

Health Insurance Portability and Accountability Act of 1996

(HIPAA)

Privacy Policy Training

**General Information
Level I Training**



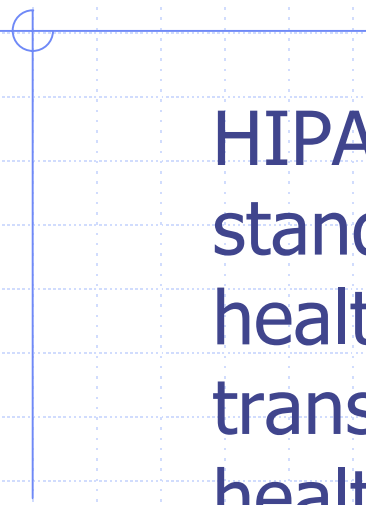
Your HIPAA Privacy Officer:
Name Goes Here

Session Facilitator:
David Shaw
HIPAA Project Management Office

Objectives of Presentation

- Refresh general knowledge of HIPAA regulations and concepts
- Understand the impact of HIPAA regulations on organization Policies and Procedures
- Identify a process for Continuous Improvement of Policies and Procedures
- Make you aware of your privacy rights as a healthcare consumer

What Is HIPAA?



HIPAA is a federal law that mandates standards that must be followed when healthcare information is used, disclosed, or transmitted for treatment, payment or healthcare operations purposes.

The rules of HIPAA affect **all** persons who have access to Protected Healthcare Information (PHI).

What Is Protected Health Information (PHI)

Any information that I can use to Individually Identify a patient.

What Is Protected Health Information (PHI)

- Names
- Address – city, state, zip code
 - The first 3 digits of a zip code may be used if more than 20,000 individuals reside in that identified area
- Any date(s) related to the individual
 - Birth date
 - Admission / Discharge / Death

What Is Protected Health Information (PHI)

- Telephone number
- Fax number
- E-mail address
- Website uniform resource locator (URL)
- Social Security number(s)
- Medical Record/Chart number(s)

What Is Protected Health Information (PHI)

- Health Plan or Beneficiary number(s)
- Vehicle Identification or License plate number(s)
- Biometric Identifiers
- Photographs

How Do We Fit Into HIPAA?

- Covered Entity (Health Plan, Service Provider, Clearinghouse)
- Hybrid Entity
- Business Associate
- Voluntary Compliance

What Is HIPAA Really Doing?

- Setting standards so that healthcare information is handled the same
- Protecting the Privacy and Security of PHI
- Creating an atmosphere that allows change to existing systems, policies, procedures

HIPAA Standards Apply To:

- Transactions (paper or electronic)
- Code Sets
- Unique Identifiers
- Security
- Privacy

Transactions

- Health Claims
- Health Claims attachments
- Health Claims Payment Advice
- Health Claim Explanation of Benefits
- Claim Status - Request & Response
- Eligibility Status - Request & Response
- Health Plan Enrollment, Dis-enrollment, Maintenance

Code Sets

- ICD-9-CM International Classification of Diseases (ICD-10-CM pending)
- CPT-4 American Medical Association - Common Procedural Terminology
- ADA American Dental Association - procedures and nomenclature
- HCPCS HCFA Common Procedure Coding System

Unique Identifiers

- EIN Employer Identification Number
- PIN Provider Identification Number
- HIN Health Plan Identification Number

Security

- Includes administrative procedures, physical safeguards, technical security
- Protect against threats or hazards to the integrity, security, confidentiality and availability of data in transit or at rest

Security

- Protect against unauthorized use or disclosure
- April 22, 2005 Compliance Deadline,
(Privacy related safeguards needed by
April 14, 2003)

Security

Safeguarding Patient Information

- Secure data transmission
- Access controls (chain of trust) for systems, data sets
 - Authentication (who asked for info)
 - Access Controls (minimum needed)
 - Data Integrity
 - Time Synchronization (time/date verified)
 - Non-repudiation (confirm data received)
 - Termination of access

Security

Safeguarding Patient Information

- Risks assessed for fax, e-mail, open shelving, etc
- Business Associate Agreements in place

Privacy

- Requires everyone in healthcare to control their access to, use of, and disclosure of Protected Health Information (PHI)
- Patient Authorization may need to be obtained before disclosing PHI in many situations
- Establishes penalties for failure to comply with HIPAA regulations

Privacy

Each of you must –

Understand the impact of HIPAA
regulations on your organizations'
Policies and Procedures

Privacy

Each of you must –

Apply HIPAA regulations to your everyday work assignment to make sure that both you as an individual and your organization are not put at risk

So What Have We Done?

- A Privacy Officer (PO) has been identified for the organization
- Standard policy and procedure templates have been applied, and a set of policies and procedures have been created and/or updated by the PO
- A copy of organization policies has been distributed to support this training

So What Have We Done?

- Procedures to support the policies are being developed
- A continuous improvement initiative was created to make sure that policies and procedures continue to follow HIPAA regulations
- This training was established to link **YOU** to the policies and procedures

What Are the Parts of HIPAA Privacy Regulation?

