


**MERCER** Building. Sustaining. Inspiring.

MONITOR | MEMBER | ROLL  
CLY COMPETER | CUNELVYVIA



## HIPAA Privacy & Security Training Part I

Wade Symons, Amy Pavlu  
CPEEHCC Training Conference  
Las Vegas

Services provided by Mercer Health & Benefits LLC

---

---

---

---

---

---

---

---

---

---

### Training modules

- Module 1: Introduction to HIPAA and the HIPAA Privacy Rule
- Module 2: Protected Health Information
- Module 3: Use and disclosure of PHI and authorization procedures
- Module 4: Individual privacy rights
- Module 5: HIPAA Security Rule

Mercer 1

---

---

---

---

---

---

---

---

---

---

### Why is this training important?

- Do you want your personal health information to get into the hands of unauthorized individuals?
- Is there anything you handle as part of your job today that you might consider to be someone else's personal health information?
- What do you know about the Health Insurance Portability and Accountability Act of 1996?
- *HIPAA training is required by law for anyone who handles protected health information.*

Mercer 2

---

---

---

---

---

---

---

---

---

---

**Module 1**  
Introduction to HIPAA and the  
HIPAA Privacy Rule

---

---

---

---

---

---

---

---

Module 1 – Intro to HIPAA

**HIPAA background**  
HIPAA administrative simplification

```

graph TD
    HIPAA[Health Insurance Portability and Accountability Act (HIPAA)]
    HIPAA --- TitleI[Title I  
Health Care Portability]
    HIPAA --- TitleII[Title II  
Administrative Simplification]
    HIPAA --- TitlesIII[Titles III, IV, V]
    TitleII --- Privacy[Privacy Standards  
April 14, 2003*]
    TitleII --- EDI[Electronic Data Interchange  
(EDI) Standards  
October 16, 2003]
    TitleII --- Security[Security Standards  
April 20, 2005*]
  
```

\*The effective date for small plans (i.e., those with less than \$5M in receipts) is April 14, 2004 (privacy rules) and April 20, 2006 (security rules)

Mercer 4

---

---

---

---

---

---

---

---

Module 1 – Intro to HIPAA

**Health Insurance Portability and Accountability Act (HIPAA) of 1996**

- **Title I – Portability** – Helps maintain coverage for employees who switch employers by prohibit discrimination in eligibility, premium and contributions, allow employees to enroll when they lose other coverage or gain dependents, and limit application of pre-existing condition limitations through use of certifications of prior coverage.
- **Title II – Accountability** – Consists of 3 parts:
  - **Privacy** – Rules that safeguard the privacy of “protected health information” (PHI) by placing limits on the use and disclosure of individually identifiable health information
  - **EDI** – Rules that standardize transactions/code sets for electronic data interchange (EDI) to encourage electronic commerce in health care
  - **Security** – Rules that maintain the confidentiality and integrity of electronic protected health information (e-PHI), prevent unauthorized use of data, and guard against physical hazards

Mercer 5

---

---

---

---

---

---

---

---

**The Privacy Rule – what it is and who is covered**

- Protects certain individually identifiable health information, e.g., “protected health information” – referred to as “PHI”
- Establishes a uniform minimum standard for protection of privacy across the states
- Imposes new administrative, contractual, and operational requirements on “Covered Entities” and “Business Associates” (more on this later)
- Gives individuals privacy rights
- It holds violators accountable with civil and criminal penalties

---

---

---

---

---

---

---

---

---

---

**The Privacy Rule – what it is and who is covered**

- The Privacy Rule applies to:
  - Health plans, including employer-sponsored health plans
  - Health care providers: doctors, hospitals, etc.
  - Organizations (called Business Associates) who provide services to or on behalf of health plans or providers
- Health Plan = Plan that provides or pays for health care
  - All insured and self-funded employer plans
  - HMOs, insurers, etc.
- Types of benefit plans covered by HIPAA privacy rules include:
  - Medical
  - Prescription drug
  - Dental
  - Vision
  - Long-term care
  - Healthcare FSA
  - Employee assistance plan

---

---

---

---

---

---

---

---

---

---

**Benefit plans NOT covered by the Privacy Rule**

- Life and AD&D insurance
- Workers' compensation and OSHA activities
- Short-term disability and long-term disability
- Return to work activities
- ADA reasonable accommodations
- FMLA leave
- Health-related absences
- Leaves of absence
- Retirement plans

---

---

---

---

---

---

---

---

---

---

### How employers/plan sponsors fit in

While employers are not directly regulated by HIPAA, the group health plans employer's sponsor ARE

