HIPAA Compliance for Health Plans

Privacy, Security and Breach Notification Rules

Presented by: AccesseHR Insurance Services

Introduction

Agenda

- Who is subject to the HIPAA Rules
- What information is protected
- Key requirements of HIPAA Rules
- Enforcement
- Compliance steps

HIPAA Overview

HIPAA Rules

HIPAA is a broad federal law that includes Privacy, Security and Breach Notification Rules for protected health information (PHI)

Privacy Rule	Security Rule	Breach Notification Rule
• Sets standards for when PHI may be used or disclosed • Gives individuals certain rights	• Sets standards for protecting electronic PHI (ePHI)	• Requires notification when there is a breach of unsecured PHI

Who Is Subject to the HIPAA Rules?

Covered Entities

The HIPAA Rules apply directly to **covered entities**

Covered entities include:

- Health plans and health insurance issuers
- Health care clearinghouses
- Most health care providers

Health Plans

- Includes any individual or group plan that provides or pays the cost of health care
- **Exemption** – A self-insured health plan with fewer than 50 eligible employees is exempt if it is administered by the employer

Covered Health Plans - Examples

- Medical plans (fully insured or self-insured)
- Dental and vision plans
- Prescription drug plans
- Health reimbursement arrangements (HRAs)
- Health flexible spending accounts (FSAs)
- Wellness programs that provide medical care

Business Associates

- HIPAA Rules also apply to business associates
- Business associate = organization that performs certain functions for (or provides certain services to) a covered entity that involve PHI
- *Examples* – Third-party administrator (TPA), pharmacy benefit manager (PBM), consultant, broker or auditor

Employers

Employment functions

- Employers are not covered entities
- HIPAA Rules do NOT apply when performing employment functions
- *Examples* – administering leave of absence or fitness for duty

Health plan functions

- Health plans are covered entities
- HIPAA Rules apply when performing administrative functions on behalf of health plan that involve PHI (for example, reviewing claims)
- Must agree to comply with certain HIPAA requirements

KEY POINT

Extent of an employer's obligations under HIPAA Rules mainly depends on its **access to PHI from the health plan**

What Information Is Protected?

Protected Health Information

Protected Health Information (PHI)	**Individually identifiable health information** that is transmitted or maintained by a covered entity (or business associate)
	Can be in **any form or media** (for example, written, verbal or electronic). *Security rule only applies to ePHI*
	Does not include **employment records** held by an employer (for example, drug screenings, leave requests, disability information)
	Does not include **de-identified health information**

Information Definitions

Summary Health Information

- Information summarizing claims history, expenses or types of claims with almost all specific identifiers removed

De-identified Information

- Health information that no longer identifies an individual. Two methods to de-identify:
  - *Statistical method* – expert determination
  - *Safe harbor method* – remove 18 identifiers

HIPAA Privacy Rule

Overview

The Privacy Rule includes three main protections:

Use and Disclosure Rules	Limit when covered entity can use or disclose individual's PHI. In general, cannot use or disclose unless permitted by Privacy Rule or authorized by individual
Individual Rights	Provide individuals with certain rights with respect to their PHI, including right to receive a Privacy Notice
Administrative Safeguards	Require covered entities to develop written privacy procedures and implement appropriate safeguards, including designating a privacy officer and training employees

Special Exception for Fully Insured Health Plans

Employers that offer fully insured health plans and are “hands off” PHI have minimal obligations under Privacy Rule

“Hands off” PHI means PHI the employer creates or receives is limited to enrollment information, summary health information and information released pursuant to a HIPAA authorization

Use and Disclosure Rules

Permitted Disclosures

- To the individual
- For public policy purposes
- For treatment, payment or health care operations

Authorized Disclosures

- Must obtain an individual's authorization for other disclosures
- Specific requirements for HIPAA authorizations

Disclosures to Employers

Health plan (or insurance issuer) may disclose the following PHI to the plan sponsor:

- Plan **enrollment** information
- **Summary health information** (to obtain premium bids or modify or terminate the plan)
- PHI of group health plan enrollees for **plan administration purposes**
- *Note:* Any other disclosures would require a HIPAA authorization from the individual

To receive PHI for plan administration purposes, the health plan document must be amended to include certain restrictions. Also, the employer cannot use PHI for any **employment-related actions** or for **another benefit plan**.

