Domain III: Compliance

RHIT Exam Review Prep

Disclaimer

Please note that these presentations are designed to serve as a valuable supplement to your overall study plan to prepare for the RHIT certification examination.

Participation in these presentations does not guarantee a passing score on RHIT the examination. For more information on the testing dates and the RHIT credential go to www.ahima.org.

It is suggested that you follow the AHIMA Candidate Guide, Appendix H as a study guide for preparing for your certification exam.

Compliance (16%)
Knowledge Clusters

1. Ensure patient record documentation meets state and federal regulations
2. Ensure compliance with privacy and security guidelines (HIPAA, state, hospital, etc.)
3. Control access to health information
4. Monitor documentation for completeness
5. Develop a coding compliance plan (i.e., current coding guidelines)
6. Manage release of information
7. Perform continual updates to policies and procedures
8. Implement internal and external audit guidelines
9. Evaluate medical necessity (CDMP – clinical documentation management program)

Compliance (16%)
Knowledge Clusters - contineud

10. Collaborate with staff to prepare the organization for accreditation, licensing, and/or certification surveys
11. Evaluate medical necessity (Outpatient services)
12. Evaluate medical necessity (Data management)
13. Responding to fraud and abuse
14. Evaluate medical necessity (ISSI (utilization review))
15. Develop forms (i.e., chart review, documentation, EMR, etc.)
16. Evaluate medical necessity (Case management)
17. Analyze access audit trails
18. Ensure valid healthcare provider credentials

HIPAA Privacy & Security

- Ensure compliance with privacy and security guidelines (HIPAA, state, hospital, etc.)
- Control access to health information

Privacy and Security Guidelines

- HIPAA drives privacy and security
- Privacy standards
  - Defines appropriate use and disclosure
  - For more information www.hhs.ove/ocr/privacy
- Security standards
  - Ensures patient identifiable health information remain confidential and protected from unauthorized access
  - Standards set by ASTM and HL7

Privacy Regulations

Key law that governs the confidentiality of protected health information (PHI)

- Passed in the 1996 HIPAA and undated in ARRA of 2009
  - HIPAA has 5 titles
    - Title II applies to HIM and covers provisions related to preventing
      - healthcare fraud and abuse and medical liability (medical malpractice) reform
    - Resides under Administrative simplification designed to streamline and standardize healthcare along with
      - National provider identification and transaction and code set standardization requirements

Privacy Rule - continued

- Covered entities include healthcare providers (such as: hospitals, LTC facilities, physicians, pharmacies, insurance carriers, etc.)
- Business Associate is a person or an organization (subcontractors), other than the covered entity and it's workforce) that performs functions or activities on behalf of or for the covered entity that's involves PHI disclosure (Sayles, 2013)
  - Consultants, billing companies, transcription companies, account firms, law firms, patient safety organizations (PSO), health information organization (HIO), e-prescribing gateways, persons who facilitate data transmissions and personal health record (PHR) vendors.
  - Services can only be rendered under a BA Agreement that comply with HIPAA and ARRA requirements
    - Review the minimum requirements for BA Agreement

Privacy Rule - definitions

- **PHI** as individual **identifiable health information** transmitted by electronic media, maintained in any electronic medium or maintained in any other form or medium such as paper and oral form.
- **Deidentified information** is PHI with all elements that can identify the patient remove
- **Designated record (DRS)** includes the health record, billing records, various claim records that are used to make decisions about the patient.
- **Minimum Necessary Standard** access is limited to covered entities to the least amount of information to accomplish the intended purpose.

Privacy Rule - definitions

- **TPO (Treatment, Payment and Operations)** key concept that permits the release of PHI without an expressed consent.
- **Right of Access** is the concept that the patient has the right to make requests and how the covered entities respond
  - request amendment to PHI,
  - request accountability
  - Request confidential communications
  - Complain of Privacy rule violation
  - Obtain the Notice of Privacy Practices

Note: More information will be covered in Legal

Privacy Rule Administrative Requirements

- Designate a Privacy Officers
  - Maintains records
  - Works with OCR on complaints and compliance
- Requirement of privacy training
  - New hires must be trained within a reasonable amount of time after joining the CE
  - Refresher training, at least annually
- Requirements for establishing privacy safeguards for handling complaints
  - Administrative, technical and physical safeguards
- Standards for policies and procedures and changes to policies and procedures.