- For the self-funded (non-insured) plans, the employer generally is responsible for ensuring that they comply with HIPAA rules
- For any insured plans, insurers are responsible for HIPAA compliance
- The employer will also be responsible for employees who handle PHI in the administration of insured or self-funded health plans

---

---

---

---

---

---

---

---

---

---

### The privacy infrastructure

To comply with HIPAA, employers must

- Designate a privacy officer
- Develop and maintain privacy policies and procedures
- Create/update plan documents, business associate contracts, forms, including privacy notices
- Provide initial and ongoing privacy training for employees who handle protected health information
- Provide a complaint resolution process
- Develop sanctions for employees and partners who violate privacy policies
- Properly retain, handle, transmit, store and dispose of PHI
- Retain documentation demonstrating compliance

---

---

---

---

---

---

---

---

---

---

### The penalties for non-compliance

#### Civil Penalties

- \$100 per violation, up to \$25,000 per year
- Monitored by Department of Health and Human Services Office for Civil Rights (OCR)

#### Criminal Penalties

- Fines up to \$250,000
- Imprisonment up to 10 years
- Enforced by the Department of Justice

---

---

---

---

---

---

---

---

---

---

## Module 2 Protected Health Information (PHI)

---

---

---

---

---

---

---

---

Module 2 – PHI

### Protected Health Information (PHI)

Protected Health Information (PHI) is at the center of HIPAA privacy rules. The rules closely regulate how PHI is used, disclosed, transmitted, and retained.

Mercer 13

---

---

---

---

---

---

---

---

Module 2 – PHI

### What is Protected Health Information (PHI)?

*Individually identifiable health information that*

- Clearly identifies an individual (or has components that reasonably could be used to identify the individual), **and**
- Is related to a past, present, or future physical or mental health condition, treatment of that condition, or payment of medical benefits, **and**
- Is created or received in any medium (verbal, written or electronic) by a plan or health care provider

Examples of documents that frequently contain PHI include:

- Individual claim and appeal records
- Large claim reports
- Detailed claims listings
- Explanations of benefits (EOBs)

Mercer 14

---

---

---

---

---

---

---

---

Individually “identifiable” health information

Any combination of data that could identify the individual who is the subject of the information, such as:

- Name
- Social Security number
- Specific dates
- Telephone/fax number
- E-mail address
- Medical record numbers
- Health plan beneficiary number
- Geographic identifiers smaller than a state
- Account numbers
- Certificate/license numbers
- Vehicle identifiers
- URLs
- IP address numbers
- Biometric identifiers
- Photographic image
- Other unique identifying numbers or codes (such as employer’s health plan ID)

---

---

---

---

---

---

---

---

---

---

---

---

When you encounter PHI

PHI can be a single record related to one person’s claim or information in a report that lists several individuals or an entire plan’s enrollment if the data is individually identifiable

- You may encounter PHI during:
  - Customer service assistance for employees with benefit plan issues
  - Claims and appeals
  - Health plan oversight
  - Medicare secondary payer administration
  - Response to internal and external parties requesting information

---

---

---

---

---

---

---

---

---

---

---

---

What is not considered PHI?

- Health information in employment records related to, for example:
  - Disability
  - Reasonable accommodations for ADA
  - Worker’s compensation
  - OSHA, ADA, FMLA
  - Other leaves of absence

The Privacy Rules do not apply to this type of medical information; because it’s not related to the health plan, it’s not considered PHI, and, therefore, not protected under HIPAA

---

---

---

---

---

---

---

---

---

---

---

---

Module 2 – PHI

**Module 2 quiz**  
Question 1

Health information is not PHI unless it contains an individual's name.

- True
- False

Mercer 18

---

---

---

---

---

---

---

---

Module 2 – PHI

**Module 2 quiz**  
Question 1

**False** is the correct answer. Health information can be PHI if it has components that reasonably could be used to identify the individual, such as a social security number or an address.

Mercer 19

---

---

---

---

---

---

---

---

Module 2 – PHI

**Module 2 quiz**  
Question 2

You are likely to encounter PHI in:

- A. Medical plan claims data
- B. Worker's compensation reports
- C. Employment records related to FMLA

Mercer 20

---

---

---

---

---

---

---

---

**Module 2 quiz**  
Question 2

A is the correct answer. PHI is information that identifies an individual, is related to treatment or payment for a medical condition, and is created or received in any medium (verbal, written or electronic).

