CHPE - HIPAA Privacy Training: Practice Questions

Chapter 1- HIPAA Basics

Topic A - HIPAA Introduction

1. Who's impacted by HIPAA?

HIPAA impacts health plans, health care clearinghouses, and health care providers that send or receive, directly or indirectly, HIPAA-covered transactions. These entities have to meet the requirements of HIPAA. Covered entities need to work with business associates and workforce members (employees, volunteers, temporary staff, agents, and contractors) who have access to health information to ensure reasonably the security and privacy of this information in any form.

2. How does HIPAA impact covered entities?

HIPAA impacts covered entities by requiring them to ensure privacy and security when health information is stored, maintained, or transmitted. In addition, specified transactions must comply with HIPAA standards. At a minimum, HIPAA requires covered entities to:

- Comply with standard transaction and code sets
- Use designated national identifiers as required by HIPAA identifier rules
- Provide information to patients and health plan members about their privacy rights and how their information can be used
- Adopt clear privacy/security policies, procedures, and practices that address availability, confidentiality, and integrity of protected health information (PHI)
- Train workforce members so that they understand the privacy/security policies, procedures, and practices
• Designate a privacy official and a security official (may be the same person) to be responsible for seeing that privacy/security compliance is met and continues to be met
• Secure patient and health plan member records containing individually identifiable health information so that they aren't readily available to those who don't need them
• Implement policies, procedures, and practices that reasonably ensure that only the minimum amount of PHI is shared when needed to conduct the business of health care
• Reasonably ensure that patients and health plan members are aware of their rights regarding access to, amendment of restriction of, etc., their medical information

3. Outline the HIPAA timeline for compliance.

• April 16, 2003 — Schedule for testing to begin no later than April 16, 2003
• April 14, 2003 — Privacy
• July 30, 2004 — National Employer Identifier
• April 21, 2005 — Security
• May 23, 2007 — National Provider Identifier
• Mid to late 2009 — Healthcare Claims Attachment

4. Imagine that you're describing HIPAA's core requirements and impact to a client. Summarize the impact HIPAA has on businesses in the health care industry.

HIPAA requires:

• Standardization of electronic, administrative, and Financial health care transactions
• Unique health identifiers for employers, health plans and health care providers, (likely not individuals)
• Security standards protecting the availability, confidentiality, and integrity of individually identifiable health information—past, present, and future
• Privacy of protected health information with specific rules around how protected information can be shared
• Continued management burden for compliance protect management, execution, testing, training, etc.
• Ongoing expenses (staff and fiscal) reasonably to ensure continued privacy and security compliance

5. Which of the following are examples of health care providers?

A. Physicians
B. Billing services
C. Hospitals
D. Medical review*
E. HMOs
F. Dentists
G. Pharmacies


Healthcare clearinghouses are organizations that process health care transactions on behalf of providers and insurers. Examples include:

• Billing services
• Repricing companies
• Medical reviewers
• Community health management information systems
• Value added networks
• Switches

Topic B - Administrative Simplification

1. Let’s say your client wants to understand HIPAA Administrative Simplification standards better. What are the key standards and supporting standards that were adopted?
The Administrative Simplification standards include:

- Standards for Electronic Transactions, Code Sets, and Identifiers
- Standards for Privacy of Individually Identifiable Health Information (otherwise known as protected health information or PHI)
- Administrative, Physical, and Technical Security Standards

Supporting standards include:

- Standards for Code Sets
- National Standard for Identifiers

2. **Why is HIPAA primarily about e-business initiatives within an organization?**

Because health care business applications include patient scheduling, registration, clinical reporting, billing, and health insurance claims. Healthcare business applications are also involved in the storage and movement of medical and claims records and transactions. The Administrative Simplification subtitle specifies that standards be adopted for the implementation of Electronic Data Interchange (EDI) standards for the electronic transmission of many administrative and financial transactions that had been predominantly performed on paper or using nonstandard transactions. In addition, standards for protecting the privacy and security of patient and health plan member health information during the transactions are also implemented.

As a result of HIPAA, all health care business applications have to be secure and need to integrate with the health organization's security infrastructure. These standards are the launch pad for e-business initiatives for electronic, and secure, medical information. The HIPAA privacy rule, though, also provides protections against inappropriate disclosure and use of PHI in any form, not just electronic.

3. **After listening to a quick executive overview of HIPAA basics, your client asks for examples of some specific and relevant transactions. What might you include in this list of examples?**
A transaction amounts to the exchange of information between two parties to carry out health care financial or administrative activities. There are transactions that cover the following types information exchanges:

- Health claims or equivalent encounter information
- Healthcare payment and remittance advice
- Coordination of benefits
- Health claims status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- Other transactions that the Secretary of HHS may prescribe by regulation

4. Identify some key technology components of a secure infrastructure for a health care organization.

- Firewalls
- Intrusion Detection Systems (IDS)
- Secure Virtual Private Networks (VPNs)
- Secure Messaging
- Biometrics
- Smart cards
- Authentication tokens
- Antivirus and antispyware applications
- Secure web sites
- Digital signatures
- Media encryption software

Topic C - HIPAA penalties

1. What type of penalties does HIPAA set for noncompliance?
HIPAA established civil and criminal penalties for noncompliance. Civil penalties take the form of monetary fines. Criminal penalties may take the form of monetary fines and/or imprisonment.
2. Give some examples of criminal penalties under HIPAA.

Criminal penalties are:

- Up to $50,000 and one year in prison for obtaining or disclosing protected health information
- Up to $100,000 and up to five years in prison for obtaining protected health information under false pretenses
- Up to $250,000 and up to ten years in prison for obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm

3. What's the civil monetary penalty for violating transaction standards?

The civil monetary penalty for violating transaction standards is up to $100 per person per violation and up to $25,000 per person per violation of a single standard per calendar year.

4. What's the penalty for misuse with intent to sell, transfer, or use identifiable health information?

If misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than ten years.