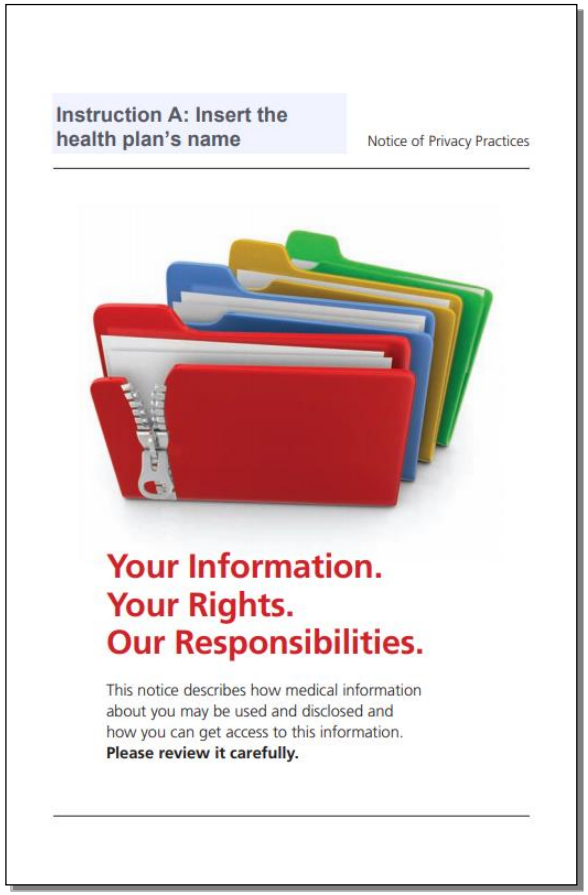
Disclosures to Business Associates

Can disclose PHI to a business associate

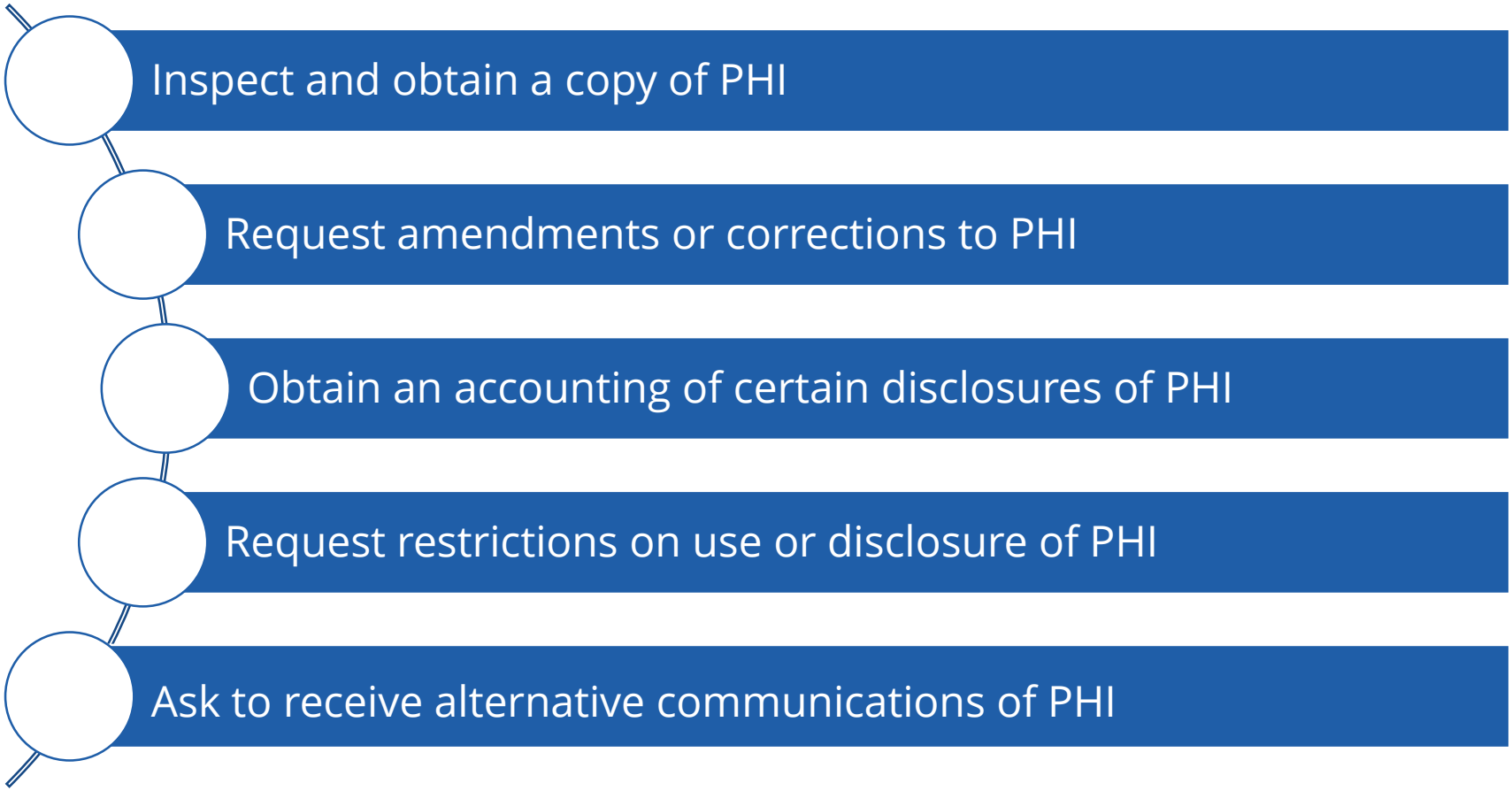
- A written business associate agreement must be in place
- Agreement must establish permitted and required uses and disclosures of PHI by business associate
- Business associate must protect PHI
- Business associate cannot use or disclose PHI in a manner that would violate the HIPAA Rules

Privacy Notice

- Health plans must provide a Privacy Notice at time of enrollment and upon request
- Every three years, health plans must provide a Privacy Notice to plan participants (or notify them of Notice's availability)