ARRA Penalties

- Ranges
  - $100 – 25,000/violations for unknowing violation
  - $1000 – 100,000/violation if due to reasonable cause
  - $10,000 – 250,000 for willful neglect that was corrected
  - $50,000 – 1,500,000 for willful neglect that was uncorrected
- Legal Action by State Attorneys General
  - Grants states the ability to bring civil action in federal court on behalf of residents who have been negatively impacted by a HIPAA violation.
  - OCR offers training to state attorney generals

ARRA Penalties

- Unannounced audits are allowed of covered entities and business associates to detect Privacy and Security Rule violation

Privacy Regulations

- **Red Flag Rule** of the Fair and Accurate Credit Transaction Act (FACTA)
  - Passed to protect patient records from the increasing medical identify theft and protecting patient identify

- State legislation
  - Protects highly sensitive health records
    - Mental health
    - HIV/AIDS
  - Can not preempt federal Privacy rule

General Rule

- Provides the objective and scope for the HIPAA Security Rule as a whole.
- They specify that covered entities must develop a security program that includes a range of security safeguards that protect individually identifiable health information maintained or transmitted in electronic form.
- Review what is covered by the General Rule

HIPAA Security Provision

- Administrative safeguard
  - Security Management Process
  - Assigned Security Responsibility
  - Workforce Security
  - Information Access Management
  - Security Awareness Training
  - Security Incident Procedures
  - Contingency Plan
  - Evaluation
  - Business Associate Agreement

HIPAA Security Provision

- Physical safeguards
  - Facility Access Controls
  - Workstation Security
  - Device and Media Controls
- Technical safeguards
  - Access Controls
  - Audit Controls
  - Integrity Controls
  - Person or Entity Authentication
  - Transmission Security
    - Including the use of encryption or other similar mechanisms

Question

- Which of the following provides the objective and scope for the HIPAA Security Rule as a whole?

A. Administrative safeguard
B. Documentation requirement
C. General Rule
D. Physical safeguards

Answer

- Which of the following provides the objective and scope for the HIPAA Security Rule as a whole?

A. Administrative safeguard
B. Documentation requirement
C. **General Rule**
D. Physical safeguards

Question

- The HIPAA Privacy Rule:

A. Applies only to certain states
B. Applies only to healthcare providers operated by the federal government
C. Applies nationally to healthcare providers
D. Serves to limit access to an individual's own health information

Answer

- The HIPAA Privacy Rule:

A. Applies only to certain states

B. Applies only to healthcare providers operated by the federal government

C. **Applies nationally to healthcare providers**

D. Serves to limit access to an individual's own health information

Question

- HIPAA regulations:

A. Never preempts state statutes
B. Always preempts state statutes
C. Preempt less strict state statutes where they exists
D. Preempt stricter state statutes where they exist

Answer

- HIPAA regulations:

A. Never preempts state statutes
B. Always preempts state statutes
C. **Preempt less strict state statutes where they exists**
D. Preempt stricter state statutes where they exist

HIPAA Security Provision

- Organizational requirements
  - Business associate or other contracts
  - Covered entity Responsibility
- Policies and procedures and documentation requirements
  - Security policies and procedures are in place
  - Documentation

Monitor documentation for completeness

Documentation Standards

- Types of standards
  - Content will vary based on the type of facility
    - Facility-specific standards
      - Facility policy and procedure manual
    - Licensure requirements
      - State Regulating Agencies driven
    - Certification standards
      - Such as Medicare, Medicaid
      - Conditions of Participation or Conditions of Coverage
    - Accreditation standards
      - Intensive external review process
      - JCAHO, CARF, AOA etc.

Acute Care Clinical Data - sampling

- Medical History & Physical Examination Report – 24 hours post admission
- Physician orders – within 24 hours
- Clinical Observations
  - Progress notes
    - Physician – based on patient's severity of illness and condition
    - Nursing – minimum of 1 note per shift plus
    - Ancillary services – per event of services
- Diagnostic & Therapeutic Procedures
- Consultation reports – per event of service
- Procedures and Surgical Documentation
  - Operative reports – immediately following procedure but no later than 24 hours post operatively
  - Anesthesia reports
  - Recovery Room reports
  - Pathology Reports
- Patient Consent Documentation
  - Implied and Expressed consents
- Discharge summary – within 30 days of discharge

Develop a coding compliance plan (i.e., current coding guidelines)

Developing a Coding Compliance Plan

- A ***Coding Compliance Plan*** is:
  - created by a coding department or HIMS department
- The ***purpose*** of the plan is to ensure compliance
  - The compliance ensured is with the rules and guidelines determined by government and other organizations a facility may belong to or be accountable to.