Topic D - HIPAA-related organizations

1. What's the target audience of the NC'PDP?

The NCPDP's target audience includes the pharmacy services sector of the health care industry. This includes organizations such as:

- Pharmacy chains
- Database management organizations
• Pharmaceutical manufacturers
• Telecommunication and systems
• Wholesale drug distributors
• Pharmacy benefit managers

2. What do WPC published Implementation Guides address?

These guides generally address industry-specific or company-specific EDI implementation issues and often include explanatory front matter, figures, examples, and cross-references.

3. Describe the XCVHS organization. How is the NCVHS involved with the HIPAA ASCA?

The National Committee on Vital and Health Statistics (NCVHS) is an advisory committee to the Secretary of Health and Human Services. The HIPAA Administrative Simplification Compliance Act (ASCA) requires that a sample of compliance plans be provided to NCVHS.

4. What’s the purpose of a DSMO? Give some examples of specific DSMOs.

The Secretary of HHS named six organizations to maintain standards using criteria specified in the Rules defined. These organizations are referred to as Designated Standards Maintenance Organizations (DSMOs). They are:

• ANSI Accredited Standards Committee (ASC) X12
• Dental Content Committee of the American Dental Association
• Health Level Seven (HL7)
• National Council for Prescription Drug Programs (NCPDP)
• National Uniform Billing Committee (NUBC)
• National Uniform Claim Committee (NUCC)
Topic E - HIPAA terminology

1. Let's say your client wants a better understanding of exactly what constitutes covered entities under HIPAA statute and rule. Describe the scope of covered entities under HIPAA.

The regulations place specific obligations upon covered entities. Covered entities include health plans (including most employer-sponsored group health plans), health care clearinghouses, and any health care provider who transmits protected health information using a HIPAA-defined standard transaction directly or indirectly.

Most health care providers use electronic transmission in some form or another when processing claims or in their financial dealings with health plans, such as Medicare or commercial plans. In these cases, the HIPAA statute and rules apply to these health care providers.

2. What's a health care clearinghouse?

A health care clearinghouse is an entity that performs the functions of format translation and data conversion to and from HIPAA standard transactions, generally on behalf of a health plan or a provider. When engaged in these activities, a billing service company, repricing company, community health management information system, community health information system, or value-added networks and switches, would be considered a health care clearinghouse.

3. Give some examples of identifiers within health information that constitute identifiable information?

- The individual's name
- City or county where the individual lives
- Zip Code
- Social Security number
- Finger print
- Telephone number
- Medical record number or fax number
- E-mail address
4. What does UMO refer to?

Utilization Management Organizations (UMOs) are insurance companies. HMOs, Preferred Provider Organizations (PPOs), health care purchasers, professional review organizations, other providers, and other utilization review entities that receive and respond to requests for authorization and certification.

5. Define the term "business associate."

A business associate is defined as an individual or third party entity that provides a service for a covered entity requiring the exchange of PHI between the covered entity and the business associate.

6. Should a hospital's board of directors sign business associate contracts? Why or why not?

This is not an easy question. Board members may have access to PHI when QA and other patient issues reach the board level. They may not be business associates, because they are part of the covered entity. The workforce definition doesn't apply to board members, because they aren't individuals under the direct control of the entity. However, board members do set policy and strategy for the organization and may review PHI from time to time. So while they may not be employees, they do represent the entity.

Generally speaking, though, the hospital's board of directors would not directly enter into contracts of any kind. Business associate contracts are generally managed as part of contracting under the oversight of the compliance officer and/or legal counsel.

7. A hospital contracts with a bank to process credit card payments by its patients for health care services. Is the bank a business associate? Why or why not?

The bank isn't a business associate of the hospital. The reason is that no business associate agreement is required between a covered entity and a financial institution if the latter only processes consumer-conducted financial transactions in payment for health care, and no information about the patient's medical condition is shared. In the event medical information is shared, the bank would then become a business associate. Also, care needs to be taken when making this determination. A covered entity, by its name or line of business (such as an alcohol and drug treatment facility, an inpatient mental health facility, etc.), may share PHI by virtue of the fact that the bank can determine the health condition of the
patient/consumer because of the nature of the facility. In such cases it's wise to enter into a business associate contract with the bank.

8. A hospital uses a courier service to deliver medical records to a laboratory. Is the courier service a business associate? Why or why not?

The courier service isn't a business associate of the hospital if it doesn't have access to PHI. The covered entity would be required to determine whether or not the courier service had access to PHI. If the answer is yes, the courier would be a business associate.

9. Would a hospital's Internet Service Provider (ISP) require a business associate agreement? Why or why not?

This depends on whether the hospital accesses PHI in the course of its normal duties. If it does, then a business associate agreement would be a requirement.

10. Would a cleaning service vendor require a business associate agreement? Why or why not?

If the cleaning services company isn't under the direct control of the covered entity, it may qualify as a business associate but only if it has regular access to PHI. Oftentimes this isn't the case.

11. Who are the exceptions to the business associate rules?

Four business associate exceptions involve treatment, financial transactions, disclosures between a group health plan and plan sponsor, and organized health care arrangements.

12. Describe an organized health care arrangement. Are participating providers required to have business associate agreements between them? Explain.

An organized health care arrangement is a clinically integrated setting in which patients receive care from multiple health care providers. Providers participating in an organized health care arrangement aren't business associates of each other. Examples include independent practice associations of physicians and hospital medical staff arrangements.
Review Questions:

1. **The definition of the term workforce is important in the contest of identifying business associates. Define this term.**

The term workforce refers to employees, volunteers, trainees, contractors, and other persons under the direct control of a covered entity, whether or not they're paid by the covered entity.

2. **Who fit into the category of covered entity?**

There are three classes of covered entities: Health plans, health care clearinghouses, and health care providers that transmit directly or indirectly HIPAA defined transactions (which include web-based transactions).

3. **What HIPAA rules have been finalized?**

The HIPAA rules that have been finalized include:

- Transaction and Code Set Rule
- Privacy Rule
- Security Rule
- National Employer Identifier Rule
- National Provider Identifier Rule

4. **What's health information?**

Health information is any information, whether oral or recorded, in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse
• Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual

5. What are the civil and criminal penalties for not adhering to the requirements of the HIPAA rules?

Civil penalties are measured by violation and amount to $100 per violation with a maximum of $25,000 per year for like violations.

