HealthStream Regulatory Script

HIPAA
Release Date: August 2009
HLC Version: 602

Lesson 1: Introduction
Lesson 2: HIPAA Overview
Lesson 3: Transactions & Code Sets
Lesson 4: Security
Lesson 5: Unique Identifiers
Lesson 6: Privacy
Lesson 1: Introduction

Introduction

Welcome to the lesson on HIPAA, the Health Insurance Portability and Accountability Act.

As your partner, HealthStream strives to provide its customers with excellence in regulatory learning solutions. As new guidelines are continually issued by regulatory agencies, we work to update courses, as needed, in a timely manner. Since responsibility for complying with new guidelines remains with your organization, HealthStream encourages you to routinely check all relevant regulatory agencies directly for the latest updates for clinical/organizational guidelines.

If you have concerns about any aspect of the safety or quality of patient care in your organization, be aware that you may report these concerns directly to the Joint Commission.
### Rationale

As a worker in the healthcare industry, you are affected by the Administrative Simplification Requirements of HIPAA. You are required by law to follow these rules.

In 2009, the American Recovery and Reinvestment Act (ARRA) made changes to HIPAA. Individuals who obtain protected information without authorization can face criminal penalty. This includes employees at a hospital.

This course will help you comply with HIPAA.

You will learn about:
- Which organizations are covered by HIPAA
- The penalties for violating HIPAA
- The Administrative Simplification Requirements of HIPAA, and how to comply with each
Course Goals

After completing this course, you should be able to:

- Identify covered entities [glossary] under HIPAA
- List eight electronic health transactions [glossary] covered by HIPAA and the medical code sets [glossary] to be used for these transactions
- Recognize safeguards required by HIPAA to ensure the security and integrity [glossary] of electronic health information
- Identify the unique employer identifier used under HIPAA
- Distinguish between uses and disclosures [glossary] of health information that are and are not allowed under the HIPAA Privacy Rule
Course Outline

This introductory lesson gave the course rationale and goals.

Lesson 2 gives an overview of HIPAA. This includes who is covered by HIPAA and penalties for violating the act.

Lesson 3 covers transactions and code sets under HIPAA.

Lesson 4 describes the HIPAA standards for security and integrity of health information.

Lesson 5 specifies the unique employer identifier required under HIPAA.

Finally, lesson 6 covers the HIPAA Privacy Rule.
Welcome to the overview of HIPAA.

After completing this lesson, you should be able to:
- List the Administrative Simplification Requirements of HIPAA
- Identify organizations required to comply with HIPAA
- Specify penalties for violating HIPAA
HIPAA has many parts.

The parts that concern you, as a healthcare worker, are the Administrative Simplification Requirements.

These requirements are summed up in the image to the right. We will discuss each requirement in detail in the following lessons.

In this lesson, we will look at:
- Which organizations are covered by HIPAA
- The penalties for violating HIPAA
An organization must follow HIPAA if the organization’s business activities involve:

- Sending protected health information (PHI) electronically
- Receiving PHI electronically

An organization also must follow HIPAA if it uses any third-party vendors [glossary] who send or receive PHI electronically.

Organizations that must follow HIPAA are called “covered entities.”
Business Associates

Business associates are hired by hospitals to deal with PHI.

Business associates are also covered by portions of HIPAA. They must properly safeguard electronic PHI.

The specific business activities covered by HIPAA will be discussed in lesson 3.
In general, penalties for violating HIPAA are civil [glossary] penalties.

Civil monetary penalties include:
- $100-$50,000 for unknowingly violating HIPAA
- $1,000-$50,000 for knowingly violating HIPAA
- $10,000-$50,000 for willful neglect, if the violation is corrected
- At least $50,000 for violations resulting from willful neglect if they are not corrected
Violating **patient privacy** under HIPAA has criminal penalties, as well as civil.

These penalties are:
- Up to $50,000 fine and up to one year in jail for knowingly obtaining or disclosing PHI in violation of HIPAA
- Up to $100,000 fine and up to five years in jail for doing the above under **false pretenses** [glossary]
- Up to $250,000 fine and up to ten years in jail for doing the above with the intent to profit by, or do harm with, the information
Who Can be Liable?

Civil penalties for HIPAA violations apply to:
- Covered entities
- Business associates

Criminal penalties apply to:
- Covered entities
- Business associates
- Any employee who obtains PHI without authorization
Notification of Problems

Patients must be notified of any unauthorized activity involving their PHI.

They must be told if their information is improperly:
- Accessed
- Used
- Disclosed
An organization that ________ must follow HIPAA:

a. Sends PHI electronically
b. Receives PHI electronically
c. Uses a third-party vendor that sends PHI electronically
d. Uses a third-party vendor that receives PHI electronically
e. All of the above

MULTIPLE CHOICE INTERACTION

Correct: E

Feedback for A, B, C, D: Not quite. The best answer is E.

Feedback for E: Correct.
Summary

You have completed the overview of HIPAA. Remember:

- An organization is a covered entity if it sends or receives PHI electronically.
- An organization is also a covered entity if it does business with a third-party vendor that sends or receives PHI electronically.
- Penalties for violating HIPAA are civil damages. There are also criminal penalties for violating the privacy part of HIPAA.
Lesson 3: Transactions and Code Sets

Introduction & Objectives

Welcome to the lesson on transactions and code sets.

After completing this lesson, you should be able to:
- List eight electronic transactions covered under HIPAA
- Define each of these transactions
- Identify the medical code sets that should be used for electronic transactions under HIPAA
Rationale

In this lesson, we will look at the part of HIPAA that deals with transactions and code sets.

This part of HIPAA sets national standards for:
  - Eight electronic business transactions performed in healthcare
  - Code sets to be used for these transactions

The goal of this part of HIPAA is to simplify and improve how health information is sent electronically.

This simplification will:
  - Improve Medicare and Medicaid and other health plans
  - Improve the efficiency of the healthcare system
Prior to HIPAA, about 400 different formats were being used for electronic health transactions.