Because Worker's compensation reports or employment records related to FMLA are not related to the health plan, neither is considered PHI, and, therefore, not protected under HIPAA

---

---

---

---

---

---

---

---



**Module 3**  
Use and disclosure of PHI & authorization procedures

---

---

---

---

---

---

---

---

**Use and disclosure of PHI**

- The HIPAA Privacy Rule regulates when covered entities can use and disclose PHI; this section discusses when:
  - The company can use or disclose PHI without authorization
  - The company must obtain an authorization from the affected participant before using or disclosing PHI

---

---

---

---

---

---

---

---

### Use and disclosure of PHI

#### Minimum necessary rule

- Individuals handling PHI may access or disclose the “minimum necessary” amount of information to accomplish the task at hand
- For example, the minimum necessary for claims payment:
  - Name of the covered employee
  - Name, address, age and gender of the patient
  - Nature of the claim
  - Coverage elected under the health plan
  - Condition for which coverage is requested
  - Name of provider

---

---

---

---

---

---

---

---

---

---

### When PHI can be used or disclosed without authorization

The plan may use and disclose PHI without participant authorization for:

- Plan administration
  - Including treatment and payment activities
- Plan operations
  - Including claims and appeal activities
- Health care data analysis and planning
- Other circumstances (for example, when required for law enforcement or public health activities)

... as long as the required HIPAA administrative infrastructure is in place

*For any other uses and disclosures, must obtain an authorization from the affected participant*

---

---

---

---

---

---

---

---

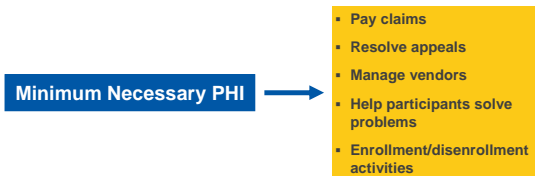
---

---

### Plan administration

#### Uses and disclosures of PHI

The HIPAA Privacy Rule allows a plan sponsor to use and disclose PHI for the following plan administration activities, **without requiring an authorization** from the affected plan participant.



---

---

---

---

---

---

---

---

---

---

**PHI disclosures requiring authorization**

- As discussed, the HIPAA Privacy Rule provides for the plan's discretion to disclose a participant's PHI to any individual without authorization if the disclosure is necessary for payment or health plan operations and administration

*But in all other situations, the participant must complete an authorization form in order for the plan to disclose PHI for employment or non-plan purposes*

- Any authorization must be verified to ensure the authorization:
  - Has not expired
  - Has not been revoked
  - Includes all required information
- Authorizations must be retained for at least six years

---

---

---

---

---

---

---

---

---

---

**Module 3 quiz**

Question 1

What is the "minimum necessary rule"?

- A. Employees are expected to use the minimum amount of time necessary to complete a task involving protected health information.
- B. Use or disclosure of PHI must be limited to the minimum necessary amount of PHI to accomplish a given task.
- C. Staff are no longer allowed to use or disclose health information under any circumstances.

---

---

---

---

---

---

---

---

---

---

**Module 3 quiz**

Question 1

B is the correct answer. HIPAA's minimum necessary rule states that any use or disclosure of PHI must be limited to the minimum necessary to accomplish the purpose of the use or disclosure.

---

---

---

---

---

---

---

---

---

---



**Module 4**  
Individual rights

---

---

---

---

---

---

---

---

Module 4 – Individual rights

**Individual privacy rights**

- The HIPAA Privacy Rule provides individuals certain rights regarding their PHI:
  - The right to receive a privacy notice that will detail how the plan can use his or her PHI without authorization and when an authorization is required
  - The right to access, inspect and copy his or her PHI and request an amendment of PHI
  - The right to request that the plan restrict the use of their PHI
  - The right to receive an accounting of non-routine disclosures of their PHI
  - The right to file complaints about privacy rule violations

Mercer 31

---

---

---

---

---

---

---

---

Module 4 – Individual rights

**Privacy notice**

- The plan must establish procedures for certain routine disclosures and requests that don't require authorization
- A privacy notice to participants documents those procedures:
  - For self-funded plans, the notice comes from the plan sponsor
  - For insured plans, the notice comes from each health insurer or HMO
  - The notice will be distributed upon plan enrollment and a reminder at least once every three years

