NeuroTrace Academy Study Guide

Domain: Domain IV – Professional Practice, Ethics & Legal Issues
Section: HIPAA Compliance in EEG Practice
Style: Comprehensive, policy-driven, scenario-based, exam-oriented

---

1. Core Principles (Must Know)

HIPAA Protects Patient Privacy

- **HIPAA = Health Insurance Portability and Accountability Act (1996)**
- **Primary Purpose:** Protect patient health information (PHI)
- **Applies to:** All healthcare providers, facilities, health plans, and healthcare clearinghouses
- **Two Main Rules:**
    1. **Privacy Rule** (2003): Protects PHI and gives patients rights
    2. **Security Rule** (2005): Requires safeguards for electronic PHI (ePHI)
- **Violations have serious consequences:** Fines, legal action, job loss, professional discipline

Protected Health Information (PHI)

PHI includes ANY information that:

- Identifies or could identify a patient
- Relates to past, present, or future physical/mental health
- Relates to healthcare services provided
- Relates to payment for healthcare
- Is created, received, maintained, or transmitted by a covered entity

Key Point: PHI is not just medical records - it includes ANY information that could identify a patient in a healthcare context.

Key Principle

Patient information is confidential and must be protected at all times

- Confidentiality is a legal requirement (HIPAA)
- Confidentiality is an ethical requirement (professional standards)
- Violations can result in:
    - Civil penalties: $100 - $50,000 per violation (up to $1.5 million per year)
    - Criminal penalties: Up to $250,000 fine and 10 years imprisonment
    - Job termination
    - Loss of professional license
    - Lawsuits from patients

Practical Application

- Always protect patient information in all settings
- Share only with authorized personnel on a need-to-know basis
- Use secure methods for storage and transmission
- Follow facility policies and HIPAA regulations strictly
- When in doubt, choose the more protective option

---

2. The 18 HIPAA Identifiers (Complete List)

All 18 Identifiers Must Be Removed for De-identification

1. **Names** (patient, family members, employers, household members)
    - First name, last name, middle initial
    - Maiden name, alias, nickname
    - Any name that could identify the patient
2. **Geographic subdivisions smaller than state**
    - Street address
    - City
    - County
    - Precinct
    - Zip code (first 3 digits if population < 20,000)
    - Any geographic identifier smaller than state
3. **All elements of dates (except year)**
    - Date of birth
    - Date of admission
    - Date of discharge
    - Date of death
    - Date of service
    - Ages over 89 (must be aggregated to "90 or older")
    - Any date that could identify the patient
4. **Telephone numbers**
    - Home, work, mobile
    - Any phone number
5. **Fax numbers**
    - Any fax number
6. **Email addresses**
    - Personal or work email
    - Any email address
7. **Social Security numbers**
    - Full SSN
    - Last 4 digits (if unique enough to identify)
8. **Medical record numbers**
    - Hospital MRN
    - Clinic patient ID
    - Any unique medical identifier
9. **Health plan beneficiary numbers**
    - Insurance member ID
    - Policy numbers
    - Any health plan identifier
10. **Account numbers**

    - Bank account
    - Credit card
    - Any financial account number

11. **Certificate/license numbers**
    - Driver's license
    - Professional license
    - Any certificate or license number

12. **Vehicle identifiers and serial numbers**
    - License plate numbers
    - VIN numbers
    - Any vehicle identifier

13. **Device identifiers and serial numbers**
    - Medical device serial numbers
    - Equipment identifiers
    - Any device serial number

14. **Web Universal Resource Locators (URLs)**
    - Personal websites
    - Social media URLs
    - Any web address

15. **Internet Protocol (IP) addresses**
    - Computer IP addresses
    - Network identifiers
    - Any IP address

16. **Biometric identifiers**
    - Fingerprints
    - Voiceprints
    - Retinal scans
    - DNA
    - Any unique biometric identifier

17. **Full face photographic images**
    - Photos showing full face
    - Any image that could identify the patient