Coding Compliance

- The ***Coding Compliance Plan*** is developed by doing the following:
  - Follow the AHIMA Standards of Ethical Coding
  - Within the department create a policy and procedure handbook
  - Work with the billing department in a way that follows policies and procedures established.
  - Conduct coding and compliance audits
  - Based on the results of the audits, create an action plan if needed.

Detailed Steps for Creating a Coding Compliance Plan

- Policy statement written regarding the commitment of the department to correct assignment and reporting of codes.
- Post the Official Coding Guidelines used the facility.
- List the people responsible for assigning codes.
- What query process needs to be followed when documentation is not clear.
- If there are payer specific guidelines that need to be used, making sure these are posted in the plan.
- A procedure is in place in the plan for correcting incorrect codes.
- How education is conducted when areas of risk are identified by an audit.
- Identification of the coding resources available to the coders.

Detailed Steps for Creating a Coding Compliance Plan - continued

- Procedure for learning how to code new or unusual procedures.
- A policy for which procedures will be coded.
- A procedure for resolving coding disputes with physicians.
- Procedure for processing claim rejections.
- Procedure in place for coding records that will need to be coded with incomplete documentation.
- Procedure for handling requests for coding amendments.
- Policy for what resources the coder will have in addition to an encoder.

Manage release of information

Managing Release of Information

- Understand and follow local, state, federal statutes and regulations (i.e.. HIPAA Privacy Rule), as well as regulatory agency requirements (TJC)
- Follow organizational policies and procedures
- Conduct Quality Improvement:
  - Staff compliance with policies and procedures, regulations or state law
  - Staff performance (productivity)
- Investigate violations with Privacy Officer

Managing Release of Information

- Understand elements of a valid authorization
- Know when to release PHI without authorization
- Follow minimum necessary
  - Release only the necessary PHI to meet the purpose of the use or disclosure
- Track ROI activity for Accounting of Disclosure
  - Six years back

Perform continual updates to policies and procedures

Perform continual updates to policies and procedures

- **Policy**
  - General guidelines that direct behavior
  - Developed by upper management and approved by the CEO
  - Written in a standard format. Kept in policy manual
- **Procedure**
  - Series of related steps to accomplish a specific task
- **Update as policy or procedure changes**
  - Date with "last update" date
  - Review regularly

Implement internal and external audit guidelines

Implement internal and external audit guidelines

- **Audits**
  - Identify risks by identifying variations from established baselines
  - Results of the audits prompt further investigation to determine cause and corrective action
  - Frequency of audits determined by facility

  - Internal reviews conducted by staff
  - External reviews conducted by consultants or 3rd party payers, government, State etc

- HIM Audit Examples: RACs, coding, compliance, documentation requirements, record completion

Medical Necessity

- Evaluate medical necessity (CDMP – clinical documentation management program)
- Evaluate medical necessity (Outpatient services)
- Evaluate medical necessity (Data management)
- Evaluate medical necessity (ISSI (utilization review))
- Evaluate medical necessity (Case management)

Clinical Documentation

- Documentation should be complete, accurate, legible and timely.
- Address the clinical significance of abnormal test results
- Support the intensity of patient evaluation and treatment and describe the process and complexity of decision making
- Include all diagnostic and therapeutic procedures, treatments, and test performed, in addition to their results
- Include any changes in the patient's condition, including psychosocial and physical symptoms
- Be updated as necessary to reflect all diagnosis relevant to the care or services provided

Clinical Documentation (Cont.)

- Include all conditions that coexist at the time of admission, that subsequently develop, or that affect the treatment received and the length of stay. Encompasses all conditions that affect patient care in terms of requiring clinical evaluation, therapeutic treatment, diagnostic procedures, extended length of hospital stay or increased nursing care and monitoring.
- Be consistent and discuss and reconcile any discrepancies.
- Be legible and written in ink, typewritten, or electronically signed, stored, and printed.