Criminal penalties are dependent on the severity of the violation and could include:

- A fine of not more than $50,000 and/or imprisonment of not more than one year
- If misuse is under false pretenses, a fine of not more than $100,000 and/or imprisonment of not more than five years
- If misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than ten years.

6. What should trading partner agreements not result in?

Specifically, trading partner agreements must NOT:

- Modify the definition, condition, or use of a data element or segment in the standard Implementation Guide
- Add any additional data elements or segments to the Implementation Guide
- Utilize any code or data values that aren't valid in the Implementation Guide
- Change the meaning or intent of the Implementation Guide
7. Give two examples of Organized Healthcare Arrangements (OCHAs)?

Examples of OCHAs include independent practice associations of physicians and hospital medical staff arrangements.
Chapter 2 - Transactions and code set overview

Topic A: Transactions

1. What type of transactions do the transaction standard apply to? What's the requirement for data storage and format?

The transaction standards apply only to Electronic Data Interchange (EDI) - when data is transmitted electronically between health care providers and health plans as part of a standard transaction. Data can be stored in any format, as long as it can be translated into the standard transaction when required.

2. What are the transaction standard requirements for Internet-based transactions?

Internet transactions are being treated the same as other electronic transactions. However, it's recognized that there are certain transmission modes in which the format portion of the standard is inappropriate. In these cases, the transaction must conform to the data content portion of the standard.

3. Describe the two-part test to determine if the transaction standard applies.

A simple two-part test, in question form, can be used to determine whether the standards are required.

- Question 1: Is the transaction initiated by a covered entity or its business associate? If no, the standard needn't be used.
- Question 2: Is the transaction one for which the Secretary of HHS had adopted a standard? If yes, the standard must be used. If no, the standard needn't be used.
4. Is a covered entity required to conduct compliant transactions with entities that aren't required to be in compliance?

A covered entity isn't required to conduct compliant transactions with entities that aren't yet required to be in compliance because they aren't conducting electronic transactions. However, once a covered entity exchanges transactions electronically, all electronic transactions subject to the HIPAA standards must be exchanged in the standard.

Review Questions

1. List the types of organizations required to adhere to the TCS Rule.

Organizations required to adhere to the TCS Rule include:

- Health plans (public and private)
- Providers who send and receive (directly or indirectly) HIPAA standard transactions, including web-based or DDE transactions
- Healthcare clearinghouses

2. Why was the TCS Rule adopted?

The TCS Rule was adopted to simplify health care administration and to adopt a standard set of transactions as opposed to the variety of transaction and code set standards that had been in use prior to the effective date of the rule.

3. Are Medicare and Medicaid programs required to adhere to the TCS Rule?

Medicare and Medicaid programs are required to adhere to the TCS Rule because they're defined as health plans. This means they're required to send and receive HIPAA standard transactions to and from covered providers and health care clearinghouses.
4. Can a health plan charge a provider if the provider sends standard HIPAA transactions directly or through a health care clearinghouse?

Health plans can't charge providers for sending and receiving HIPAA standard transactions. If the health plan needs the assistance of a health care clearinghouse to translate the transaction from the HIPAA standard to a proprietary format, the health plan is responsible for the cost and can't pass the cost along to the provider.
Chapter 3- Transactions - ANSI X12 and NCPDP transaction types

Topic A - ANSI ASC X12 standards

A-1: Discussing ANSI ASC X12 standards Questions and answers

1. List the EDI transaction standards that are addressed as part of HIPAA requirements.

   - Health claims
   - Health encounter information
   - Health claims attachments (after this standard is defined/
   - Health plan enrollments and disenrollments
   - Health plan eligibility inquiry and response
   - Health care claims payment and remittance advice
   - Health plan premium payments
   - First report of injury (after this standard is defined)
   - Health claim status inquiry and response
   - Referral certification and authorization

2. Which EDI transaction format replaces HCFA/CMS 1500?

   The 837 format replaces electronic versions of the uniform billing claim and the HCFA/CMS 1500. It can carry HMO medical encounter accounting information as well as billing claims.

3. Let's say your client, a health care provider, wants to understand better the Benefit Enrollment and Maintenance provision. Describe this provision.

   A provider uses the Enrollment or Disenrollment in a Health Plan (834) transaction to ask what the benefits, deductibles, and co-pays of the patient's health plan are and if the patient is on file and currently covered by the plan. The inquiry can ask whether a specific benefit is covered by the plan. The transaction has the capability to inquire if a specific benefit is covered for the patient on a given day, but the payer isn't required to answer in this level of detail. The response is conditional. That is, it isn't a guarantee of payment.
4. What are the most common 270 & 271 transaction flows? For example, who would be involved in each type?

This is the health plan eligibility inquiry and response transaction. Intermediaries are used through the health care industry. Intermediaries add significant complexity relative to the most basic 270/271 transaction "conversation" directly between a provider and a single payer. A single 270 request to an intermediary can result in multiple 270 requests to multiple payers. In another scenario, a 270 inquiry to an intermediary may generate another inquiry to a second intermediary before reaching the intended payer. The three most common 270/271 transaction scenarios include:

- Basic Transaction Flow
- Multiple-Payer Transaction Flow
- Multiple Intermediary Transaction Flow

5 What's the purpose of the ASC X12N 278 transaction?


6. What's the purpose of the ASC X12N 834 transaction?

ASC X12N 834 - Benefit Enrollment and Maintenance, or Enrollment or disenrollment in a Health Plan

7. What's the purpose of the ASC X12N 270/271 transaction?

ASC X12N 270/271 - Health Care Eligibility Benefit Inquiry and Response, or Health plan eligibility inquiry and response

Review Questions

1. List the types of payer organizations that send the 277 transaction.
Organizations sending the 277 Health Care Claim Status Response include:

- Insurance companies
- Third Party Administrators (TPAs)
- Service corporations
- State and federal agencies and their contractors
- Plan purchasers
- Any other entity that processes health care claims

2. List the transactions that have been defined and approved for use to date.

- 837P, I, D- Claims transaction
- 835 - Remittance advice (can include EFT)
- 834 - Enrollment and dis-enrollment
- 270/271 - Eligibility inquiry and response
- 276/277 - Claims status inquiry and response
- 820 - Premium payment
- 278 - Certification and authorization
Chapter 4 - Code sets and national identifiers

Topic A - Code Sets

1. Your client wants to understand better the significance of standardized code sets within health care transactions. Describe the relationship between transactions and code sets?