This lack of standardization:
- Made it difficult and costly to have software for electronic transactions
- Made it difficult for providers and health plans to be efficient and save money
Standardized Transactions

HIPAA sets standards for eight categories of electronic transactions:

1. Healthcare claims or equivalent encounter information
2. Eligibility for a health plan
3. Referral certification and authorization
4. Healthcare claim status
5. Enrollment and disenrollment in a health plan
6. Healthcare payment and remittance advice
7. Health plan premium payment
8. Coordination of benefits

For a brief description of each type of transaction, click on each.

On the following screens, we will take a closer look at each transaction.

1. Provider asks health plan for payment.
2. Provider or health plan asks another health plan about a patient’s benefits.
3. Provider asks health plan to authorize care or a referral.
4. Provider and health plan communicate about the status of a claim.
5. Information is sent to a health plan to start or end a patient’s healthcare coverage.
6. Health plan sends provider a payment or an explanation of benefits (EOB).
7. Premium payments are sent to a patient’s health plan.
8. Claims are sent to a health plan, to determine how much of the cost the plan will pay.
A **healthcare claim transaction** happens when a provider asks a health plan for payment. This request includes the information to support the claim.

An **equivalent encounter information transaction** happens when a provider reports to a health plan that he or she has given care to a patient. This type of transaction is used when the provider does not have a direct claim for payment, because the health plan is not set up to pay the provider for specific services.

HIPAA sets standards for:
- Retail pharmacy drug claims
- Dental healthcare claims
- Professional healthcare claims
- Institutional healthcare claims

Click on each type of claim to see the HIPAA standard.

---

**Retail pharmacy drug claims**

The HIPAA standards for these claims are:

**Dental healthcare claims**

The HIPAA standard for these claims is ASC X12 837:

**Professional healthcare claims**

The HIPAA standard for these claims is ASC X12 837:
### Institutional healthcare claims

The HIPAA standard for these claims is ASC X12 837:

## An eligibility for health plan transaction

An *eligibility for health plan transaction* happens when a provider or health plan asks another health plan about:

- A patient’s benefit eligibility
- Coverage of care
- Plan benefits

This includes the response of the health plan.

HIPAA sets standards for:

- **Retail pharmacy drug eligibility**
- **Dental, professional, and institutional eligibility**

Click on each type of transaction to learn the HIPAA standard.

### CLICK TO REVEAL

#### Retail pharmacy drug eligibility

The HIPAA standards for these transactions are:


#### Dental, professional, and institutional eligibility

The HIPAA standard for these transactions is ASC X12 270/271:


**A referral certification and authorization transaction** is any of the following:

- Asking a health plan to review and approve care
- Asking a health plan to approve a referral
- A response from the health plan

The HIPAA standard for this type of transaction is ASC X12 278:

### Category 4

**A healthcare claim status transaction** is:
- Asking about the status of a healthcare claim
- Responding about the status

The HIPAA standard for this type of transaction is ASC X12 276/277:
An **enrollment and disenrollment transaction** is sending patient information to a health plan to:
- Start insurance coverage
- End insurance coverage

The HIPAA standard for this type of transaction is ASC X12 834:
- The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Benefit Enrollment and Maintenance (834), August 2006, ASC X12N/005010X220.
A **healthcare payment and remittance advice transaction** happens when a health plan sends:

- Payment or payment information to a healthcare provider
- An EOB to a healthcare provider

HIPAA sets standards for:

- **Retail pharmacy drug claims and remittance advice**
- **Dental, professional, and institutional healthcare claims and remittance advice**

Click on each type of transaction to learn the HIPAA standard.

**Retail pharmacy drug claims and remittance advice**

The HIPAA standards for these transactions are:


**Dental, professional, and institutional healthcare claims and remittance advice**

The HIPAA standard for these transactions is ASC X12 835:

- The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221.
A *health plan premium payment transaction* happens when an organization that makes health plan payments for an individual:

- Sends a payment to a health plan
- Sends information about payment to a health plan
- Sends payment processing information to a health plan

The HIPAA standard for this type of transaction is ASC X12 820:

Transaction Category 8: Coordination of Benefits

A *coordination of benefits* transaction happens when healthcare claims are sent to a health plan, to determine how much of the cost the plan has to pay.

HIPAA sets standard in this category for:
- **Retail pharmacy drug claims**
- **Dental healthcare claims**
- **Professional healthcare claims**
- **Institutional healthcare claims**

Click on each for more information about the standard.

**CLICK TO REVEAL**

**Retail pharmacy drug claims**
The HIPAA standards for these claims are:

**Dental healthcare claims**
The HIPAA standard for these claims is ASC X12 837:

**Professional healthcare claims**
The HIPAA standard for these claims is ASC X12 837:
Institutional healthcare claims
The HIPAA standard for these claims is ASC X12 837:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Review</strong></td>
<td><strong>MULTIPLE CHOICE INTERACTION</strong></td>
</tr>
<tr>
<td>Which of the following is NOT a transaction type covered under HIPAA:</td>
<td>Correct: C  Feedback for A, B, D, E: Incorrect. The correct answer is C.</td>
</tr>
<tr>
<td>b. Healthcare claim status</td>
<td></td>
</tr>
<tr>
<td>c. Medical malpractice suit</td>
<td></td>
</tr>
<tr>
<td>d. Eligibility for health plan</td>
<td></td>
</tr>
<tr>
<td>e. Healthcare payment and remittance advice</td>
<td></td>
</tr>
</tbody>
</table>
When performing a transaction covered under HIPAA, standard code sets must be used.
### Code Sets: ICD-9-CM

The *ICD-9-CM, Volumes 1 and 2* should be used for coding:
- Diseases
- Injuries
- Impairments
- Other health problems and their symptoms
- Causes of health problems

The *ICD-9-CM, Volume 3*, should be used for coding the following types of healthcare procedures:
- Prevention
- Diagnosis
- Treatment
- Management
ICD-9-CM code sets will be replaced with:
- ICD-10-CM for diseases
- ICD-10-PCS for procedures

### Why replace ICD-9-CM code set?
- ICD-9-CM does not cover new diagnoses and procedures. It cannot capture new technology.
- It lacks precision because very different procedures are grouped together.
- Preventative services are not covered.
- The terminology is inconsistent.
- ICD-10 code sets contain more codes.
  - ICD-10-CM: 68,000 versus 13,500 in ICD-9-CM volumes 1 and 2
  - ICD-10-PCS: 72,500 versus 4,000 in ICD-9-CM volume 3
The National Drug Codes (NDC) should be used for coding:

- Drugs
- Biologics
For coding dental services, the *Code on Dental Procedures and Nomenclature* should be used.

