CHAPTER 3

Accreditation, Regulation, and HIPAA
Pretest (True/False)

• The acronym EPHI stands for protected health information in an electronic format.
• Medicare provides healthcare benefits for people who are poor.
• Local city and county governments may regulate or license healthcare facilities.
• Providing a patient with a copy of the privacy policy implies authorization for the practice to use PHI for almost anything.
• In general, a medical office must track the disclosure of PHI for purposes other than treatment, payment, or office operations and keep the records for at least six years.
Accreditation and Regulation

- Healthcare facilities and practitioners are licensed and regulated by federal, state, and local governments.
- Voluntary compliance with standards set by recognized accreditation organizations also assist in meeting government requirements.
- Government Regulation influences healthcare delivery by:
  - Requiring licensure of both facilities and their providers.
  - Requiring they meet certain conditions to participate in programs that reimburse them for treating patients.
    - Examples: Medicare, Medicaid.
CMS (Centers for Medicare and Medicaid Services)

- Medicare: provides healthcare coverage for people ages 65+, people with disabilities or end-stage renal disease (kidney failure)
- Medicaid: provides healthcare benefits (partially paid by the states) for people who are poor, blind, or have disability, pregnant women, and some persons over age 65 (in addition to Medicare)
Intermediaries

• Administer Medicare and Medicaid on state level
• Contract with CMS to handle claims processing, payments, authorizations, provider inquiries for region or state
• Follow rules set by CMS regarding preauthorization, payments, and coverage of medical services
• Example: Blue Cross/Blue Shield
Influence of CMS on Healthcare Delivery System

- Utilization management (UM)
- Quality improvement organizations (QIOs)
- Reimbursement rates
- Prospective payment system (PPS) and Diagnosis-Related Groups (DRG)
- Conditions of participation (COP) and deemed status
- HIPAA security standards enforcement
Other HHS Agencies Related to Healthcare Facilities

- Food and Drug Administration (FDA)
- Drug Enforcement Agency (DEA)
- Centers for Disease Control and Prevention (CDC)
- Office of Civil Rights (OCR)

(HHS – U.S. Dept. of Health and Human Services)
State Laws

- Provide detailed regulations concerning facility operations, sanitation, medical and nursing staff requirements, patient records
- May limit hospital services or require special licenses per department
- Require reporting of incidents of infectious diseases, child abuse, certain injuries (gunshots)
- Require reporting of substantial amount of statistical data concerning birth defects, cancer tumors, patients using facility
Deemed Status

• Means an accredited facility is deemed to have complied with CMS’s conditions of participation (COP) by virtue of having complied with standards set by another approved organization
  – Examples: Joint Commission, CAP, CARF

(CAP – College of American Pathologists)
(CARF – Commission on Accreditation of Rehabilitation Facilities)
Joint Commission

• Formerly known as JCAHO
• Leading accreditation organization for acute care facilities; submit statistical data quarterly
• Also accredits long-term, behavioral health, and ambulatory care settings

(JCAHO – Joint Commission on Accreditation of Healthcare Organizations)
Other Accreditation Organizations

- College of American Pathologists (CAP):
  - Accredits medical laboratories
  - Operates as CMS authority (has deemed status)
  - A laboratory facility with a CAP accreditation is deemed to have complied with Medicare COP standards.
Other Accreditation Organizations (continued)

• Commission on Accreditation of Rehabilitation Facilities (CARF):
  – Accredits organizations offering behavioral health, physical, and occupational rehabilitation services, assisted living, continuing care, community services, employment services
HIPAA (1996): Administrative Simplification Subsection

- Transactions and Code Sets
- Uniform Identifiers
- Privacy
- Security
HIPAA: Transactions and Code Sets

- First section of implemented regulations
- Govern electronic transfer of medical information for business purposes
  - Example: insurance claims, payments, eligibility
- Ensure that electronically exchanged information between systems uses same format
HIPAA: Transactions and Code Sets