- Administrative/Legal Requirements
- Patient Authorization
- Use and Disclosure of Protected Health Information (PHI)
- Rights of the individual

Administrative Requirements

- Staff Training
- HIPAA Penalties for misuse
 - Accidental / Incidental disclosure
 - Intended disclosure
 - Disclosure for profit
- Documentation

Staff Training

- All members of the workforce must be trained in awareness of HIPAA concepts
- Anyone using or disclosing PHI must be trained on a organization policy and procedure
- Continuous training is required – refresher courses, training on changes to policy/procedure
- Training must be documented

HIPAA Penalties for Misuse

- **Penalties for misuse** – Enforcement will be by the Office of Civil Rights (OCR) since these violations are of an individuals' rights
 - **Maximum Civil Penalty**
\$100/each violation - \$25,000/person/year/violation
 - **Improperly obtaining/disclosing PHI**
Up to \$50,000 + up to 1 year federal prison

HIPAA Penalties for Misuse

- Obtaining/disclosing PHI under 'false pretenses'

Up to \$100,000 + up to 5 years federal prison

- Obtaining/disclosing PHI for commercial advantage, personal gain, malicious harm

Up to \$250,000 + up to 10 years federal prison

Documentation

- All policies and procedures must be kept in written format
- All changes to policies and procedures must be distributed to affected employees
- Any violation or employee sanction, and the issue resolution must be documented
- Policy templates are copyrighted materials

Which Policies / Procedures Are Affected by This Regulation?

- List appropriate Policies/Procedures
General Information Policies

Discussion of Our Affected Policies/procedures

- Do we need all the PHI that is used
- Where are we vulnerable to disclosures/penalties
- What can be done to strengthen our:
 - Policy
 - Procedure
 - Processes/systems

Patient Authorization

A patient may authorize the use of PHI, for specified purposes other than for treatment, payment or operations.

- Privacy Notice must be presented
- Authorization vs TPO

Patient Authorization

Notice of Privacy Practices

- A copy of the Notice of Privacy Practices for a covered entity must be made available for any individual
- The Notice of Privacy Practices binds the provider to specific uses and disclosures of patient information
- Providers must attempt to obtain an acknowledgement of receipt

Patient Authorization

Notice of Privacy Practices

- The Notice of Privacy Practices must contain:
 - A description of the types of uses and disclosures the provider will make for treatment, payment and operations purposes
 - A description of any state laws that are more protective of patient information
 - A statement of the individuals rights and how to exercise those rights

Patient Authorization

Notice of Privacy Practices

- The Notice of Privacy Practices must contain: (cont'd)
 - A statement of uses and disclosures made only upon receipt of patient authorization
 - Safeguards of PHI
 - Information on how and where to file complaints

Patient Authorization

- Authorization is NOT required for:
 - Treatment, Payment or Healthcare Operations uses and disclosures
 - Disclosures made to the individual or their personal representative(s), family, friends
 - For facility directories (identification and location)
 - Custodial situations
 - Victims of a crime

Patient Authorization

- Authorization is NOT required for:
 - As required by state/federal law
 - Public Health purposes
 - Military and veterans
 - Medical Suitability Determination
 - Emergency/Disaster situations
 - National security, Intelligence, law enforcement
 - Research

Which Policies / Procedures Are Affected by This Regulation?

- List appropriate Policies/Procedures
Patient Authorization Policies

Discussion of Our Affected Policies/procedures

- Do we need all the PHI that is used
- Where are we vulnerable to disclosures/penalties
- What can be done to strengthen our:
 - Policy
 - Procedure
 - Processes/systems

Use and Disclosure of PHI

- Minimum Necessary Info accessed
- State Law pre-emption
- De-identified information
- Business Associate Agreement
 - Internal vs external release of info

Which Policies / Procedures Are Affected by This Regulation?

- List appropriate Policies/Procedures
General Use and Disclosure Policies

Discussion of Our Affected Policies/procedures

- Do we need all the PHI that is used
- Where are we vulnerable to disclosures/penalties
- What can be done to strengthen our:
 - Policy
 - Procedure
 - Processes/systems

Individuals Rights

- Individuals have the right to:
 - Receive an accounting of disclosures made
 - Amend their PHI
 - Inspect and copy their PHI
 - Restrict use/disclosure of their PHI
- Must know how to lodge a complaint

Which Policies / Procedures Are Affected by This Regulation?

- List appropriate Policies/Procedures
Individuals Rights Policies

Discussion of Our Affected Policies/procedures

- Do we need all the PHI that is used
- Where are we vulnerable to disclosures/penalties
- What can be done to strengthen our:
 - Policy
 - Procedure
 - Processes/systems

Continuous Improvement of Our Policies and Procedures

- Each of you are commissioned to:
 - Monitor PHI usage and disclosures in your work assignments and those around you
 - Analyze gaps in protection and security of information
 - Report/Discuss any issues to your HIPAA Privacy Officer
 - Suggest resolutions and/or Policy/Procedure changes

Teamwork Is the Answer