This code is updated and distributed by the American Dental Association.
A combination of the *HCPCS* and *CPT-4* should be used for coding:

- Physician services
- Physical and occupational therapy services
- Radiology procedures
- Clinical lab tests
- Other medical diagnostic procedures
- Hearing and vision services
- Transportation services (including ambulance)
- Other healthcare services
### Code Sets: Medical: Other

The *HCPCS* should be used for coding all other medical items.

Examples of other medical items are:
- Medical supplies
- Orthotic and prosthetic devices
- Durable medical equipment

[IMAGE: 3020.JPG]
Each code set is valid for the dates given by the organization that maintains that code set.

Who maintains each code set?
- ICD-10-CM is maintained by the National Center for Health Statistics (NCHS).
- ICD-10-PCS is maintained by CMS.
- The HCPCS coding system is maintained and distributed by CMS.
When coding diseases on a transaction, which code set should be used?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>CPT-4</td>
</tr>
<tr>
<td>b.</td>
<td>HCPCS</td>
</tr>
<tr>
<td>c.</td>
<td>ICD-9-CM</td>
</tr>
<tr>
<td>d.</td>
<td>National Drug Codes</td>
</tr>
</tbody>
</table>

**MULTIPLE CHOICE INTERACTION**

Correct: C

Feedback for A, B, D: Incorrect. The correct answer is C.

Feedback for C: Correct.
You have completed the lesson on transactions and code sets. Remember:

- HIPAA covers eight electronic transactions.
- Covered entities must follow HIPAA standards for these transactions.
- Standard codes sets must be used for these transactions.
Lesson 4: Security
4001

Introduction & Objectives

Welcome to the lesson on security.

After completing this lesson, you should be able to:
• List general HIPAA security standards
• List administrative, physical, and technical security standards under HIPAA
• Identify steps for complying with each standard
4002

Security Risks

PHI could be at risk if:
- There is improper access to stored information.
- Information is intercepted when sent electronically.

The HIPAA security rule establishes national standards for protecting:
- The confidentiality of electronic PHI
- The integrity of this information
- The availability of this information

REMEMBER!

PHI is any health information that identifies a specific individual.
In general, entities covered under HIPAA must do the following:

- Ensure the confidentiality, integrity, and availability of electronic PHI
- Protect against threats to the security of PHI
- Protect against any unauthorized use or disclosure of PHI

Covered entities may choose their own specific steps to achieve these goals.

However, under HIPAA, certain general steps are required.

These steps are covered in the rest of the lesson.
HIPAA sets security standards in three categories:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

Let’s take a closer look at the standards in each category.
Under HIPAA, covered entities must:
- Prevent security violations
- Detect violations
- Contain violations
- Correct violations

Steps in complying with this standard are policies and procedures for:
- **Risk analysis**
- **Risk management**
- **Employee sanction**
- **Information system activity review**

Click on each step to learn more.

**Risk analysis**
This means looking at how the organization’s electronic PHI might be at risk.

**Risk management**
This means taking steps to address the risks found in the analysis.

**Employee sanction**
The organization must punish staff members who do not follow security rules.

**Information system activity review**
This means looking at records of activity within information systems. For example, the following should be reviewed regularly:
- Audit logs
- Access reports
- Security incident tracking records
<table>
<thead>
<tr>
<th>Admin. Safeguards: Assigned Security Responsibilities</th>
</tr>
</thead>
</table>

Covered entities must have a specific security officer for health information.

This officer is in charge of the policies and procedures for keeping PHI safe.
Admin. Safeguards: Workforce Security

Covered entities must make sure that:
- Employees who need access to electronic PHI have that access.
- Employees who should not have access to electronic PHI are not able to access PHI.

Steps in complying with this standard are policies and procedures for:
- Authorization and / or supervision
- Workforce clearance procedure
- Termination procedures

Click on each step to learn more.

CLICK TO REVEAL

Authorization and / or supervision
Organizations should authorize or supervise employees who:
- Work with electronic PHI
- Work in areas with access to electronic PHI

*Authorized* employees have permission to access PHI. *Supervised* employees have oversight by a manager when they work with or near PHI.

Workforce clearance procedure
Organizations should make sure that employees who access electronic PHI are authorized to do so.

Termination procedures
Organizations should prevent ex-employees from accessing electronic PHI.
Admin. Safeguards: Information Access Management

Covered entities must give appropriate employees the authority to access PHI.

Steps in complying with this standard are policies and procedures for:

- **Isolating healthcare clearinghouse functions**
- **Access authorization**
- **Access setup and change**

Click on each step to learn more.

**CLICK TO REVEAL**

**Isolating healthcare clearinghouse functions**
This applies to healthcare clearinghouses that are part of larger organizations. These organizations must protect electronic PHI from unauthorized access by the larger organization.

**Access authorization**
Authorized employees must have ways of accessing electronic PHI. For example, employees may be able to access electronic PHI because they are given access to:

- Workstations
- Transactions
- Programs
- Processes

**Access setup and change**
Policies and procedures should be put in place to set up, document, review, and change employee access to the mechanisms listed above.
Admin. Safeguards: Security Awareness and Training

Covered entities must train their employees on security and security awareness.

Steps in complying with this standard are policies and procedures for:

- **Security reminders**
- **Protection from viruses**
- **Log-in monitoring**
- **Password management**

Click on each step for more information.