Transactions contain both code sets and identifiers. Code sets are mandated by HIPAA to be standardized, and certain fields in transactions must be completed only with values from code sets.

2. Specify the primary purpose of code

The primary purpose of the code sets is to standardize the identification of those things for which health care providers submit claims for reimbursement. These include:

• Medical diagnosis codes
• Medical procedure codes
• Medical concepts
• Medical supplies

3. Name the code sets that were adopted under HIPAA.

• International Classification of Diseases, Clinical Modification (ICD-9-CM), Volumes 1 and 2
• Current Procedural Terminology, 4th Revision (CPT-4)
• Code on Dental Procedures and Nomenclature (CDT)
• ICD-9-CM, Volume 3
• National Drug Code (NDC)
• Health Care Common Procedure Coding System (HCPCS)
4. Which one of the following code sets is used to describe diseases, injuries, and impairments?

A. ICD-9-CM Volumes 1 and 2
B. CPT-4
C. CDT
D. HCPCS

5. Which one of following code sets describes physician services or procedures?

A. ICD-9-CM, Volume 3
B. CDT
C. CPT-4
D. HCPC

6. Which code set is used to describe dentist services or procedures?

CDT

7. Which code set is used to describe inpatient hospital services and surgical procedures?

ICD-9-CM, Volume 3

8. Which one of the following code sets is used to describe drugs in HIPAA transactions?

A. CDT
B. NDC
C. ICD-9-CM, Volume 3
D. HCPCS
9. Which of the following organizations is responsible for maintaining the ICD-9-CM Volumes 1 and 2 code set?

A. AMA  
B. ADA  
C. CMS  
D. FDA

10. Which of the following organizations is responsible for maintaining the CPT-4 code set?

A. AMA  
B. ADA  
C. CMS  
D. FDA

11. Which of the following organizations is responsible for maintaining the CDT code set?

A. AMA  
B. ADA  
C. CMS  
D. FDA

12. Which of the following organizations is responsible for maintaining the ICD-9-CM Volumes 3 code set?

A. AMA  
B. ADA  
C. CMS  
D. FDA
13. Which of the following organization is responsible for maintaining the NDC code set?

A. AMA  
B. ADA  
C. CMS  
D. FDA

Topic B - National healthcare identifiers

1. What are the different types of identifiers?

- National Provider Identifier (NPI)
- National Health Plan Identifier (Plan ID)
- National Employer Identifier for Health Care
- National Health Identifier for Individuals

2. What’s the significance of identifiers? For transaction require?

Identifiers are used extensively in all transactions between any combination of individuals, employers, health care providers, health plans, health care clearinghouses, and third party business associates. For example, every billing transaction will eventually require:

- The identifier of the provider submitting the claim
- The individual who received the care (currently on indefinite hold)
- The health plan to which the claim is sent for payment (likely not to be implemented until 2010; the industry is allowed a minimum of two years to implement any new HIPAA rule)
- The employer identifier, as applicable
3. List the types of identifiers typically associated with a physician.

Provider identifier and an employer identifier.

4. List the types of identifiers typically associated with an HMO.

Provider identifier, health plan identifier, and an employer identifier.

5. Describe the enumerator.

The enumerator refers to the CVS contractor organization that actually assigns the NPIs. The enumerator is also responsible for maintaining the NPPES database by entering the information sent by the providers or provider organizations (subparts) that have completed the screening successfully and have been assigned an NPI.

6. Describe the National Provider and Payer Enumeration System (NPPES).

The NPPES database is a central electronic enumerating and data storage system. HHS will implement the NPI and likely the PlanID through the NPPES.

7. Describe the National Employer Identifier for health care.

The National Employer Identifier for health care is the IRS-based Employer Tax Identification Number (TIN). The identifier is 9 digits in length and issued by the IRS.

Review Questions

1. What's a code set for HIPAA purposes, and what is it used for?

A code set is any set of codes used for data elements. A number of different code sets have been adopted under HIPAA. The primary purpose of the code sets is to standardize the identification of those things for which health care providers submit claims for reimbursement. These include:
• Medical diagnosis codes
• Medical procedure codes
• Medical concepts
• Medical supplies

2. What are the various code sets adopted to date to use with HIPAA-defined transactions?

Six code sets have been adopted under HIPAA:

• International Classification of Diseases, Clinical Modification (ICD-9-CM) Volumes 1 and 2
• Current Procedural Terminology, 4th Revision (CPT-4)
• Code on Dental Procedures and Nomenclature (CDT)
• ICD-9-CM, Volume 3
• National Drug Code (NDC)
• Health Care Common Procedure Coding System (HCPCS)

3. What's the HCPCS code set used to define?

The Health Care Common Procedure Coding System (Level II of HCPCS) is the code set that must be used to identify or describe health-related services that aren't physician services, dentist services, or hospital surgical procedures.

Codes include those services such as:

• Medical and surgical supplies
• Certain drugs
• Certain durable medical equipment (DME)
• Orthotic and prosthetic devices
• Procedures and services performed by non-physicians
4. What national identifiers have been adopted to date?

The national identifiers that have been adopted to date include the national employer identifier and the national provider identifier. The effective date for adoption of the national provider identifier was May 23, 2007.

5. When will the remaining identifiers be adopted for use by the healthcare industry?

The national health plan identifier adoption date is uncertain. CMS has announced the draft rule will likely not be published until 2008. The national patient identifier isn't likely to be adopted due to concerns raised by Congress and patients. It's on indefinite hold.

