



# North American Learning Institute

## HIPAA Course Outline

1. HIPAA?
  - a. What is it?
  - b. The privacy rule
  - c. The security rule
  - d. HIPAA objectives
    - i. Insurance portability
    - ii. Fraud prevention
      1. Identity theft
    - iii. Efficiency
    - iv. Protect personal info
    - v. Gather illness data
  - e. Patient information
    - i. Individually identifiable information
    - ii. Patient rights
  - f. HITECH Act
    - i. What is it?
    - ii. Enforcement
    - iii. Investigations
    - iv. Fines
    - v. Patient notification
    - vi. Electronic Health Records (EHRs)
    - vii. Vendors
  - g. The HIPAA Final Rule
    - i. What is it? (aka Omnibus Rule)
    - ii. Notice of privacy practices
    - iii. Breach notification rules
    - iv. Expanded patient rights
    - v. Electronic Health Records (EHRs)
    - vi. Subcontractors
    - vii. Penalties

viii. Investigations

2. HIPAA terms/definitions

- a. Authorization
- b. Business associate
- c. Clearinghouses
- d. Covered entity
- e. Disclose
- f. EHR
- g. Legal representative
- h. Medical providers
- i. Minimum necessary rule
- j. Health plans
- k. HIPAA
- l. HITECH
- m. Notice of privacy practices (NPP)
- n. Protected health information (PHI)
  - i. Electronic PHI (ePHI)
- o. Treatment, payment, healthcare operations (TPO)

3. Privacy rule

- a. What is it?
- b. PHI
  - i. What is it?
  - ii. Protecting patients
  - iii. Exceptions
    - 1. Routine uses
    - 2. Authorization
- c. Covered entities
  - i. Examples
  - ii. Business associates

4. Security rule

- a. ePHI
  - i. Confidentiality
  - ii. Integrity
  - iii. Availability
  - iv. Reasonably anticipated threats
  - v. Safe computing
    - 1. Family and friends
    - 2. Passwords
      - a. Strong password
      - b. Don't share your password
      - c. Don't use others' passwords
    - 3. Locking your PC
    - 4. Screen saver
    - 5. Virus protection

6. Spyware protection
7. Encrypted email
8. Hacker awareness
9. ID verification

## 5. HIPAA compliance

- a. What is it?
- b. Requirements
  - i. Privacy policies and procedures
  - ii. HIPAA officer
  - iii. Training
    1. HIPAA
    2. Internal policies
  - iv. Data safeguards
  - v. Privacy complaints
  - vi. Protection from retaliation
  - vii. Documentation
- c. Violations
  - i. Types of violations
    1. Minor violation
      - a. What is it?
      - b. Fines
    2. Serious violation
      - a. What is it?
      - b. Fines
    3. Criminal violation
      - a. What is it?
      - b. Fines
      - c. Jail time
  - ii. Problem corrected?
  - iii. Accidental or intentional?
  - iv. Emergencies
    1. Local emergencies
      - a. Examples
      - b. Compliance exception
    2. National security emergencies
      - a. Examples
      - b. Compliance exception
    3. Natural disasters
      - a. Examples
      - b. Compliance exception
  - v. OCR
    1. Who are they?
    2. What do they do?

## 6. Patient rights

- a. Notice of Privacy Practices (NPP)
    - i. First visit
    - ii. Privacy policies
    - iii. Complaints
  - b. Copy of PHI
    - i. Right to see and obtain
    - ii. Timeframe
    - iii. Unavailable portions
    - iv. Nonpayment
    - v. Other provider info
    - vi. Allowable fees
  - c. PHI amendments
    - i. Making a request
    - ii. Refusal to update
      - 1. Basis for denial
      - 2. State of disagreement
      - 3. Complaint right
      - 4. Privacy officer info
  - d. Disclosure restrictions
    - i. Authorization
    - ii. Treatment exception
    - iii. Friends and family
    - iv. Health plan for out-of-pocket
    - v. Contact preferences
    - vi. Immunization records and schools
  - e. PHI by alternative means
  - f. Disclosure accounting
  - g. File Privacy complaints
  - h. Digital copy of PHI
  - i. Sale, marketing, and fundraising
    - i. Sale of PHI
    - ii. CE patient communication
    - iii. Fundraising opt out
7. My responsibility
- a. Protect PHI
    - i. Shred documents
    - ii. Keep patient information private
    - iii. Beware of potential criminals/hackers
    - iv. Don't browse friends'/family records
  - b. Follow company policies and procedures
  - c. Help prevent violations
    - i. Remember/reference training materials
    - ii. Report potential access by past employees
    - iii. Report suspicious co-worker behavior

## 8. HIPAA Officer

- a. What is the HIPAA officer?
- b. Responsibilities
  - i. Activities
  - ii. Compliance
- c. Contact person
- d. Who is your HIPAA Officer?

## 9. Company policies

- a. HIPAA requirement
- b. More than HIPAA
  - i. Clear and understandable
  - ii. State law requirements
  - iii. Other laws
  - iv. Third party requirements
  - v. Prioritized over HIPAA rules

## 10. Disclosures

- a. Choices
  - i. Authorization
  - ii. De-identify data
  - iii. Research
    - 1. Limited data set
    - 2. Data Use Agreement
  - iv. Do not disclose
- b. Treatment purposes
- c. Mandatory PHI Disclosures
  - i. Person's own PHI
    - 1. ID verification
    - 2. Reasonable fees
  - ii. Required by law
  - iii. Official request from Secretary of HHS
- d. Minimum necessary standard
  - i. What is it?
  - ii. Exceptions
    - 1. Treatment
    - 2. Individual PHI
    - 3. Individual PHI of minor children
    - 4. Valid authorization
    - 5. HHS investigations
    - 6. HHS reviews
    - 7. HIPAA enforcement
    - 8. Required by law
- e. Family and friends
  - i. What's permissible
  - ii. If patient present

- iii. If patient not present
- iv. If patient is incapacitated
- v. Documentation of patient's decision

11. Resources and references