### Security reminders
Employees should be given updates on the security program at their facility.

### Protection from viruses
Organizations must protect against computer viruses and other dangerous software. There should be procedures for:

- Guarding against software dangers
- Detecting dangers
- Reporting dangers

### Log-in monitoring
Procedures should be in place to:

- Keep track of log-in attempts
- Report any suspicious log-in activity

### Password management
Procedures should be in place for:

- Creating and changing passwords
- Keeping passwords safe
Covered entities must handle security incidents.

Steps in complying with this standard are policies and procedures for:
- **Identification and response**
- **Mitigation**
- **Documentation**

Click on each step for more information.

**Identification and response**
Security incidents should be identified. A proper response should be made.

**Mitigation**
Steps should be taken to lessen the harmful effects of known security incidents.

**Documentation**
Security incidents and their outcomes should be documented.
Admin. Safeguards: Contingency Plan

Covered entities must respond to damage to electronic systems that contain PHI.

Steps in complying with this standard are policies and procedures for:

- Data backup plan
- Disaster recovery plan
- Emergency mode operation plan
- Testing and revision
- Applications and data analysis

Click on each step to learn more.

<table>
<thead>
<tr>
<th>CLICK TO REVEAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data backup plan</td>
</tr>
<tr>
<td>Exact copies of electronic PHI should be made and kept.</td>
</tr>
<tr>
<td>Disaster recovery plan</td>
</tr>
<tr>
<td>Organizations should have procedures for recovering lost data.</td>
</tr>
<tr>
<td>Emergency mode operation plan</td>
</tr>
<tr>
<td>Organizations should have procedures for continuing to protect electronic PHI even during emergencies.</td>
</tr>
<tr>
<td>Testing and revision procedures</td>
</tr>
<tr>
<td>The plans listed above should be tested and modified as needed on a periodic basis.</td>
</tr>
<tr>
<td>Applications and data analysis</td>
</tr>
<tr>
<td>Organization should look at which data and software programs are most important for supporting their plans.</td>
</tr>
</tbody>
</table>
## Admin. Safeguards: Evaluation

Covered entities must periodically evaluate how well they are doing in keeping electronic PHI secure.
Finally, covered entities must be careful in doing business with vendors that they hire to deal with electronic PHI. Covered entities may only do business with vendors if they are certain the vendor will properly safeguard electronic PHI.
Under HIPAA, termination procedures:
   a. Protect electronic PHI from being corrupted.
   b. Prevent ex-employees from accessing electronic PHI.
   c. Ensure that backup copies of electronic PHI will be made.
   d. Punish employees who do not follow administrative safeguards.

MULTIPLE CHOICE INTERACTION

Correct: B

Feedback for A, C, D: Incorrect. The correct answer is B.

Feedback for B: Correct.
The first HIPAA physical safeguard is that covered entities must:
- Limit physical access to facilities where electronic PHI is stored.
- Make sure that authorized employees have access to these facilities.

Steps in complying with this standard are policies and procedures for:
- **Contingency operations**
  - Employees should be able to enter facilities to restore lost data during an emergency.
- **Facility security plan**
  - Facilities and electronic equipment should be protected from:
    - Unauthorized physical access
    - Tampering
    - Robbery
- **Access control and validation**
  - Organizations should control physical access to facilities. Access control should be based on each person’s role or function. This includes access control for:
    - Employees
    - Visitors
    - Patients
- **Maintenance records**
  - Work done on physical parts of the facility that have to do with security should be documented. For example, document work on:
    - Hardware
    - Walls
    - Doors
    - Locks

Click on each step for more information.
Phys. Safeguards: Workstation Use

The second HIPAA physical safeguard has to do with the use of workstations.

There should be policies and procedures for:
- What each type of workstation is used for
- How that use should be carried out
- The acceptable physical surroundings for each type of workstation
<table>
<thead>
<tr>
<th>Phys. Safeguards: Workstation Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>All workstations that access electronic PHI should have physical protections.</td>
</tr>
<tr>
<td>These physical protections should ensure that only authorized users have physical access to the workstation.</td>
</tr>
</tbody>
</table>
**Phys. Safeguards: Device & Media Controls**

Covered entities must monitor the movement of hardware and electronic media with PHI:
- Into and out of the facility
- Within the facility

Steps to comply with this standard are policies and procedures for:
- **Disposal**
- **Re-use**
- **Accountability**
- **Data backup and storage**

Click on each step to learn more.

<table>
<thead>
<tr>
<th>CLICK TO REVEAL</th>
</tr>
</thead>
</table>

**Disposal**
Electronic PHI that is no longer in active use must be disposed of in a secure manner.

**Re-use**
Electronic PHI must be removed from media before the media are reused.

**Accountability**
A record should be kept of:
- The movement of hardware and electronic media
- The responsible person for each move

**Data backup and storage**
Before equipment is moved, an exact copy of its electronic PHI should be made.
Under HIPAA:
- a. All employees should have physical access to electronic PHI.
- b. All employees should have authorization to access electronic PHI.
- c. Employees who need access to PHI should have physical access and authorization.
- d. None of the above.

**MULTIPLE CHOICE INTERACTION**

Correct: C

Feedback for A, B, D: Incorrect. The correct answer is C.

Feedback for C: Correct.
Tech. Safeguards: Access Control

The first HIPAA technical safeguard is that only authorized employees should have technical access to electronic PHI.

Steps to comply with this standard are policies and procedures for:

- **Unique user ID**
- **Emergency access procedure**
- **Automatic log-off**
- **Encryption and decryption**

Click on each step to learn more.

**CLICK TO REVEAL**

**Unique user ID**
Each authorized user should have a unique name or number. This ID should be used to identify and track the user’s access to electronic PHI.

**Emergency access procedure**
Organizations should have technical procedures for accessing electronic PHI in an emergency.

**Automatic log-off**
Electronic sessions should be ended automatically after a certain period of inactivity by the user.

**Encryption [glossary]** and **decryption [glossary]**
Electronic PHI may need to be encrypted and decrypted to ensure its security.
Covered entities must have ways to record and analyze the activity within information systems that contain electronic PHI.

These ways could be based on:
- Hardware
- Software
- Procedures
Covered entities must protect electronic PHI from being changed or destroyed improperly.