6. There are two types of national provider identifiers (NPI). What are they, and what are they used for?

The two different types NPI are the type 1 or individual NPI. It's assigned to covered (and in some cases non-covered providers) and remains their permanent identifier for the life of their business. The second type of identifier is the type 2 or subpart (sometimes called organizational) NPI. Providers can obtain one or more type 2 NPIs, and they're generally used to identify subparts of an organization that bill separately. They're primarily used in HIPAA-covered transactions to identify to whom the payment is to be made.
Chapter 5 - HIPAA and e-Health - Security and privacy requirements

Topic A - HIPAA, EHRs, and e-health

1. What are some key phases for your organization to consider as you plan and prepare for launching HIPAA initiatives?

- Awareness training
- Strategic planning
- Assessment
- Action
- Test and rollout

2. What's the purpose of the strategy phase?

This phase is about defining HIPAA strategy and determining a high-level program plan. Critical areas that need to be addressed include prioritized approach and budget costs. Also, accountability needs to be defined and accountable parties identified.

3. What's the purpose of the action phase?

This phase is about planning and developing policies and procedures so that initiatives, such as pilots, may be launched. Understand that HIPAA compliance requirements cause significant changes in policies, procedures, and processes within the organization in the handling of all PHI and individual records. This step requires planning for a compliant transactions model and solution for business operations and the development of IT security and privacy solutions, including the development of the policies and plans required.
Topic B - Planning for privacy compliance

1. What are some responsibilities of the HIPAA Privacy Officer?

The HIPAA Privacy Officer is responsible for overseeing ongoing activities related to the organization's policies and procedures covering the privacy of, and access to, all PHI in compliance with all federal and state laws and the health care organization's information privacy practices including the following:

- Development
- Implementation
- Maintenance
- Adherence

2. What are the questions that need to be asked to determine which organizations are possibly business associates of the enterprise?

The two questions that need to be asked as you determine which organizations are possibly business associates of the enterprise are:

- Does the entity provide business associate services for your organization?
- Which of these services require access to PHI?

3. What are the key steps for a small physician's office to comply with the Privacy Rule?

a) Site assessment
b) Gap analysis report
c) Remediation
d) Policies and procedures
e) Certification
Topic C - Planning for security compliance

1. What are the responsibilities of a HIPAA Security Officer?

A HIPAA Security Officer reviews, upgrades, documents, and implements the practice’s information security policies and procedures for the following areas:

- Access to information
- Confidentiality of information
- Physical security of information
- Disaster recovery and business continuity planning
- Security audit systems
- Information security and confidentiality training

A HIPAA Security Officer also:

- Prepares the practice's disaster recovery and business continuity plans for information systems breakdowns (both minor and major)
- Provides direct information security training to all employees, contractors, alliances, and other third parties, initiates, facilitates, and promotes activities to foster information security awareness within the organization

2. What are the deliverables or output of the gap analysis phase?

There are two deliverables from the gap analysis phase: HIPAA Security Strategy and Budget.

3. What's the objective of the baseline assessment phase? What areas are reviewed in the organization's environment?

In this phase, the objective is to establish the current state of the business. It essentially captures the organization's environment in the following specific areas:
• Business initiatives
• Processes
• Locations
• IT infrastructure
• Applications
• Skills and competencies

Topic D - Scenario: Possible framework for compliance

1. What are some key documents that need to be created as part of the Administrative Procedures Requirements of HIPAA's Security Rule?

The development of a security policy is a key HIPAA requirement. If encryption is to be deployed within the health care organization, then encryption-related security policy documents, such as descriptions of how and when encryption is to be used must also be created.

2. What's an example of a technique to secure access to data when it's sent over the enterprise network, from a physician to a pharmacy? What vendors provide a security solution for such access?

The technique to secure all such data is encryption. With encryption, access is limited to those who can decrypt the data. It's also possible to deploy security technology that enables organizations to encrypt documents or e-mail exchanges. One example is the use of encryption technology with products available from vendors such as Verisign, Microsoft, Entrust, CertifiedMail, and RSA Security.

3. What's the purpose of emergency access control? What must be the requirement for emergency access control in the security policy?

HIPAA requires that emergency access practices be implemented to allow access to needed information in the event the data owner is unavailable. Such emergency access requires that emergency access controls also be established to identify clearly when data have been accessed in the event of an emergency.
4. Is HIPAA an IT implementation issue?

HIPAA compliance is better focused as a business issue than as an Information Technology issue, although IT plays a major role in implementing compliant systems. HIPAA implementation is:

- Some technology challenge
- A large business process challenge

Review Questions

1. Review the requirements for the final Security Rule's Certification in Administrative Safeguards. Why would you possibly recommend an outside firm to provide the certification for a health care entity?

Certification is about each organization's being required to evaluate its computer system(s) or network designs to certify that the appropriate security has been implemented. It's important at least to involve an outside firm that has expert knowledge on HIPAA Security, as such a firm can determine if there may still be gaps that need to be closed. An outsider can be objective and its core focus is to look only at the infrastructure from a compliance perspective.

2. What's the objective of the Business Associate Contract?

The key objective is that the health care entity establishes a contract for each organization that it exchanges data with electronically, protecting the security of all such data.

3. What are some steps that must be considered before PHI is released to third parties?

These are the steps that need to be taken before PHI is released to third parties.

   a) Receiving the request
   b) Obtaining the patient's permission
   c) Reviewing of information requested
d) Preparing the information requested  
e) Sending the information requested

For questions 4 and 5, you need to pair up with one of your classmates. If the class has an odd number of students, one team of three needs to be formed.

4. Working with your partner(s), discuss the relationship between the Privacy Rule and the Security Rule. Identify areas that are possibly linked between the two rules.