Medical Necessity

- When Did This All Happen?
  - Around since 1965
- Medicare Carriers Manual 3/1/96 required documentation of medical necessity for chemistry profiles/panels
  - ABNs (Advance Beneficiary Notices)
- Heightened with the Balance Budget Act of 1997 (effective 1/1/98) (Section 4317 and Subtitle D Anti-fraud and Abuse Provisions)
- 3/10/2000 Federal Register – National Coverage Policies
- We should be obtaining ABNs for testing/services that a**re** not deemed medically necessary by Medicare

WHEN Should the ABN be Obtained?

- Must be given sufficiently in advance of the service to permit an "informed" refusal
- Must be given with enough information to permit "informed" agreement
- Must be signed by the patient before the service is rendered.

What Services Trigger the Need for an ABN?

- Services that can be "covered" services under Medicare but qualify for denial based on an LCD (Local Coverage Determination)rules
- Statutory screen exams of limited frequency when the prior test date is not known
  - Conditions disassociated with the test
  - Homecare to a non-homebound patient
  - There are more….
- More info on ABNs or the Beneficiary Notice Initiative
  - http://www.cms.hhs.gov/BNI

Intensity of Service/Severity of Illness

- Intensity of Service (IS) Criteria
  - Measures the level of intensity of treatment needed or resources used. "How much care do they need?"

  - Severity of Illness (SI) Criteria

    Measures how serious the patient's illness or condition.

    "How sick are they?"

Medical Necessity and Continued Stay

- **Example Policy:** The following criteria indicate medical necessity and continued hospital stay.
  - IV pain medications 3 or more times daily
  - White blood count >15,000/cu.mm.
  - Special neurological monitoring every 2 hours or more
  - Oral temperature > or equal to 101 degrees
  - Uncontrolled active bleeding at present time
  - Sudden onset of unconsciousness
  - Blood culture positive for pathogens
  - Respiratory assistance required
  - Surgery performed
  - Acute onset of chest pain/pressure

Answer

INTENSITY OF SERVICE	SEVERITY OF ILLNESS
IV pain medications 3 or more times daily.	White blood count >15,000/cu.mm.
Special neurological monitoring every 2 hours or more.	Oral temperature > or equal to 101 degrees
Respiratory assistance required	Uncontrolled active bleeding at present time.
Surgery performed	Sudden onset of unconsciousness.
	Blood culture positive for pathogens
	Acute onset of chest pain/pressure

Complete the **Utilization Review Form** indicating if the documentation supports continued stay or if the patient should be discharged.

Patient 1:

- 8/16/xx
- 0200 Sleeping in bed, breathing easily.
- 0115 SVN with albuterol 0.5 cc given.
- 0130 Breathing easy, good air exchange. Lungs fields with only minor crackles. No c/o at
- this time.
- 0640 Feels better after treatment. Improving air flow in all lung fields. Foley catheter removed.
- IV discontinued.
- 0700 Up to BR, voids well.
- 0800 Dr. Wainwright visits. Patient resting well. Blood sugar 130, vital signs stable. Ext. no edema. VS stable. Patient alert & oriented.

Utilization Review Form (Cont.)

- **Patient 2:**
- 3/29/xx
- Afebrile, VSS
- Drainage minimal
- Continue present treatment.
- IV Percocet every 4 hours
- 3-30-xx
- Afebrile
- VSS
- Vitals stable
- Drainage minimal
- Drains removed.
- IV Percocet every 6 hours

Answer

	SAMPLE	PATIENT 1	PATIENT 2	PATIENT 3
Criteria Indicator	Onset of chest pain	None	IV pain meds 4 x per day	Temp greater than 101
Decision (Continued stay or discharge)	Continued stay	Discharge	Continued Stay	Continued stay
Action (none, Discharge Form to Dr.)	None	Discharge Form to Doctor	None	None

Collaborate with staff to prepare the organization for accreditation, licensing, and/or certification surveys

Accreditation and Licensing Documentation Requirements

- Accrediting bodies and state licensing bodies are among the groups that have established standards for health record documentation.
- The Joint Commission is a not-for-profit organization that offers and accreditation program for hospitals and other healthcare organizations.
- Accreditation for healthcare facilities is voluntary.
- Without accreditation from an approved entity, cannot qualify for Medicare reimbursement.
- Facilities are "deemed" to be in compliance with the Medicare Conditions of Participation.