Organizations should have electronic ways of checking that electronic PHI has not been changed or destroyed without authorization.
Covered entities must have technical ways of protecting the security of PHI while it is being sent electronically.

Steps to comply with this standard are:
- **Integrity controls**
- **Encryption**

Click on each step to learn more.

**Integrity controls**
Measures should be taken to ensure that:
- PHI sent electronically is not changed improperly.
- Any improper changes will be detected.

**Encryption**
Electronic PHI should be encrypted whenever this is considered necessary for security.
Electronic PHI must be encrypted:
   a. For long-term storage
   b. Whenever the PHI is sent electronically
   c. Whenever encryption is necessary for security
   d. To protect it from personnel who have physical and technical access to PHI, but are not authorized to work with PHI

**MULTIPLE CHOICE INTERACTION**

Correct: C

Feedback for A and C: This is not the best answer. The best answer is C.

Feedback for D: Incorrect. The correct answer is C.
Summary

You have completed the lesson on security.

Remember:
- Security of electronic PHI includes confidentiality, integrity, and availability of the PHI.
- Entities covered under HIPAA are responsible for protecting the security of PHI against possible threats.
- To ensure the security of PHI, covered entities must put different types of safeguards in place.
Welcome to the lesson on employer identifiers.

After completing this lesson, you should be able to:

- Identify the unique employer identifier used under HIPAA
### Rationale

Employers may need to be identified when they:
- Send information to a health plan to enroll or disenroll an employee
- Send health plan payments relating to an employee

For these reasons, HIPAA sets a standard for identifying employers.
Unique Employer Identifier: EIN

In all electronic health transactions, employers must use their employer identification number (EIN), issued by the IRS, as their unique employer identifier.

Healthcare providers must obtain and use a National Provider Identifier (NPI). The NPI is:
- A 10 digit number
- Issued by the National Provider System
- Used for HIPAA standardized transactions
Summary

You have completed the lesson on identifiers.

Remember:
- Employers may need to be identified by health plans.
- An employer’s unique ID under HIPAA is the EIN.
Lesson 6: Privacy

6001

Introduction & Objectives

Welcome to the lesson on privacy.

After completing this lesson, you should be able to:

- List uses and disclosures of PHI allowed under the HIPAA Privacy Rule
- Recognize what must be included in written permission for uses and disclosures
- Define “minimum necessary” use or disclosure
- List individual patient rights under HIPAA
HIPAA Privacy Rule

The Privacy Rule is perhaps the most well known part of HIPAA.

The HIPAA Privacy Rule sets the first national standards for protecting the confidentiality of PHI.

The goal of the Privacy Rule is to balance two important aspects of healthcare:

- Protecting the privacy of patients
- Allowing flow of health information when needed to 1) ensure high quality healthcare and 2) protect public health
### Allowed & Required Disclosures

<table>
<thead>
<tr>
<th>Under HIPAA, a covered entity <strong>must</strong> disclose PHI in only two cases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• When the patient requests access to his or her PHI</td>
</tr>
<tr>
<td>• When the Department of Health and Human Services (DHHS[glossary]) is doing an investigation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A covered entity <strong>may</strong> use or disclose PHI only in two cases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• When the patient authorizes the use or disclosure in writing</td>
</tr>
<tr>
<td>• When the use or disclosure is allowed by the Privacy Rule</td>
</tr>
</tbody>
</table>

Let’s start by looking at uses or disclosures allowed by the Privacy Rule.
The Privacy Rule allows disclosure of PHI to the patient.
Allowed Disclosures: Treatment, Payment, Healthcare Operations

The Privacy Rule allows use / disclosure of PHI by a covered entity for:
- Its own treatment activities
- Its own payment activities
- Its own healthcare operations activities

Click on each to learn more.

**CLICK TO REVEAL**

**Treatment activities**
PHI may be used / disclosed among providers when two or more providers:
- Provide healthcare services for a patient
- Coordinate healthcare services for a patient
- Manage healthcare services for a patient

Examples are:
- Consultation between providers
- Referral from one provider to another

**Payment activities**
PHI may be used / disclosed by a health plan to:
- Obtain premiums
- Determine responsibility for coverage / benefits
- Fulfill responsibilities for coverage / benefits
- Give or receive payment for healthcare provided to a patient

PHI may be used / disclosed by a provider to:
- Obtain payment for providing care to a patient
- Obtain reimbursement for providing care

**Healthcare operations activities**
PHI may be used / disclosed when an organization is:
- Doing quality assessment and improvement
- Evaluating provider competency
- Conducting or arranging for medical services, audits, or legal services
- Performing certain insurance functions
- Planning, developing, managing, or administering business activities
Allowed Disclosures: Opportunity to Agree or Object

The Privacy Rule allows use / disclosure of PHI when:

- The patient gives informal permission.
- The patient is given a clear chance to either agree or object to the disclosure.

If the patient is not available or able to agree or object, this sort of use / disclosure is still allowed if the covered entity believes the use / disclosure is in the best interest of the patient.

Examples of this type of disclosure are:

- Listing a patient’s contact information in a facility directory
- Dispensing a filled prescription to a patient’s husband or wife
- Informing a patient’s family of the patient’s condition
Allowed Disclosures: Incidental

Sometimes, PHI is used or disclosed as a result of a separate, allowed use / disclosure.

This type of “incidental” use / disclosure is allowed, as long as the organization has safeguards to keep it to a minimum.
### Allowed Disclosures: Public Interest & Benefit

The Privacy Rule allows use / disclosure of PHI, without the patient’s permission, for 12 purposes in the public interest.

These purposes fall into the following categories:

- **Required by law**
- **Public health activities**
- **Victims of abuse, neglect, or domestic violence**
- **Health oversight**
- **Judicial and administrative proceedings**
- **Law enforcement**
- **Decedents**
- **Organ donation**
- **Research**
- **Serious threat**
- **Essential government functions**
- **Workers’ compensation**

Click on each purpose to learn more.
When there is a medical emergency, and a healthcare provider must disclose PHI to inform the law about a crime, the location of the crime or victims, or the criminal, it is considered a serious threat.