- Special exceptions for **fully insured health plans**:
  - *"Hands on" PHI:* Must maintain a Privacy Notice and provide upon request
  - *"Hands off" PHI*: No Privacy Notice required (issuer has entire responsibility)



Other Individual Rights



Administrative Requirements

Group health plans must comply with these requirements:

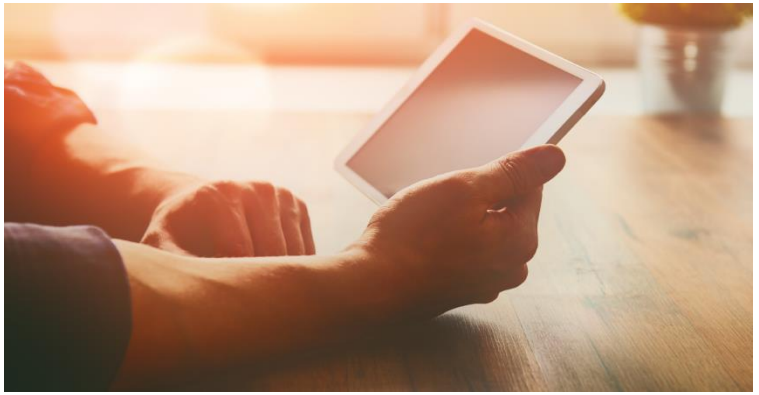
- Implement privacy **policies and procedures**
- Designate a **privacy officer**
- **Train employees** on privacy policies
- Provide a **complaint process**
- Establish and apply **sanctions** for privacy violations
- Protect the privacy of PHI through **safeguards**