Documentation Standards

- Good documentation practices are required for organizations to be in compliance with established regulations and standards from a variety of groups.
- HIM director establishes mechanisms to ensure specific regulatory standards are upheld.
- Targets are identified to monitor in order to maintain compliance.
- Processes are in place within the department to monitor compliance.

Examples:

- Record completion process
  - Monitoring delinquency rates
  - Monitoring timely completion of medical reports
  - Monitoring health record completion
- Documentation
  - Monitoring the use of abbreviations, acronyms, and symbols
  - Confidentiality of information
  - Access to patient records

Management and Supervisory Process

- HIM departments play significant roles in operations of a healthcare facility.
- Policies and procedures serve as the foundation of the HIM department.
- Policies and procedures follow a specific format and must be up to date.
- Policies are broad statements while procedures are specific statements on how the work is performed.
- Both must be dated, have a revision date if revised, and signatures.

Collaboration with Staff

- To prepare for the surveyors for the accreditation process, the entire department is involved in the preparation.
- Policies and procedures should be updated by the manager or supervisor and kept available to all staff.
- Department should be neat and organized.
- Staff should be prepped on how to communicate with the surveyors.
- Charts filed away and neatly organized on the shelf.
- Process in place on how to fulfill chart request from the surveyors.

Collaboration - Continuous

- Vacation time should be suspended for the timeframe the surveyors are expected.
- Manager/director consulted before any actions are taken by the staff.
- Department clear of any debris, food, clutter.
- Charts signed out using established procedure.

Responding to fraud and abuse

Responding to fraud and abuse

- **Fraud:** Crime against payers
  - Ie) Upcoding, Unbundling, Billing for services not performed
- **Abuse:** Pattern of practice inconsistent with sound business
  - Ie) Submitting claims for not medically necessary services, not following Medicare guidelines or agreements

- **Follow your compliance plan:**
  - Written standards of conduct
  - Consult Chief Compliance Officer
  - Follow process for receiving complaints of violations
  - Respond to allegations of improper acts and enforce disciplinary actions
  - Investigate and correct problems

Develop forms (i.e., chart review, documentation, EMR, etc.)

Develop forms

- 1. Determine the purpose of the form
- 2. Keep the form simple
- 3. Follow basic, consistent information on each form
  - -Title placement, margins, size, content, appearance, signature lines
- 6. Consider paper requirements
- 7. Prepare draft for review
- 8. Pilot the form

Analyze access audit trails

Audit Log (audit trail)

- List of all changes made to patient documentation in an electronic health record system, including all transaction and activities, date, time, and users who performed the transacton. (Green 2009)

- HIPAA Administrative safeguards
  - Used by system administrators as an application control
  - Automated checks that help preserve data confidentiality and integrity
  - Audit trail is a software program that tracks every single access to date in the computer system
  - Can be used to reconstruct adverse events

Ensure valid healthcare provider credentials

Provider Credentialing

- In the healthcare environment it is important to ensure that healthcare providers have proper credentials meeting set standards and maintain their credentials by meeting set standards on an ongoing basis.
- A healthcare organization is responsible for ensuring that the healthcare providers it hires have proper credentials.
- From a risk management perspective and a patient quality of care perspective, this is an important process that must be in place in a healthcare organization.

Provider Credentialing

- A healthcare provider credential makes a statement that the provider can provide quality care to a patient.
- As a provider works at a facility, data is gathered on the provider over a period of time to determine ongoing ability of the provider to provide quality care.
- This data is most often collected by the Health Information Management department.
  - There is usually one person in the department who is designated to manage this information to determine proper credentialing and facility privileges on an ongoing basis.
  - Credentials are always being reviewed and verified by the hospital or facility to ensure proper credentialing at all times by their health care providers.

Credentialing Committee

- In a healthcare organization there is usually a Credentials Committee that reviews all physician credentials based on the following criteria:

- Required education
- Required training on site
- Licensing
- Board Certification
- Insurance Coverage
- Work History
- Medicare and Medicaid Sanctions
- Malpractice Claims History
- TB Screening
- Criminal background checks
- Letters of Reference
- Criteria met for re-certification when needed

- Providers must submit proof of their experience in their field before being approved to join the medical staff. There is a one year appointment if approved and then reviewed every two years after that. Physician data collected by the Health Information Department is an important part of this process to verify and re-verify provider credentials.

Terms you need to know…

What are these?