**Decedents**
The Privacy Rule allows covered entities to disclose PHI to funeral directors as needed. PHI also may be disclosed to coroners or medical examiners to:
- Identify a body
- Determine cause of death
- Perform other functions allowed by law

**Organ donation**
The Privacy Rule allows covered entities to use/disclose PHI to facilitate donation and transplantation of a dead body’s:
- Organs
- Eyes
- Tissues

**Research**
Research means a systematic study that will add to general knowledge. The Privacy Rule allows covered entities to use/disclose PHI for research, without the patient’s permission, if certain conditions are met.

**Serious threat**
The Privacy Rule allows covered entities to use/disclose PHI if there is a serious and immediate threat. The disclosure must be made to someone who can lessen the threat, for example, the police.

**Essential government functions**
The Privacy Rule allows covered entities to use/disclose PHI if the PHI is necessary to assist certain government functions, such as:
- Military operations
- Intelligence and national security activities allowed by law
- Protecting the President
- Protecting the health and safety of prison inmates or employees
- Determining eligibility for government benefit programs

**Workers’ compensation**
The Privacy Rule allows covered entities to disclose PHI in compliance with workers’ compensation laws.
Allowed Disclosures: Limited Data Set

A “limited data set” means PHI with its patient identifiers removed.

The Privacy Rule allows covered entities to use / disclose limited data sets for certain purposes, if safeguards are put in place to protect the PHI remaining in the data.

The allowed purposes are:
- Research
- Healthcare operations
- Public health activities
Drag and drop situations from the word bank to identify each situation as an allowed or disallowed use or disclosure of PHI.

### Use / Disclosure of PHI Allowed under the Privacy Rule

- Providers share a patient’s PHI when consulting about the case.
- A provider notifies a patient’s parents that the patient is HIV-positive. This notification is not required by law.
- A pharmacist dispenses a filled prescription to the patient’s daughter.

### Use / Disclosure of PHI Not Allowed under the Privacy Rule

- Providers gossip about a patient’s prognosis in the hospital cafeteria.
- A provider notifies a patient’s sexual partner that the patient is HIV-positive. This notification is required by law.
- A patient objects to having his contact information listed in a facility directory. The information is listed anyway.
Authorization

For any use or disclosure of PHI not allowed by the Privacy Rule, the covered entity must get written permission from the patient.

Written permission must:
- Be in plain language
- Specify which information will be used or disclosed
- Specify who will be disclosing and receiving the information.
- Give an expiration date for the permission
- Give information about the patient’s right to revoke the permission in writing
Minimum Necessary

In all uses / disclosures of PHI under the Privacy Rule, covered entities must use / disclose the *minimum amount of PHI necessary* to achieve the purpose of the use / disclosure.

For example, only the patient’s most recent lab results should be disclosed, if this will achieve what is needed.

The entire medical record should never be used or disclosed, unless the covered entity can clearly show that the entire medical record is needed to achieve the purpose of the use / disclosure.
Covered entities must inform patients of their privacy practices.

The notice of privacy practices must contain information about:

- How the organization may use and disclose PHI
- The organization’s duty to protect patient privacy
- How the organization protects and does not protect privacy
- The patient’s right to complain about a possible violation of privacy rights, including contact information for making complaints
Patients have a right to review and obtain a copy of their PHI.

Exceptions to the right of access are:
- Psychotherapy notes
- Information put together for legal proceedings
- Certain lab results
- Certain research information
<table>
<thead>
<tr>
<th>Individual Rights: Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under the HIPAA Privacy Rule, patients have the right to ask to have their PHI amended when PHI is inaccurate or incomplete.</td>
</tr>
<tr>
<td>If a covered entity agrees to amend PHI, the entity must provide the amendment to anyone who needs it for the wellbeing of the patient.</td>
</tr>
<tr>
<td>If the covered entity refuses to amend, it must:</td>
</tr>
<tr>
<td>- Provide a written denial to the patient.</td>
</tr>
<tr>
<td>- Allow the patient to write a statement of disagreement to be included in the medical record.</td>
</tr>
</tbody>
</table>
Individual Rights: Disclosure Accounting

The Privacy Rule gives patients the right to find out how their PHI has been disclosed.

Patients will be able to ask to see disclosures made from an electronic health record over the past three years. This includes those made for:

- Treatment
- Payment
- Healthcare operations

*Individual Rights: Disclosure Accounting*
Individual Rights: Restriction Request

Patients have the right to request that covered entities restrict:

- Use or disclosure of PHI for treatment or healthcare operation reasons
- Disclosure of PHI to persons involved in the patient’s healthcare
- Disclosure of the patient’s condition, location, or death to family members

Covered entities do not have to agree to these requests.
Individual Rights: Confidential Communication

Covered entities must agree to some patient requests.

Consider this case:

Amanda is treated for depression. She wants to keep her treatment private. She does not want her health insurer to know about her treatment.

Can Amanda restrict disclosure to her health insurer?

Yes, if she:
- Asks that this information be kept private
- Pays for the treatment 100% “out-of-pocket”

The healthcare provider cannot disclose information in this situation. They can grant or deny the request if she does not pay 100% of the costs.
Individual Rights: Confidential Communication

Under the Privacy Rule, patients have the right to request that they receive PHI in an atypical way.

For example, patients may request that PHI be delivered to a P.O. box, rather than a home address.

Health plans must accept reasonable requests if patients specify that disclosure of PHI could endanger them. Health plans are not allowed to question the danger to the patient.
### Administrative Requirements

The HIPAA Privacy Rule requires that covered entities have:

- **Privacy policies and procedures**
- **Privacy personnel**
- **Workforce training and management**
- **Mitigation**
- **Data safeguards**
- **Complaint procedures**
- **Retaliation and waiver policies**
- **Documentation and record retention**

Click on each to learn more.

#### CLICK TO REVEAL

**Privacy policies and procedures**
Covered entities must put in place privacy policies and procedures that follow the Privacy Rule.