- HIPAA standardized formats by requiring specific transaction standards for eight types of electronic data interchange (EDI)
- Two additional EDI transactions not yet finalized???
Ten HIPAA Transactions

1. Claims or equivalent encounters and coordination of benefits (COB)
2. Remittance and payment advice
3. Claims status
4. Eligibility and benefit inquiry and response
5. Referral certification and authorization
6. Premium payments
7. Enrollment and de-enrollment in a health plan
8. Health claims attachments (*not final*) – Jan. 1, 2013 (compliance date)
9. First report of injury (*not final*) – Workers’ Compensation???
10. Retail drug claims, coordination of drug benefits, and eligibility inquiries
HIPAA: Two Standard Code Sets Required

- ICD-9-CM codes for diagnoses (and some inpatient procedures)
  - Changing to ICD-10-CM on October 1, 2014
- CPT-4 and HCPCS codes for outpatient procedures

(ICD-9-CM – International Classification of Diseases, 9th revision, Clinical Modification)
(HCPCS – Healthcare Common Procedure Coding System)
HIPAA: Standards for Transactions

• Required for any coded information within a transaction
• Examples include codes for:
  – Sex
  – Race
  – Type of provider
  – Relation of policyholder to patient
HIPAA: Uniform Identifier Standards

- National Provider Identifier (NPI) for doctors, nurses, other healthcare providers
- Federal Employer Identification Number for employer-sponsored health insurance
- National Health Plan Identifier for each insurance plan and organizations that administer insurance plans
HIPAA: Privacy Rule

- Protects patient’s protected health information (PHI) (i.e. a patient’s identifiable health information) from unauthorized disclosure or use in any form.
- Creates foundation of federal protections for privacy of PHI while not replacing more stringent state or federal privacy regulations.
HIPAA Privacy: Safeguards to Protect Patient Confidentiality

- Speaking quietly when discussing patient’s condition with family members in public area
- Avoiding use of patients’ names in public areas
- Posting signs to remind employees to protect patient confidentiality
- Isolating or locking file cabinets or records rooms
- Providing additional security, such as passwords
HIPAA Privacy: Medical Office Compliance

- Providing copy of office privacy policy to patients
- Asking patient to acknowledge receiving copy of policy and/or signing consent form
- Obtaining signed authorization forms
- Tracking PHI disclosures when unrelated to treatment, billing, payment purposes
- Adopting clear privacy procedures
- Training employees to understand privacy procedures
- Designating individual responsible for seeing that privacy procedures are adopted and followed
- Securing patient records containing individually identifiable health information
HIPAA Privacy: Use of PHI without Consent

- Healthcare entity may use/disclose PHI for treatment, payment, healthcare operations
- Healthcare provider may disclose PHI about individual as part of payment claim
- Healthcare provider may disclose PHI related to treatment or payment activities of any healthcare provider
  - Including providers not covered by Privacy Rule
HIPAA Privacy: Other Uses of PHI

- Clinical staff may use related to patient care
- Nonclinical staff may use related to billing, claims, records-related activities, office or facility operations activities
HIPAA Privacy: Authorization Versus Consent

• **Authorization** requires a form signed by patients or their representatives for each type of PHI disclosure.

• **Consent** is inferred from patient’s receipt of a copy of the Privacy Policy and allows provider to share PHI for:
  – Patient treatment
  – Obtaining payment
  – Operation of medical practice or facility
HIPAA Privacy: Authorization Form

• Must Include:
  – Date signed
  – Expiration date
  – To whom information may be disclosed
  – What is permitted to be disclosed
  – For what purpose the information may be used
Figure 3-4 Sample Authorization Form with elements required by HIPAA.
HIPAA Privacy: Patients’ Rights

• Individuals have the right to request and receive reports of all disclosures made for purposes other than treatment, payment, operation of healthcare facility
  – Report must include date, whom information was provided to, description of information, and purpose
  – The patient can request the report at any time and the practice must keep the records for at least six years.