18. **Any other unique identifying number, characteristic, or code**
    - Any other identifier not listed above
    - Unique combinations of data
    - Any code that could identify the patient

Key Rules for De-identification

- **All 18 identifiers must be removed** - removing just the name is NOT sufficient
- **Must prevent re-identification** - even if all identifiers are removed, if the data can still identify the patient, it's not de-identified
- **Rare findings can be identifiers** - unique clinical findings, rare patterns, or unique combinations can allow re-identification
- **When in doubt, don't use it** - if you're unsure if data is de-identified, don't use it

Examples of Re-identification Risks

- **Rare EEG pattern:** "Only 2 patients in facility history had this pattern" = identifiable
- **Specific timing:** "EEG performed on 3/15/2023 at 2:30 PM" = identifiable (even without name)
- **Unique combinations:** "45-year-old male with rare syndrome X and pattern Y" = identifiable
- **Geographic + timing:** "Patient from City Z with rare finding on Date X" = identifiable

---

3. Minimum Necessary Rule

Core Principle

Share only the minimum patient information necessary to perform the specific task

- Not everyone needs all information
- Only share on a "need-to-know" basis
- Limit access to what is required for the specific purpose
- Do not share more than necessary

Examples by Role

Ordering Physician:

- Needs: Clinical indication, EEG findings, interpretation
- Does NOT need: Billing codes, insurance details, payment information

Billing Department:

- Needs: Procedure codes, dates of service, patient demographics (for billing)
- Does NOT need: Detailed clinical findings, EEG interpretations, medical history

Quality Assurance:

- Needs: De-identified data only (no PHI)
- Does NOT need: Patient names, MRNs, or any identifiers

Teaching/Education:

- Needs: Fully de-identified data only
- Does NOT need: Any patient identifiers or unique details

Other Technologists:

- Needs: Only if directly involved in patient care
- Does NOT need: Information about patients they're not caring for

Practical Scenarios

Scenario 1: Billing Request

- **Request:** Billing department asks for patient information
- **Appropriate:** Share procedure codes, dates, basic demographics
- **Inappropriate:** Share detailed clinical findings, EEG interpretations, medical history

Scenario 2: Teaching Conference

- **Request:** Use EEG tracing for teaching
- **Appropriate:** Fully de-identified tracing (all 18 identifiers removed)
- **Inappropriate:** Tracing with MRN, date, or any identifier

Scenario 3: Physician Consultation

- **Request:** Ordering physician asks about findings
- **Appropriate:** Share relevant clinical findings and observations
- **Inappropriate:** Share information about other patients or unrelated details

Key Principle

Minimum necessary = only what is needed for the specific task

- Ask yourself: "Does this person need this information to do their job?"
- When in doubt, share less, not more
- Follow facility policies for information sharing

---

4. Appropriate Settings for Discussion

Private Settings (APPROPRIATE)

These settings are appropriate for discussing patient information:

1. **Private patient rooms** (with door closed)
    - One-on-one with patient
    - With authorized family members (with patient consent)
    - Door must be closed
2. **Designated work areas** (not public)
    - EEG reading rooms
    - Technologist workstations (not in public view)
    - Private offices with closed doors
3. **Secure conference rooms**
    - For case discussions
    - For teaching (with de-identified data)
    - Door closed, not accessible to public
4. **Private offices with closed doors**
    - Physician offices
    - Administrative offices
    - Any private, secured space
5. **Secure electronic communication systems**
    - Encrypted email (facility-approved)
    - Secure messaging platforms (HIPAA-compliant)
    - Electronic health record systems

Inappropriate Settings (HIPAA VIOLATIONS)

These settings are INAPPROPRIATE for discussing patient information:

1. **Public hallways**
    - Anyone can overhear
    - No privacy protection

    - Common HIPAA violation
2. **Elevators**
    - Public space
    - Others present
    - No privacy
3. **Cafeterias**
    - Public dining area
    - Others can overhear
    - Common violation location
4. **Waiting rooms**
    - Other patients present
    - Family members present
    - No privacy
5. **Public areas where others can overhear**
    - Lobbies
    - Public restrooms
    - Parking lots
    - Anywhere others can hear
6. **Social media platforms**
    - Facebook, Twitter, Instagram, etc.
    - Even "private" groups
    - Never appropriate for PHI
7. **Unsecured email or text messages**
    - Personal email
    - Personal text messages
    - Unencrypted communication
8. **Phone conversations in public**
    - Where others can overhear
    - In public spaces
    - Without privacy

Key Rules

- **Never discuss patient information in public or where others can overhear**
- **Assume others can hear in public settings** - even if you think no one is listening
- **Use private settings for all patient discussions**
- **If unsure, choose the more private option**
- **Close doors when discussing patient information**

Common Violation Scenarios

Scenario 1: Hallway Discussion

- **Violation:** Two technologists discussing a patient's EEG findings in the hallway
- **Problem:** Others can overhear (staff, visitors, other patients)

- **Fix:** Move to private room or designated work area

Scenario 2: Elevator Conversation

- **Violation:** Technologist on phone discussing patient with physician while in elevator
- **Problem:** Others in elevator can hear
- **Fix:** Wait until in private area, or step out of elevator

Scenario 3: Cafeteria Discussion

- **Violation:** Staff discussing interesting case during lunch break
- **Problem:** Others at nearby tables can overhear
- **Fix:** Only discuss in private, secure areas

---

5. De-identification for Teaching Materials

Complete De-identification Required

Teaching materials must be completely de-identified:

1. **Remove all 18 HIPAA identifiers** (see Section 2)
2. **Remove unique clinical details** that could identify patient
3. **Remove rare findings** that could allow re-identification
4. **Ensure re-identification is not possible**

Examples of Re-identification Risks

Rare Patterns or Findings:

- "Only 2 patients in facility history had this pattern" = identifiable
- "Unique combination of findings" = identifiable
- "Rare syndrome presentation" = identifiable

Specific Dates or Timing:

- "EEG performed on 3/15/2023 at 2:30 PM" = identifiable
- "Patient admitted on specific holiday" = identifiable
- "Unique timing of events" = identifiable

Unique Combinations:

- "45-year-old male with rare syndrome X and pattern Y" = identifiable
- Multiple details together can identify patient
- Combination of age, gender, and rare finding = identifiable

Geographic Details:

- "Patient from City Z with rare finding on Date X" = identifiable
- Location + timing + findings = identification
- Even without name, can be identified

De-identification Checklist

Before using material for teaching, verify:

- ☐ All 18 HIPAA identifiers removed
- ☐ Dates removed or generalized (year only, if necessary)
- ☐ Rare findings removed or generalized

- [ ] Unique combinations removed
- [ ] Geographic details removed
- [ ] Re-identification not possible
- [ ] Material approved by facility privacy officer (if required)

Key Principle

De-identification must prevent re-identification

- Simply removing the name is NOT enough
- Must remove all identifiers AND unique details
- When in doubt, do not use the material
- Get approval from privacy officer if unsure

---

6. Social Media and Electronic Communication

Social Media Rules

NEVER post patient information on social media:

1. **No patient photos** (even without names)
    - Photos can identify patients
    - Even with faces blurred, other details can identify
    - Never post patient images
2. **No EEG tracings** (even if de-identified)
    - Rare patterns can identify patients
    - Unique findings can allow re-identification
    - Even "de-identified" tracings may violate policy
3. **No patient stories or cases**
    - Even without names, stories can identify patients
    - Unique details allow re-identification
    - Never share patient cases on social media
4. **No facility-specific information**
    - Facility name, location, or identifying details
    - Information that could identify where patient was treated
5. **No discussions about patients**
    - Even in "private" groups
    - Even without names
    - Social media is never appropriate for PHI

Violations:

- Violates HIPAA
- Violates facility policies
- Can result in termination
- Can result in legal action

Electronic Communication

Use secure methods for electronic communication:

1. **Secure email systems** (encrypted, facility-approved)
    - Facility email systems
    - Encrypted email platforms
    - HIPAA-compliant systems
2. **Secure messaging platforms** (HIPAA-compliant)
    - Approved messaging apps
    - Encrypted communication
    - Facility-approved platforms
3. **Electronic health record systems**
    - Secure messaging within EHR
    - Secure communication features
    - HIPAA-compliant systems

NEVER use:

- Personal email (Gmail, Yahoo, etc.)
- Personal text messages (SMS, iMessage, etc.)
- Unsecured cloud storage (Dropbox, Google Drive, etc.)
- Social media messaging (Facebook Messenger, etc.)