**Privacy personnel**
Covered entities must have:
- A privacy official who puts in place the organization’s privacy policies and procedures
- A contact person or office responsible for receiving complaints and providing information about the organization’s privacy practices

**Workforce training and management**
Covered entities must train their workforce on privacy policies and procedures. They also must punish workers who violate their privacy policies.

**Mitigation**
If a disclosure of PHI that violates the Privacy Rule is discovered, the covered entity must take steps to lessen the harm caused by this disclosure.

**Data safeguards**
Covered entities must put into place administrative, physical, and technical safeguards against the use or disclosure of PHI in violation of the Privacy Rule.

**Complaint procedures**
Covered entities must have procedures for patients to complain about possible non-compliance with the Privacy Rule.

**Non-retaliation and non-waiver policies**
Covered entities must not retaliate against any person who:
- Exercises rights under the Privacy Rule
- Helps an investigation by DHHS or other appropriate agencies
- Disagrees with doing something that the person thinks is a violation of the Privacy Rule

Covered entities also may not require anyone to waive rights under the Privacy Rule in exchange for:
- Treatment
- Payment
- Enrollment / benefits eligibility

**Documentation and records**
All records of practices, etc. under the Privacy Rule must be kept for at least six years.
In general, the HIPAA Privacy Rule overrules any state law that is inconsistent with the Rule.
Penalties

We talked about the penalties of violating the Privacy Rule in lesson 2.

Now that you know more about the Rule, let’s review:

- **Civil penalties**
- **Criminal penalties**

Click on each to review.

In general, penalties for violating HIPAA are **civil penalties**. Civil monetary penalties include:

- $100-$50,000 for unknowingly violating HIPAA
- $1000-$50,000 for knowingly violating HIPAA
- $10,000-$50,000 for willful neglect, if the violation is corrected
- At least $50,000 for violations resulting from willful neglect if they are not corrected

**Criminal penalties**

- Up to $50,000 fine and up to one year in jail for knowingly obtaining or disclosing PHI in violation of HIPAA
- Up to $100,000 fine and up to five years in jail for doing the above under false pretenses
- Up to $250,000 fine and up to ten years in jail for doing the above with the intent to profit by, or do harm with, the information
Covered entities **must** comply with a patient’s request to:
   a. Amend PHI
   b. Review and obtain a copy of PHI
   c. Restrict disclosure of PHI to providers involved in the patient’s care
   d. All of the above

**MULTIPLE CHOICE INTERACTION**

Correct: B

Feedback for A, C, D: Incorrect. The correct answer is B.

Feedback for B: Correct.
Summary

You have completed the lesson on privacy.

Remember:
- The HIPAA Privacy Rule allows certain uses and disclosures of PHI.
- All other uses and disclosures require written permission from the patient.
- Use and disclosure of PHI should always follow the “minimum necessary” rule.
- Patients have the right to access and request amendment of their PHI.
- Patients can restrict disclosure to health insurers if they pay for the treatment out-of-pocket.
- Patients have other individual rights under HIPAA, as well.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>code set</td>
<td>combinations of numbers and/or letters that identify items in a group</td>
</tr>
<tr>
<td>covered entity</td>
<td>an organization that must comply with HIPAA</td>
</tr>
<tr>
<td>transaction</td>
<td>an action or set of actions between two or more persons related to doing business</td>
</tr>
<tr>
<td>DHHS</td>
<td>Department of Health and Human Services (HHS); the federal government's principal agency for protecting the health of all Americans and providing essential human services</td>
</tr>
<tr>
<td>integrity</td>
<td>a state of information in which the information has not been changed during storage or transmission</td>
</tr>
<tr>
<td>disclosure</td>
<td>the act of revealing or giving out information</td>
</tr>
<tr>
<td>vendor</td>
<td>supplier of goods or services</td>
</tr>
<tr>
<td>amend</td>
<td>to alter an existing document</td>
</tr>
<tr>
<td>encryption</td>
<td>scrambling of computer data so that it cannot be used by unwanted parties</td>
</tr>
<tr>
<td>decryption</td>
<td>the process of unscrambling encrypted or encoded data</td>
</tr>
<tr>
<td>civil</td>
<td>a type of legal case in which money damages can be awarded</td>
</tr>
<tr>
<td>false pretenses</td>
<td>intentionally untrue statement(s) meant to mislead</td>
</tr>
</tbody>
</table>
Pre-Test

1. Which organization is a covered entity under HIPAA?
   
   a. An organization without access to PHI  
   b. An organization that sends and receives PHI electronically  
   c. An organization without business activities that involve PHI  
   d. An organization that does not send or receive PHI electronically  

   Correct: B  
   Rationale: An organization must follow HIPPA if the organization's business activities involve sending and/or receiving PHI electronically.

2. What is the civil penalty for unknowingly violating HIPAA?
   
   a. $1,000 - $50,000  
   b. $100 - $50,000  
   c. At least $50,000  
   d. $10,000 - $50,000  

   Correct: B  
   Rationale: The civil penalty for unknowingly violating HIPAA is $100 - $50,000.

3. A provider asks a health plan for payment. What type of transaction is this?
   
   a. Healthcare claim  
   b. Coordination of benefits  
   c. Eligibility for health plan  
   d. Healthcare payment and remittance advice  

   Correct: A  
   Feedback: When a provider asks a health plan for payment, this is a healthcare claim transaction.
4. Claims are sent to a health plan, to determine how much of the cost the plan will pay. What type of transaction is this?
   a. Coordination of benefits
   b. Health plan premium payment
   c. Enrollment and disenrollment in a health plan
   d. Healthcare claim or equivalent encounter information

Correct: A
Feedback: When claims are sent to a health plan, to determine how much of the cost the plan will pay, this is a coordination of benefits transaction.

5. An injury is being coded on an electronic transaction. What code set should be used?
   a. NDC
   b. CPT-4
   c. HCPCS
   d. ICD-9-CM

Correct: D
Rationale: The ICD-9-CM is the source of HIPAA standard code sets for injuries.