• Individuals may see and obtain copies of their medical records and request corrections if necessary
  – Facilities must provide access within 30 days of patient’s request, but may charge patients for copying/mailing costs
HIPAA Privacy: HIM Responsibilities

- Ensuring appropriate consent or authorization forms on file
- Ensuring requests for release of information occur within time frame of authorization
- Ensuring minimum necessary portion of chart sent to patient and disclosure tracked
- Providing patients with copies of records and disclosure reports (within office setting)
HIPAA: Security Standards

• Administrative
• Physical
• Technical

Note: Privacy rule applies to PHI in electronic, oral, or paper form. Security rule applies to PHI in electronic form only (i.e. EPHI).
HIPAA: Security Standards

• Administrative safeguards
  – Administrative functions implemented to meet security standards, including assignment or delegation of security responsibility to individual and security training requirements
HIPAA: Security Standards (continued)

• Physical safeguards
  – Mechanisms required to protect electronic systems, equipment, data from threats, environmental hazards and unauthorized intrusion
  – Include restricting access to EPHI and retaining off-site computer backups
HIPAA: Security Standards (continued)

• Technical safeguards:
  – Primarily automated processes used to protect data and control access to data
  – Include using authentication controls to verify authorization to use computer, or encrypting and decrypting data as it is stored and/or transmitted
1. Security Management Process

- **Risk Analysis**: Identify potential security risks, likelihood, and seriousness

- **Risk Management**: Decisions about how to address security risks, vulnerabilities and develop strategy to protect confidentiality, integrity, and availability of EPHI

- **Sanction Policy**: Define consequences of failing to comply with security policies, and procedures

- **Information System Activity Review**: Regularly review records to determine if any EPHI has been used, or disclosed in an inappropriate manner
2. **Assigned Security Responsibility**
   - Designate a security officer

3. **Workforce Security**
   - Authorization and/or Supervision
   - Workforce Clearance Procedure
   - Termination Procedures
4. Information Access Management

- **Access Authorization:** Organization identifies who has authority to grant access and the process for doing so.
- **Access Establishment and Modification:** How access is established and modified.
- **Isolating Healthcare Clearinghouse Functions:** Isolation of clearinghouse computers from other systems in organization.
HIPAA Security: Administrative Safeguards

5. Security Awareness and Training
   • Security Reminders
   • Protection from Malicious Software
   • Log-in Monitoring
   • Password Management
6. Security incident procedures – to identify and report security incidents
7. Contingency plan – for recovering access to EPHI
8. Evaluation – periodically review strategy and systems
9. Business Associate Contracts and Other Arrangements – ensure security of EPHI
HIPAA Security: Physical Safeguards

Protect electronic information systems and related buildings and equipment

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls
HIPAA Security: Technical Safeguards

Protect electronic PHI and control access to it

1. Access Control
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security
## Privacy and Security: Comparison

<table>
<thead>
<tr>
<th>Category</th>
<th>Privacy Rule</th>
<th>Security Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Type</td>
<td>EPHI</td>
<td>EPHI only</td>
</tr>
<tr>
<td></td>
<td>Oral PHI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Written PHI</td>
<td></td>
</tr>
<tr>
<td>Enforcing Agency</td>
<td>Office of Civil Rights (OCR)</td>
<td>CMS</td>
</tr>
<tr>
<td>Types/Coverage</td>
<td>Patient</td>
<td>Administrative</td>
</tr>
<tr>
<td></td>
<td>Business Associates</td>
<td>Physical</td>
</tr>
<tr>
<td></td>
<td>Minors</td>
<td>Technical</td>
</tr>
<tr>
<td></td>
<td>Personal Representative</td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td>Consent Authorization</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addressable (does not mean optional)</td>
</tr>
</tbody>
</table>