses and disclosures
- Statement of the individual’s rights (like an accounting)
- Statement of the covered entity’s duties
- A statement of how to issue a complaint
- Contact information
- An effective date

# Responsibility for and Delivery of the Privacy Notice

A Covered Entity is responsible for delivering the notice to participants:

- For self-funded plans, the plan must furnish the notice.
- For fully insured plans:
  - **Where employer handles PHI**. Here, the insurer or HMO must furnish the notice, or the employer if the plan has access to PHI (other than summary health information and participation and enrollment data).
  - **Hands-off plans**. Where the employer sponsor of a fully insured plan does not create or handle PHI, except for summary health information and participation and enrollment data, the notice obligation falls on the health insurer or the HMO.

# Renewal of the Privacy Notice

The plan must maintain the current notice and provide it to the named insured:

- Upon request
- Within 60 days of a material revision –and–
- At least once every three years notifying covered individuals of the availability of and how to obtain the notice

# Need for a Privacy Officer

A group health plan must:

- Appoint a privacy official who is responsible for monitoring and enforcing privacy policies and procedures –and– Designate a contact person or office to receive complaints under the Privacy Rule

# Additional HIPAA Administrative Responsibilities

In addition to establishing HIPAA policies and procedures and safeguarding PHI, the plan must also satisfy the Privacy Rule by:

- **Establishing a complaint procedure**. The plan must establish a process for individuals to make complaints concerning the plan's privacy policies and procedures and document all complaints and their disposition.
- **Applying sanctions.** The plan must apply and document sanctions against workforce members who fail to comply with its privacy policies and procedures.
- **Mitigating impermissible PHU disclosures.** The plan must mitigate any use or disclosure of PHI in violation of its policies and procedures or the Privacy Rule.
- **Documenting violations.** The plan must document any use or disclosure of PHI in violation of its policies and procedures or the Privacy Rule.

# HIPAA's Security Rule

# What is HIPAA's Security Rule?

HIPAA's Security Rule requires covered entities and business associates to implement basic safeguards to protect electronic PHI from unauthorized:

- Access
- Alteration
- Deletion other than under recordkeeping processes, and
- Transmission

# Security Rule Standards

The Security Rule sets forth standards for the protection of ePHI in the following areas:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational requirements –and–
- Policies and procedures

# Apply Reasonable and Appropriate Measures

Group health plans and other covered entities may use any security measures that allow them to reasonably and appropriately implement the standards of the Security Rule.

Consider the following when determining what security measures are reasonable and appropriate:

- Size, complexity, and capabilities of the plan
- Technical infrastructure, hardware, and software security capabilities of the plan
- Costs of security measures –and–
- Probability and importance of potential risks to ePHI

# Required or Addressable Standards

Most of the Security Rule standards have implementation specifications, which are categorized either as required or addressable.

- **Required** means a process must be implemented by a covered entity or business associate.
- **Addressable** means a covered entity or business associate can make an assessment on whether to implement or not implement.

# Security Officer

HIPAA regulations require all Covered Entities to identify a **HIPAA Security Officer** who is responsible for the development and implementation of policies and procedures ensuring the integrity of electronic PHI (ePHI).

# Questions?