6. A drug is being coded on an electronic transaction. What code set should be used?
   a. NDC
   b. CPT-4
   c. HCPCS
   d. ICD-9-CM

Correct: A
Rationale: The NDC (National Drug Codes) is the source of HIPAA standard code sets for drugs and biologics.
7. Which of the following is an administrative safeguard for PHI?
   a. Encrypting electronic PHI prior to transmission
   b. Punishing staff members who do not follow security rules
   c. Disposing of non-active electronic PHI in a secure manner
   d. Analyzing activity within systems that contain electronic PHI

Correct: B
Rationale: An administrative safeguard for PHI, required under HIPAA, is employee sanction: punishing staff members who do not follow security rules.

8. Which of the following is a physical safeguard for PHI?
   a. Encrypting electronic PHI prior to transmission
   b. Punishing staff members who do not follow security rules
   c. Disposing of non-active electronic PHI in a secure manner
   d. Analyzing activity within systems that contain electronic PHI

Correct: C
Rationale: A physical safeguard for PHI, required under HIPAA, is disposing of electronic PHI in a secure manner.

9. Which use/disclosure of PHI is allowed under the HIPAA Privacy Rule?
   a. Releasing information about a celebrity patient to the media
   b. Requesting unnecessary information about a patient out of curiosity
   c. Discussing a patient's case with a provider involved in the patient's care
   d. Chatting about a patient with a provider not involved in the patient's care

Correct: C
Rationale: PHI should be disclosed only to those with a need to know, such as providers involved in the patient's care.
10. Under the HIPAA Privacy Rule, which use/disclosure of PHI is acceptable?
   a. Providers gossip about a patient in a public area.
   b. A limited dataset is released for research purposes.
   c. A patient tells her providers that her children should not be informed of her condition. Her children are informed anyway.
   d. A patient specifies that a filled prescription should not be released to his wife. The pharmacy dispenses the prescription to his wife anyway.

Correct: B
Rationale: A limited dataset consists of PHI with patient identifiers removed. Limited datasets may be released for purposes of research, healthcare operations, or public health activities.
Post-Test

1. Which statement is true of an organization that sends and/or receives PHI electronically?
   a. The organization is a covered entity under HIPAA.
   b. The organization is exempt from HIPAA requirements.
   c. The organization may choose whether or not to follow HIPAA.
   d. The organization is required to follow only the HIPAA Privacy Rule.

Correct: A
Rationale: An organization must follow HIPAA if the organization's business activities involve sending and/or receiving PHI electronically.

2. What is the civil penalty for a violation of HIPAA resulting from willful neglect, when the violation is not corrected?
   a. $1,000 - $50,000
   b. $100 - $50,000
   c. At least $50,000
   d. $10,000 - $50,000

Correct: C
Rationale: The civil penalty for violating HIPAA through willful neglect, when the violation is not corrected, is at least $50,000.

3. A health plan sends a provider an explanation of benefits (EOB). What type of transaction is this?
   a. Healthcare claim status
   b. Eligibility for a health plan
   c. Referral certification and authorization
   d. Healthcare payment and remittance advice

Correct: D
Rationale: When a health plan sends a payment or EOB, this is a healthcare payment and remittance advice transaction.
4. Information is sent to a health plan to start a patient's coverage. What type of transaction is this?
   a. Healthcare claim
   b. Coordination of benefits
   c. Health plan premium payment
   d. Enrollment and disenrollment in a health plan

Correct: D
Rationale: When information is sent to a health plan to start or end a patient's healthcare coverage, this is an enrollment and disenrollment in a health plan transaction.

5. The cause of a health problem is being coded on an electronic transaction. Which code set should be used?
   a. NDC
   b. CPT-4
   c. HCPCS
   d. ICD-9-CM

Correct: D
Rationale: ICD-9-CM code sets are used to code causes of health problems.

6. A prosthetic device is being coded on an electronic transaction. Which code set should be used?
   a. NDC
   b. CPT-4
   c. HCPCS
   d. ICD-9-CM

Correct: C
Rationale: HCPCS code sets are used to code medical items such as medical supplies, orthotic and prosthetic devices, and durable medical equipment.
7. Which of the following is an administrative safeguard for PHI?
   a. Removing electronic PHI from media before media reuse
   b. Ensuring that PHI sent electronically is not changed improperly
   c. Controlling physical access to workstations with access to electronic PHI
   d. Authorizing and/or supervising employees who work with electronic PHI

Correct: D
Rationale: An administrative safeguard for PHI, required under HIPAA, is authorization and/or supervision of employees with access to PHI.

8. Which of the following is a technical safeguard for PHI?
   a. Removing electronic PHI from media before media reuse
   b. Ensuring that PHI sent electronically is not changed improperly
   c. Controlling physical access to workstations with access to electronic PHI
   d. Authorizing and/or supervising employees who work with electronic PHI

Correct: B
Rationale: A technical safeguard for PHI required under HIPAA is integrity control: measures for ensuring that 1) PHI sent electronically is not changed improperly and 2) any improper changes will be detected.

9. Which disclosure/use of PHI is allowed under the HIPAA Privacy Rule?
   a. Releasing a patient's PHI to the patient, when he or she requests access
   b. Releasing a patient's PHI to the media, when the media requests access
   c. Releasing a patient's PHI to the patient's best friend, when the friend requests access
   a. Releasing a patient's PHI to the patient's co-workers, when the co-workers request access

Correct: A
Rationale: PHI must be released to a patient when he or she requests access. Friends, co-workers, and the media should not be given access to PHI, unless the patient provides clear, written permission.
10. Under the HIPAA Privacy Rule, which of the following is an acceptable use/disclosure of PHI?
   a. Releasing PHI not needed to coordinate care
   b. Releasing the minimum amount of PHI needed
   c. Releasing the patient's full medical record, when only a recent X-ray film is needed
   d. Releasing the patient's full medical record, when only the patient's most recent lab results are needed

Correct: B
Rationale: In all uses/disclosures of PHI under the Privacy Rule, covered entities must use/disclose the minimum amount of PHI necessary to achieve the purpose of the use/disclosure.