- **OASIS**-Outcomes and Assessment Information Set.
  - Standardized data to gather data about outcomes for Medicare beneficiaries receiving services from home health agency.
- **OIG**- Office of Inspector General
  - Issues guidelines for compliance programs
- **OCR** – Office of Civil Rights
  - Charged with oversight of Privacy & Security Rules
  - Monitors and investigates reports of breaches by covered entities and business associates.
- **AHRQ-**Agency for Healthcare Research and Quality
  - Organization within federal government that looks for efficiency and effectiveness of delivery systems, disease protocols, guidelines to improve disease outcomes

What are these?

- **UR –** Utilization Review
  - Process of determining whether care is necessary
  - preadmission review, continued stay review, discharge review
- **CMS** - Medicare
  - Federally funded health program established 1965 as part of the Social Security Act to assist in medical care costs of Americans 65 years and older and qualified disabled individuals

What are these?

- **HIPAA – Health Insurance Portability & Accountability Act of 1996**
  - 45 CFR 160, 162, and 164
  - Federal legislation enacted to provide continuity of health care coverage, control fraud and abuse, reduce healthcare costs, and guarantee the security and privacy of protected health information

What are these?

- **Privacy Rule**
  - The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes.

What are these?

- **Security Rule**
  - The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

What are these?

- **Medical staff** operates by medical staff bylaws. These are legally binding policies.

- **CEO-**responsible for implementing policies and strategic direction set by Board. Responsible for executive management team and coordinating hospital services

Examples of Questions

Question

- A statement or guideline that directs decision making or behavior is called a:

- A. Directive
- B. Procedure
- C. Policy
- D. Process

Answer

- A statement or guideline that directs decision making or behavior is called a:

- A. Directive
- B. Procedure
- **C. Policy**
- D. Process

Question

- The act of granting approval to a health care organization based on whether the organization has met a set of voluntary standards is called:

- A. Accreditation
- B. Licensure
- C. Acceptance
- D. Approval

Answer

- **The act of granting approval to a health care organization based on whether the organization has met a set of voluntary standards is called:**

- **A. Accreditation**
- B. Licensure
- C. Acceptance
- D. Approval

Why?

- Joint Commission is an example of an accreditation agency.
- Agency has been granted deemed status by Medicare program. This means they survey for compliance with the Medicare CoP instead of the government. CoP rules by CMS
- Standards set by Joint Commission- continual improvement in place from governing body down
- Tracer Methodology for on-site surveys-entire healthcare process

Question

- What does access control mean?

- A. ID security risks
- B. ID data employees have a right to use
- C. Implement safeguards to protect physical media
- D. Restricting access to computer rooms

Answer

- What does access control mean?

- A. ID security risks
- B. ID data employees have a right to use
- C. **Implement safeguards to protect physical media**
- D. Restricting access to computer rooms

Why?

- Physical access controls protect equipment, media or facilities
- Locks on doors to mainframes, terminals to protect against theft
- Computer screen positions to protect confidential data
- Access control also IDs which employees have access to what data

Question

- Which is a software program that tracks every access to data in the computer system?

- A. Access control
- B. Audit trail
- C. Edit check
- D. Risk assessment

Answer

- Which is a software program that tracks every access to data in the computer system?

- A. Access control
- **B. Audit trail**
- C. Edit check
- D. Risk assessment

Why?

- Name of person, date time, action taken such as read, modify, delete, print
- Organization's policies determine when audit trails are reviewed
- Purpose: Detect breach of security

Question

- If HIM acts in deliberate ignorance or in disregard of official coding guidelines, it is committing:

- A. Abuse
- B. Fraud
- C. Malpractice
- D. Kickbacks

Answer

A. Abuse

B. **Fraud**

C. Malpractice

D. Kickbacks

- Three areas of risk for claim submission
  - 1. Coding and billing
  - 2. Documentation
  - 3. Medical necessity

Billing for non-covered services, duplicate billing, failing to return overpayments, unbundling, unnecessary services, overcoding, services not rendered

Question

- Security policies and procedures for an organization should be reviewed at least:

A. Every six months

B. Once a year

C. Every two years

D. Every five years

Answer

A. Every six months

B. Once a year

C. Every two years

D. Every five years

Resources

Here's a great HIPAA Privacy & Security Review that's fun too. This link takes you to HealthIT.gov and you can enjoy 2 games on privacy and security as it relates to healthcare.

- http://www.healthit.gov/providers-professionals/privacy-security-training-games

Q&A