Key Rules

Assume all social media and unsecured communication violates HIPAA

- When in doubt, do not share
- Use only facility-approved secure methods
- Protect patient information in all electronic formats
- Follow facility policies strictly

Common Violation Scenarios

Scenario 1: Facebook Post

- **Violation:** Technologist posts "Interesting EEG case today" with photo
- **Problem:** Even without name, may identify patient or violate policy
- **Fix:** Never post anything patient-related on social media

Scenario 2: Personal Email

- **Violation:** Technologist emails EEG tracing to colleague using personal email
- **Problem:** Personal email is not secure, violates HIPAA
- **Fix:** Use only facility-approved secure email systems

Scenario 3: Text Message

- **Violation:** Technologist texts patient information to physician
- **Problem:** Text messages are not secure, violate HIPAA
- **Fix:** Use only secure, facility-approved communication methods

---

7. Patient Access to Records

Patient Rights Under HIPAA

Patients have the right to:

1. **Access their medical records**
    - Right to request copies
    - Right to inspect records
    - Right to receive electronic copies (if available)
2. **Request amendments**
    - Right to request corrections
    - Right to add statements
    - Right to dispute information
3. **Request accounting of disclosures**
    - Right to know who accessed their records
    - Right to know when records were shared
    - Right to know why records were shared
4. **File complaints**
    - Right to file complaints about privacy violations
    - Right to file complaints with HHS Office for Civil Rights
    - Right to file complaints with facility
5. **Request restrictions**
    - Right to request restrictions on use/disclosure
    - Right to request confidential communications
    - Right to request alternative communication methods

Technologist Role

Technologists should:

1. **Direct patient requests to medical records department**
    - Do not provide records directly
    - Follow facility policy
    - Direct to appropriate department
2. **Follow facility policy for patient access**
    - Know facility procedures
    - Follow proper authorization requirements
    - Maintain confidentiality during process
3. **Do not provide records directly without proper authorization**
    - Require proper authorization
    - Follow facility procedures
    - Protect patient privacy
4. **Maintain confidentiality during the process**

    - Protect patient information
    - Follow privacy requirements
    - Ensure secure handling

Key Principle

Follow facility policy for patient access requests

- Do not provide records directly without authorization
- Direct patients to appropriate department
- Maintain confidentiality throughout the process
- Know your facility's procedures

Common Scenarios

Scenario 1: Patient Requests Copy

- **Appropriate:** Direct to medical records department
- **Inappropriate:** Provide copy directly without authorization

Scenario 2: Family Member Requests

- **Appropriate:** Require proper authorization (patient consent, power of attorney, etc.)
- **Inappropriate:** Provide based on verbal permission or assumptions

Scenario 3: Patient Wants to See Results

- **Appropriate:** Direct to ordering physician or medical records
- **Inappropriate:** Interpret results or provide detailed explanations without physician involvement

---

8. Reporting HIPAA Violations

If You Witness a Violation

Report HIPAA violations through appropriate channels:

1. **Report to supervisor or privacy officer**
    - Immediate reporting required
    - Follow facility reporting procedures
    - Document the incident
2. **Document the incident**
    - What happened
    - When it happened
    - Who was involved
    - What information was disclosed
3. **Follow facility reporting procedures**
    - Know your facility's procedures
    - Follow proper channels
    - Complete required documentation
4. **Do not ignore violations**
    - Reporting is required

- Ignoring violations is itself a violation
- Protect patient privacy

If You Commit a Violation

If you commit a violation:

1. **Report it immediately**
   - Report to supervisor or privacy officer
   - Do not try to cover it up
   - Immediate reporting is required
2. **Document the incident**
   - What happened
   - When it happened
   - What information was disclosed
   - Who may have accessed the information
3. **Complete additional HIPAA training**
   - May be required
   - Understand what went wrong
   - Prevent future violations
4. **Follow facility corrective action procedures**
   - Complete required actions
   - Follow facility policies
   - Prevent recurrence

Key Principle

HIPAA violations must be reported immediately

- Do not ignore or cover up violations
- Report through appropriate channels
- Complete required training and corrective actions
- Protect patient privacy

Breach Notification Requirements

If a breach occurs:

1. **Report immediately** to supervisor/privacy officer
2. **Attempt to mitigate** (recall email, recover documents, etc.)
3. **Follow facility breach notification procedures**
4. **May require patient notification** (if breach is significant)
5. **May require HHS notification** (if breach affects 500+ patients)

---

9. Security Rule Requirements

Administrative Safeguards

Facilities must have:

1. **Security management process**
    - Risk analysis
    - Risk management
    - Sanction policy
    - Information system activity review
2. **Assigned security responsibility**
    - Security officer designated
    - Clear responsibilities
    - Accountability
3. **Workforce security**
    - Authorization/supervision
    - Workforce clearance procedure
    - Termination procedures
4. **Information access management**
    - Access authorization
    - Access establishment
    - Access modification
5. **Security awareness and training**
    - Security reminders
    - Protection from malicious software
    - Log-in monitoring
    - Password management

Physical Safeguards

Facilities must protect:

1. **Facility access controls**
    - Contingency operations
    - Facility security plan
    - Access control and validation procedures
    - Maintenance records
2. **Workstation use**
    - Workstation security
    - Workstation use restrictions
3. **Workstation security**
    - Physical safeguards for workstations
    - Access restrictions
4. **Device and media controls**
    - Disposal
    - Media re-use
    - Accountability

- Data backup and storage

Technical Safeguards

Facilities must implement:

1. **Access control**
   - Unique user identification
   - Emergency access procedure
   - Automatic logoff
   - Encryption and decryption
2. **Audit controls**
   - Record and examine activity
   - Log access and activity
   - Monitor system use
3. **Integrity**
   - Ensure ePHI is not improperly altered or destroyed
   - Implement mechanisms to authenticate ePHI
4. **Transmission security**
   - Integrity controls
   - Encryption

Technologist Responsibilities

Technologists must:

1. **Use secure passwords**
   - Strong passwords
   - Never share passwords
   - Change passwords regularly
2. **Log off when finished**
   - Never leave workstations unattended
   - Log off when leaving area
   - Lock screens when away
3. **Protect electronic devices**
   - Secure laptops, tablets, phones
   - Encrypt devices if required
   - Report lost/stolen devices immediately
4. **Follow facility security policies**
   - Know and follow policies
   - Report security concerns
   - Complete security training

---

10. Business Associates

Business Associate Agreements

Business associates are:

- Third-party vendors who handle PHI
- Examples: Billing companies, transcription services, cloud storage providers
- Must have Business Associate Agreement (BAA) with covered entity
- Must comply with HIPAA Security Rule

Technologist Role

Technologists should:

- Know which vendors are business associates
- Only share PHI with authorized business associates
- Follow facility policies for sharing with business associates
- Report concerns about business associate compliance

---

11. Penalties and Consequences

Civil Penalties

Tier 1: Unknowing violation

- $100 - $50,000 per violation
- Up to $1.5 million per year

Tier 2: Reasonable cause (not willful neglect)

- $1,000 - $50,000 per violation
- Up to $1.5 million per year

Tier 3: Willful neglect (corrected within 30 days)

- $10,000 - $50,000 per violation
- Up to $1.5 million per year

Tier 4: Willful neglect (not corrected within 30 days)

- Minimum $50,000 per violation
- Up to $1.5 million per year

Criminal Penalties

Knowingly obtaining or disclosing PHI:

- Up to $50,000 fine
- Up to 1 year imprisonment

Under false pretenses:

- Up to $100,000 fine
- Up to 5 years imprisonment

With intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm:

- Up to $250,000 fine

- Up to 10 years imprisonment

Professional Consequences

- **Job termination**
- **Loss of professional license**
- **Loss of certification**
- **Lawsuits from patients**
- **Damage to professional reputation**

---

12. ABRET Exam High-Yield Topics

Must-Know Facts

1. **18 HIPAA identifiers** - Know all 18 by heart
2. **Minimum necessary rule** - Share only what is needed
3. **Appropriate settings** - Private settings only for discussions
4. **De-identification** - Complete removal of all identifiers
5. **Social media** - Never post patient information
6. **Patient rights** - Access, amendments, accounting of disclosures
7. **Reporting violations** - Report immediately
8. **Security safeguards** - Administrative, physical, technical

Common Exam Questions

Question Type 1: HIPAA Identifiers

- "Which of the following must be removed for de-identification?"
- Answer: All 18 identifiers

Question Type 2: Minimum Necessary

- "The minimum necessary rule means..."
- Answer: Share only what is needed for the specific task

Question Type 3: Appropriate Settings

- "Which setting is appropriate for discussing patient information?"
- Answer: Private room with door closed

Question Type 4: De-identification

- "To use an EEG tracing for teaching, you must..."
- Answer: Remove all 18 identifiers and ensure re-identification is not possible

Question Type 5: Social Media

- "Posting a de-identified EEG tracing on social media is..."
- Answer: Potentially a HIPAA violation (even if de-identified)

Question Type 6: Patient Access

- "A patient requests access to their EEG report. You should..."
- Answer: Direct to medical records department following facility policy

Question Type 7: Reporting Violations

- "You witness a HIPAA violation. You should..."

- Answer: Report immediately to supervisor or privacy officer

---

13. Exam Readiness Checklist

Use this checklist to verify your understanding:

- [ ] Can identify all 18 HIPAA identifiers
- [ ] Understand minimum necessary rule
- [ ] Know appropriate vs inappropriate settings for discussion
- [ ] Can de-identify materials for teaching
- [ ] Understand social media restrictions
- [ ] Know patient access rights
- [ ] Can identify HIPAA violations
- [ ] Know how to report violations
- [ ] Understand consequences of violations
- [ ] Know facility policies for HIPAA compliance
- [ ] Understand security rule requirements
- [ ] Know technologist responsibilities for security
- [ ] Understand breach notification requirements
- [ ] Know penalties for violations

---

14. Study Tips

1. **Memorize the 18 HIPAA identifiers** - Know all 18 by heart
2. **Understand minimum necessary** - Share only what is needed
3. **Know appropriate settings** - Private settings only for discussions
4. **Learn de-identification** - Complete removal of all identifiers
5. **Remember social media rules** - Never post patient information
6. **Know reporting procedures** - Report violations immediately
7. **Understand consequences** - Fines, job loss, legal action
8. **Know patient rights** - Access, amendments, accounting
9. **Understand security requirements** - Administrative, physical, technical safeguards
10. **ABRET focus** - Expect questions on identifiers, minimum necessary, appropriate settings, de-identification, and reporting

---

15. Internal Cross-Links

Workflow

- **Ethics & Confidentiality:** Core ethical principles
- **Documentation & Reporting:** Confidentiality in documentation
- **Patient Safety:** Privacy in patient care

Cases

- **HIPAA violation scenarios:** Cases involving privacy violations
- **De-identification scenarios:** Cases involving teaching materials
- **Patient access scenarios:** Cases involving patient rights

Quizzes

- **HIPAA compliance MCQs:** Questions on HIPAA regulations
- **Confidentiality questions:** Questions on patient privacy
- **De-identification questions:** Questions on teaching materials
- **Patient rights questions:** Questions on patient access

End of Study Guide

For additional practice, complete quiz questions tagged: hipaa, confidentiality, privacy, patient-rights, security, de-identification