The Privacy Rule is about PHI, and the Security Rule is focused on how to protect all data electronically. There’s definitely a relationship in several areas between the two rules. These include:

- Sanctions policy
- Training of all members of the workforce
- Development of agreements, such as BACs
- Termination policy
- Security policy (must address PHI as well as threats to data and infrastructure)

5. Working with your partner(s), discuss the flow of PHI within an organization. Now discuss the flow of PHI between that organization and another covered entity. What are some safeguards that you’d recommend that must be considered by the organization?

The organization must consider safeguards in the areas of:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

Also, what can’t be overlooked is adequate training for all employees so they understand PHI and patients’ rights. Finally, authorization and authentication are important considerations in terms of defining limited and controlled access to patient information.
6. During the ____________ phase, a detailed overall project plan first needs to be defined.

Assessment. Then, both business and system assessments need to be done.
Chapter 6 - HIPAA Privacy Rule

Topic A - Introduction to the Privacy Rule

1. In the contest of the HIPAA guidelines, what's privacy?

Privacy is defined as having policies and procedures in place to control access to PHI and assuring that those policies and procedures are regularly applied. The privacy regulation provides individuals with access to their medical records and ensures a level of control over how their personal health information is used and disclosed.

2. Who’s impacted by HIPAA privacy regulations?

The Privacy regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically, such as enrollment, billing, and eligibility verification. The Privacy Rule also extends to those who perform certain contracted functions for a covered entity.

3. What are the civil and criminal penalties for covered entities that misuse Protected Health Information (PHI)?

Civil penalties: Offenses for each requirement or prohibition violated will result in $100 per violation, up to $25,000 per year in fines. Criminal penalties:

- For certain offenses, up to $50,000 and/or up to one year in prison
- False pretenses, up to $100,000, and/or up to five years in prison
- Offenses committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain, or malicious harm up, to $250,000 and/or up to ten years in prison

4. What type of health information is governed by the Privacy Rule?

Any individually identifiable health information held by a covered entity is called Protected Health Information (PHI), regardless of the medium or format in which it exists.
5. What are the core requirements of the Privacy Rule?

- Provide individuals with certain privacy rights.
- Adopt written privacy policies, procedures, and contract provisions.
- Train employees and designate a privacy officer.
- Establish privacy safeguards

Review Questions

1. What's the purpose of the Privacy Rule?

The purpose of the Privacy Rule is to define privacy safeguards to protect the security and confidentiality of all health information, no matter the form, and require HIPAA covered entities to comply with the rule requirements.

2. The Privacy Rule creates national standards to protect individuals' medical records and other identifiable health information. What are some of the specific standards adopted to protect individual's medical records?

The Privacy Rule adopted the following standards:

- Individual control of health information
- Boundaries on use and release of health information by covered entities
- Establishment of policies, procedures, and appropriate safeguards to protect privacy
- Accountability for violations with civil and criminal penalties

3. Who's responsible for enforcing the privacy protections and access rights for consumers under Privacy Rule?

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR)
4. What are the limitations of Office for Civil Rights under the Privacy Rule?

The Privacy Rule limits OCR's access to information that's pertinent to ascertaining compliance. In some cases, no personal health information is needed. For instance, OCR might need to review only a business contract to determine whether a health plan included appropriate language to protect privacy when it hired an outside company to help process claims.

5. What are some of the key responsibilities covered entities need to attend to in an effort to avoid inappropriate release of protected health information (PHI)?

Some of the key privacy protections that need to be addressed include:

- Ensuring that health information isn’t used for non-health purposes
- Clear, strong protections against marketing
- Providing the minimum amount of information necessary
Chapter 7 - Privacy Rule - Organizational and individual relationships, rights, and responsibilities

Topic A- Organizational requirements and relationships

1. What are the types of organizational choices that may be available to a covered entity for the purposes of the Privacy Rule?

- Single covered entity
- Hybrid entity
- Affiliated covered entity
- Organized health care arrangement
- Jointly administered government program (for government entities only)

2. What is the difference between a trading partner and a business associate?

Trading partners perform clinical, medical, and health services functions (health plan and health care provider functions), functions that they perform whether or not a covered entity contracts with them. Most of these entities are also independently subject to HIPAA.

Business associates are persons or entities who are not employees of the covered entity who, on behalf of a covered entity, perform certain activities that involve the use or disclosure of PHI. A business associate is not a member of the covered entity's workforce. Covered entities are therefore required to obtain assurances that its business associates will appropriately safeguard all PHI held, accessed, used or created for those functions.

3. What are examples of workforce policies and procedures required by the Privacy Rule?

Non-retaliation, training, sanctions, and safeguards
4. List the services that define a business associate.

Examples of the services are: Legal, Actuarial, Consulting, Administration, Accreditation, Financial Services, Data Aggregation, Management, and Accounting.

5. What are the requirements of a business associate contract?

- Specify the PHI to be disclosed and the uses and disclosures that may be made of that information
- Limit use and disclosures of PHI as permitted by state or federal law
- Limit the use and disclosure of PHI to terms of the agreement
- Bind all BA agents and subcontractors to the same assurances in the contract
- Report all unauthorized uses and disclosures to your organization
- State that your organization will take "reasonable steps" to correct any misuse of PHI, including canceling the contract without penalty
- Impose security, inspection and reporting requirements on the business associate;

6. Give five examples of routine communications involving PHI

- Admissions > Third Party payers.
- Admissions > Patient Care Areas.
- Admissions > Patient Accounting Billing.
- Admissions > Internal "Hospital' Functional Departments
- Admissions > Information Services.

7. List some of the steps in an assessment.

- Create, maintain, and/or update a comprehensive list of all PHI
- Identify all known uses and disclosures.
- Identify and document the subset of PHI required to satisfy each activity, using minimum necessary except for treatment-related activities.
• Determine if any of the activities' information needs can be met using de-identified information, and if so, document.
• Define jobs or job categories for PHI access. Identify current access to PHI and justify.
• Identify and define the designated record set(s) in your organization
• Examine existing policies, procedures and training for documentation of all organizational decisions around use, disclosure, and protection of PHI
• Document any gaps for risk analysis and, where required, remediation.
• Build a project plan to remediate gaps
• Execute the plan.