Fully insured health plans that are "hands off" PHI are not subject to these administrative requirements

HIPAA Security Rule

Overview

- Establishes standards for securing ePHI
- Requires covered entities to perform a **risk analysis**



- Requires covered entities to implement **reasonable and appropriate safeguards** to protect ePHI, based on risk analysis

Electronic PHI (ePHI) – PHI maintained in or transmitted by electronic media (e.g., PHI on computers, electronic devices and smartphones).

Risk Analysis

Crucial first step for compliance with Security Rule

Common steps include:

- Identify ePHI
- Identify potential threats and vulnerabilities
- Assess current security measures
- Determine likelihood and potential impact of threats
- Determine risk level
- Implement security safeguards

Security Safeguards

KEY POINTS

- Covered entities must maintain **reasonable and appropriate** safeguards for protecting ePHI
- What is reasonable and appropriate depends on nature of entity's business, including size, complexity and resources
- Each type of security safeguard has certain standards and rules associated with it
- No special exceptions for fully insured health plans, but may have fewer obligations if "hands off" PHI

Examples of Safeguards

Administrative

- Security officer designation
- Business associate contracts
- Security incident procedures

Physical

- Facility access controls
- Workstation use
- Data backup and storage

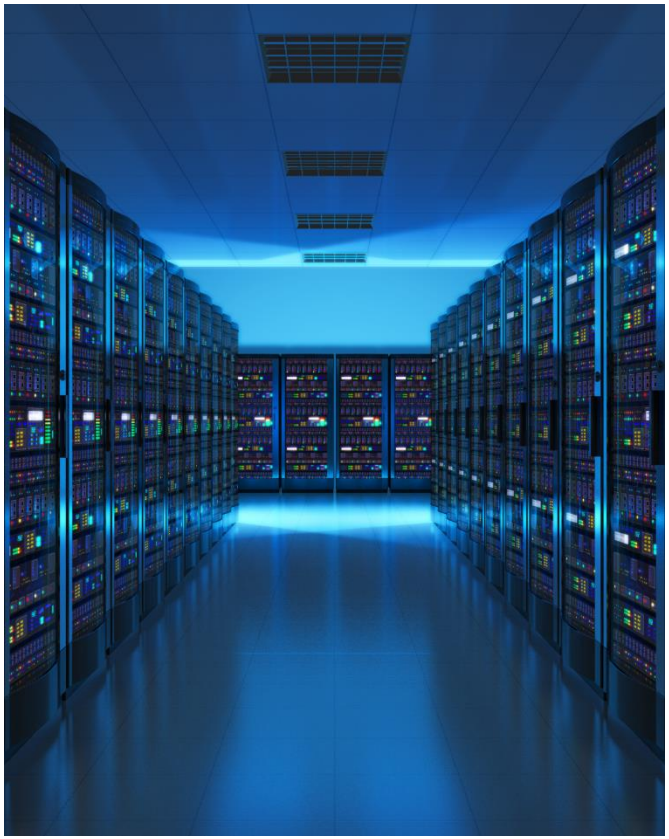
Technical

- Encryption and destruction
- Automatic logoff

Breach Notification Rule

Overview

- Covered entities must notify individuals when there has been a **breach of unsecured PHI**
- Covered entities must notify Department of Health and Human Services (HHS) of breaches
- In some cases, covered entities must notify the media



What Is a Breach?