Mercer 32

---

---

---

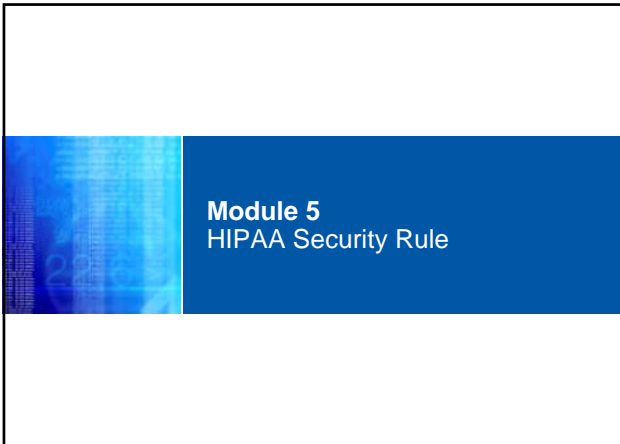
---

---

---

---

---




---

---

---

---

---

---

---

---

Module 5 – HIPAA Security Rule

**HIPAA Security Rule**

- The HIPAA Security Rule contains additional requirements specific to PHI in electronic form
- **Electronic PHI (e-PHI) is:**
  - Electronically created;
  - Electronically received;
  - “At rest” or maintained in a storage device such as a computer hard drive, disk, CD, or tape; or
  - “In transit” via the Internet, dial-up lines, etc.
    - For example, e-mail, FTP (file transfer protocol), EDI (electronic data interchange), IVR (interactive voice response), and fax-back systems used to transmit PHI

Mercer 34

---

---

---

---

---

---

---

---

Module 5 – HIPAA Security Rule

**HIPAA Security Rules**  
What is electronic PHI (e-PHI)?

**e-PHI is NOT...**

**e-PHI is not:**

- **De-identified information**
  - 18 specific identifiers are removed
- **Information that was not in electronic form before transmission**
  - Person-to-person phone calls
  - Copy machines
  - Paper-to-paper fax machines
  - Voicemail

Mercer 35

---

---

---

---

---

---

---

---

Examples of e-PHI common to group health plans:

Function	e-PHI
Customer Service & Claim Advocacy	E-mail, imaging system
Claim Audit	Receipt of vendor claim tape
Data Analysis	Review of vendor claim data
Claim Appeals	E-mail, imaging system
Incoming e-PHI from Vendors	E-mail, receipt of eligibility or enrollment from vendors
Outgoing e-PHI to Vendors	E-mail, sending eligibility or enrollment to vendors

---

---

---

---

---

---

---

---

---

---

What are the objectives of the HIPAA Security Rule?

- Secure e-PHI “at rest,” while in the custody of group health plans
- Secure e-PHI “in transit,” both between health plans and from a health plan to a third party
- Protect against reasonably anticipated:
  - Threats or hazards to e-PHI security or integrity
  - Unauthorized uses or disclosures

---

---

---

---

---

---

---

---

---

---

What employer plan sponsors must do  
Security infrastructure requirements

**HIPAA Security Infrastructure**

Plans are required to:

- Appoint a Security Official
- Conduct a security risk assessment
- Develop written policies and procedures
- Train staff and impose sanctions on violators
- Require contractual compliance by Business Associates

---

---

---

---

---

---

---

---

---

---

Module 5 quiz

Question 1

Which of the following is not e-PHI?

- A. Claims data sent via e-mail
- B. A letter to a TPA saved to the network in Microsoft Word format regarding an employee claims dispute
- C. A fax received from a doctor regarding an employee's health condition

---

---

---

---

---

---

---

---

Module 5 quiz

Question 1

The correct answer is C.

- **Explanation:** Paper to paper faxes are not e-PHI because e-PHI is limited to information that was in electronic form prior to transmission. However, a fax can be PHI and must be protected under the Privacy Rule. But is not subject to the extra protections of the Security Rule.

---

---

---

---

---

---

---

---

Module 5 quiz

Question 2

What should I do if I receive an e-mail from an unknown sender?

- A. Open the e-mail and any attachments so virus protection software can quarantine any viruses
- B. Delete the e-mail and report the incident to the help desk
- C. Open the e-mail immediately – some of the funniest jokes are sent by unknown senders!

---

---

---

---

---

---

---

---

**Module 5 quiz**  
Question 2

- The correct answer is **B**.
  
- **Explanation:** You should not open e-mails or e-mail attachments that are from suspicious or unknown sources or have suspicious subjects. You must report suspicious e-mail and other potential security incidents to the Help Desk. Also make sure to comply with instructions to ensure your workstation virus protection software is kept up to date.

---

---

---

---

---

---

---

---

Questions?



---

---

---

---

---

---

---

---

**MERCER**



---

---

---

---

---

---

---

---