Topic B - Individual Privacy rights

1. What are the individual privacy rights?

• Inspect and Copy. The individual has the right to inspect and obtain a copy of PHI in designated record sets.
• Amendment. The individual has the right to request an amendment of PHI in designated record sets.
• Authorization. The individual has the right to approve or deny a request for certain uses and disclosures of PHI, and to revoke that Authorization at any time.
• Accounting. The individual has a right to receive an accounting of certain disclosures of PHI.
• Restriction request. The individual has a right to request restrictions on certain uses and disclosures of PHI for TPO purposes.
• Alternate communications. The individual has the right to request certain alternate means of communications by the provider.
• Notice. The individual has the right to obtain a paper copy of the Notice of Privacy Practices from the provider upon request.
• Complaints. The individual has a right to submit a complaint to the covered entity or to the Secretary of HHS for any perceived violations of the Privacy Rule.
2. What is the designated record set?

Any PHI used by or for the covered entity to make treatment and payment decisions about an individual, regardless of the media or format in which it exists, is called the Designated Record Set (DRS).

3. What are the unreviewable grounds for denial of a request for an amendment?

Denials made in the following situations are not subject to review:

- If the information was not created by the covered entity, unless the originator of the information is no longer available to act on the amendment
- If the information is not part of the DRS
- If the information would not be available for access, such as for psychotherapy notes
- If the information is accurate and complete

4. Who is a personal representative?

A personal representative is an individual who is legally authorized to make decisions related to health care on behalf of an individual. For example, court-appointed guardians for non-competent adults or persons who have been granted power of attorney.

5. What are the parent's rights of access to children's health information?

In general, the Privacy Rule allows parents, as their minor children's representatives, to have access to information about the health and well being of their children when state or other underlying law allows parents to make treatment decisions for the child.

6. What are the exceptions?

- When the child can lawfully consent to or obtain a health care service and has not specifically requested that the parent act as the personal representative for that service
• When the parent agrees that the minor and the health care provider may have a confidential relationship, the provider is allowed to withhold information from the parent to the extent of that agreement.
• When the provider reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the provider is permitted not to treat the parent as the child’s personal representative with respect to health information.

Review Questions

1. **Differentiate between direct and indirect treatment relationships**

HIPAA considers direct treatment relationships to exist when the provider delivers health care without relying on the orders of another provider and communicates the results of diagnostic or other procedures directly to the patient. An example is the primary care physician or family practitioner.

2. **What is a Business Associate Contract?**

It is a written arrangement between the covered entity and its business associate to document that the covered entity has obtained satisfactory assurance that the business associate will appropriately safeguard the protected health information.

3. **What is an Organized Health Care Arrangement (OHCA)?**

It is an arrangement in which PHI may be shared for the purposes of joint management and operations among different health care providers.

4. **What are some examples of an individual's rights under the HIPAA Privacy Rule?**

Individuals are provided the right of access to inspect and obtain a copy of their own protected health information. This right of access does not extend to psychotherapy notes, to information compiled in reasonable anticipation of or for use in, a civil, criminal, or administrative action or proceeding. Individuals
also have the right to have a covered entity amend protected health information or record about the individual that are maintained by the covered entity, with limited exceptions.

5. Let’s say your client, as part of its standard business practices, discloses health information to its partners and business associates. How does HIPAA impact such disclosure?

In order to make disclosures of protected health information to a business associate, a covered entity must have in place a written Business Associate Contract (BAC) or written arrangement with the business associate to document that the covered entity has obtained satisfactory assurance that the business associate will appropriately safeguard the protected health information. Specific provisions in these contracts are required.

6. List some organizations that you believe may be a potential associate of a hospital.

This includes vendors, companies, and individuals that your enterprise conducts business with who may have access to PHI either for business purposes or inadvertently when providing a service.

7. For each of organization you listed for question 6, what service does the organization provide?

Answers will vary.

8. For each organization you listed in question 6, what is the PHI exposure and how is it accessed?

Answers will vary.

9. For each organization you listed in question 6, is a contract required?

Answers will vary.
Chapter 8 - Privacy Rule - Notice of Privacy Practices

Topic A - Notice of Privacy Practices and Authorizations

1. What are the core elements of a Notice?

   • Must be written in plain, simple language
   • Must prominently include specific language, the header of the Notice must read as follows: "This Notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review carefully."
   • Must describe the uses and disclosures of PHI
   • Must describe an individual's rights under the Privacy Rule
   • Must describe the covered entity's duties
   • Must describe how to register complaints concerning suspected violations of privacy rights with the entity
   • Must specify a point of contact
   • Must specify an effective date.

2. When must the Notice be provided?

   The first time an individual requests services, the Notice must be provided automatically and either on the initial contact or as soon as possible after the initial contact, if it isn't in person (such as by phone, via email, or on referral from another provider).

3. Can an individual revoke the Authorization verbally?

   No, the Authorization can't be revoked verbally. An individual must revoke it in writing.

4. What are the content requirements of an Authorization?

   Authorizations requested by individuals must contain the following minimum elements:
• Description of the information to be used or disclosed
• Name of the covered entity, or class of entities or persons, authorized to make the use or disclosure
• Name or types of recipient(s) of the information
• Expiration date
• Individual's signature and date of signature
• If signed by a personal representative, a description of the personal representative’s authority to act for the individual
• A statement regarding the individual's right to revoke the Authorization
• A statement that the information may be subject to re-disclosure by the recipient and no longer protected by the Privacy Rule

5. What's the difference between a Consent and an Authorization?

Consent under the Privacy Rule, refers to an optional Consent by an individual for the covered entity to use or disclose PHI for TPO purposes only. Authorization is the term used to describe a request for an individual to approve certain uses and/or disclosures of his or her health information.

Review Questions

1. What's the purpose of the notice of privacy practices (NPP)?

The notice of privacy practices is intended to educate patients and health plan members of their privacy rights under HIPAA, the privacy policies of the covered entity and clearly note when a patient or health plan member's protected health information (PHI) can/will be released without specific consent or authorization of the patient or health plan member.
2. If a covered entity makes significant changes to its NPP, what's the covered entity's responsibility?