Breach

- Unauthorized acquisition, access, use or disclosure of unsecured PHI that compromises the security or privacy of the information

Exceptions

- Disclosures where there is no retention of information
- Certain unintentional, internal disclosures
- Certain inadvertent disclosures among people authorized to access PHI

Unsecured PHI

- PHI not secured by a technology or methodology approved by HHS (Encryption and destruction are approved methods)

Breach Notification

Individuals	Individuals whose PHI was breached
	Provide without unreasonable delay
	In no case later than **60 days after breach discovered**
HHS	Breaches involving fewer than 500 individuals – provide within 60 days after end of calendar year
	Breaches involving 500 or more individuals – provide at the same time notice is given to individuals
Media	Must notify prominent media outlets if breach involves more than 500 residents of state or jurisdiction
	Provide within same time frame as notice to individuals

Enforcement

Overview

Enforcement

- Office for Civil Rights (OCR) is responsible for enforcing HIPAA Rules
- Most investigations are triggered by **individuals' complaints** or **breach notification reports**
- HIPAA audit program

OCR Website

Filing a Complaint

If you believe that a HIPAA-covered entity or its business associate violated your (or someone else's) health information privacy rights or committed another violation of the Privacy, Security, or Breach Notification Rules, you may file a complaint with the Office for Civil Rights (OCR). OCR can investigate complaints against covered entities (health plans, health care clearinghouses, or health care providers that conduct certain transactions electronically) and their business associates.

Complaint Process

Anyone can file a complaint if they believe there has been a violation of the HIPAA Rules. Learn what you'll need to submit your complaint online or in writing.

File a Complaint Online

File your complaint electronically via the OCR Complaint Portal.

Common HIPAA Mistakes

OCR's **most investigated** HIPAA-compliance issues:

- Impermissible uses and disclosures of PHI
- Lack of PHI safeguards
- Lack of patient access to PHI
- Lack of administrative safeguards for ePHI

Enforcement Data: As of Dec. 31, 2019, OCR has received over 225,378 HIPAA complaints and initiated over 993 compliance reviews. OCR has resolved 99 percent of those cases. To date, OCR has settled or imposed a civil monetary penalty in 73 cases, resulting in a total dollar amount of **$111,855,582**.

HIPAA Penalties

Civil penalty amounts *depend on the type of violation involved*. Penalties may not apply if the violation is corrected **within 30 days**. The penalty amounts are subject to annual adjustments for inflation. Criminal penalties may also be imposed.

Type of violation	Penalty Amount
Did not know	$119-$59,522 per violation
Reasonable cause	$1,191-$59,522 per violation
Willful neglect, corrected	$11,904-$59,522 per violation
Willful neglect, not corrected	$59,522 (up to a maximum of $1,785,651 per year)

Enforcement Examples

No business associate agreement

- Health care provider that did not have a business associate agreement in place agreed to pay OCR **$31,000** to settle the investigation.

Inadequate security safeguards

- Data storage device containing ePHI was stolen from insurance company (where it was left without safeguards overnight). Insurance company paid **$2.2 million** in OCR settlement.

Untimely breach notification

- Health care provider that did not provide timely notification following breach of unsecured PHI agreed to pay OCR **$475,000** to settle the investigation.

Compliance Steps

Compliance Tips

- Analyze how the HIPAA Rules apply to your health plans
- Perform a risk analysis for ePHI
- Implement reasonable and appropriate safeguards
- When in doubt, consult with legal counsel

Checklist of Key Steps

Fully insured health plan -“hands off” PHI

- Perform risk analysis for ePHI
- Adopt security safeguards for ePHI (requirements are scalable)
- Designate security official
- Adopt breach notification policy

Fully insured health plan - “hands on” PHI

- Implement Privacy Rule policies and procedures
- Train workforce
- Designate privacy officer and security official
- Perform risk analysis for ePHI
- Adopt security safeguards for ePHI
- Adopt breach notification policy
- Maintain a privacy notice (provide upon request)

Self-insured health plan

- Same steps as above for fully insured health plan that is “hands on” PHI, but must maintain and provide own privacy notice at enrollment

Questions?

Thank you