   The covered entity is required to notify patients/health plan members of any significant changes to the covered entity's notice of privacy practices.

3. How frequently does a covered entity need to notify patients/health plan members that the covered entity's NPP is available?

   Covered entities are required to notify patients/health plan members of the availability of their NPP at least once every three years. (Health plans, under the Gram-Leach-Bliley Act, are required to send an NPP to all health plan members at least annually.)

4. What are the NPP requirements for covered entities that maintain a Web site?

   Covered entities that maintain a Web site are required to post the NPP prominently on the covered entity's Web site.

5. What are the covered entity's responsibilities regarding the content of the NPP?

   The covered entity is required to adhere to the privacy practices documented in the NPP. If the covered entity is unable to adhere reasonably to any of the practices included in the NPP, the covered entity is required to amend the NPP and notify patients/health plan members of the change, if it's significant.
Chapter 9 - Privacy Rule - Use and disclosures of PHI

Topic A - Uses and disclosures: General

1. Differentiate between Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI).

   - IIHI is created or received by a health care provider, health plan, employer, or clearinghouse.
   - IIHI relates to past, present, or future physical or mental health conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
   - IIHI identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Any individually identifiable health information held by a covered entity is Protected Health Information (PHI) regardless of the media or format it's in (electronic, paper, oral), and is the information governed by the HIPAA Privacy Rule.

2. What's the difference between use and disclosure?

Use refers to sharing, employing, applying, utilizing, examining, or analyzing IIHI by employees or other members of an organization's workforce. Information is used when it moves inside within an organization.

Disclosure is defined as the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. Information is disclosed when it's transmitted between or among organizations.

Under HIPAA, use limits the sharing of information within a covered entity, while disclosure restricts the sharing of information outside an entity holding the information. Both uses and disclosures are permitted or prohibited based on the purpose of the use or disclosure. Therefore, the Privacy Rule provisions apply to sharing PHI both internally within an organization and externally with other entities.
3. What are two methods to use or disclose health information other than as PHI?

- As de-identified information. De-identified information is no longer considered PHI and is not subject to the Privacy Rule. Therefore, it can be freely used and disclosed without conditions or restrictions.

- As a limited data set. A limited data set can be used only for research, public health, or other health care operations purposes and requires a data use agreement prior to disclosure.

4. Explain reasonable reliance.

In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that's needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency for a disclosure permitted under the Privacy Rule
- Another covered entity
- A professional who's a workforce member or business associate of the covered entity holding the information
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board

5. What's the minimum necessary determination to disclose to federal or state agencies?

Disclosure to federal or state agencies, such as, the Social Security Administration (SSA) or its affiliated state agencies must be authorized by an individual and, therefore, are exempt from the minimum necessary requirements.

6. What are all the conditions that may be associated with particular uses and disclosures?

- Minimum necessary
- Tracking disclosures
- Verification
• Agreements

7. Explain some policies and procedures to restrict the use of PHI.

Policies and procedures must be developed to restrict the use of PHI to the minimum necessary information for the performance of specific functions or duties. Policies must include procedures that:

• Identify the persons or classes of persons in the entity's workforce who need access to PHI to carry out their duties
• Identify the category or categories of PHI to which each person or class of persons needs access
• Identify the conditions that apply to such access

Topic B - Uses and disclosures: treatment, payment, and health care operations

1. What are the general rules for uses and disclosures for TPO?

• Treatment: Can share with any other provider (covered entity or not) to facilitate its own or the other provider's treatment activities. Minimum necessary doesn't apply.
• Payment: Can share with any other covered entity or any provider (covered entity or not) to facilitate its own or the other provider's payment activities. Minimum necessary does apply.
• Health care operations: Can share with any other covered entity to facilitate its own or the other covered entity's health care operations when the individuals whose PHI is involved have relationships with both entities. Minimum necessary does apply.

2. When do psychotherapy notes require an authorization for use or disclosure?

Psychotherapy notes require an authorization for all uses and disclosures except:

• For use by the originator of the psychotherapy notes for his/her own treatment activities
• For supervised training programs for its own mental health care professionals, trainees, and students
• To defend itself from a legal action brought by the individual
• For legal oversight of the originator of the notes
• When necessary to determine cause of death or when the subject of the notes poses a threat to public health and safety

3. What are other disclosures related to treatment where the individual must be given an opportunity to agree or object?

• For the facility directory
• Involving others in care and treatment
• Notification purposes
• Disaster relief

4. What are some examples of activities that are considered part of health care operations?

• Quality assessment and improvement activities, fraud and abuse
• Education and provider credentialing and certification
• Underwriting, rating, and other insurance-related functions
• Medical review, legal services, and auditing functions
• Business planning and development
• Business management and general administrative activities

5. What's marketing under Privacy Rule?

The Privacy Rule defines marketing as a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

6. What are the limitations on marketing communications?

If a communication is marketing, a covered entity may use or disclose PHI to create or make the communication in the following circumstances only:

• Kit's a face-to-face communication with the individual. For example, sample products may be provided to a patient during an office visit.
- If it involves products or services of nominal value. For example, a provider can distribute pens, toothbrushes, or key chains with the name of the covered entity or a health care product manufacturer on it
- Every other marketing activity requires an Authorization. Only activities that are defined as not marketing can proceed without an Authorization.

7. What are limitations on the use or disclosure of PHI for marketing?

The Privacy Rule requires the patient's Authorization for selling or disclosing PHI for marketing activities for example:

- Selling PHI to third parties for their use and reuse. Under the Privacy Rule, a hospital or other provider can't sell names of pregnant women to baby formula manufacturers or magazines.
- Disclosing PHI to outsiders for the outsiders' independent marketing use. Under the Privacy Rule, doctors can't provide patient lists to pharmaceutical companies for those companies' drug promotions.

8. Are there any exceptions to the disclosure of PHI for marketing?

Authorization for the use or disclosure of the PHI isn't required if:

- Made to describe a health-related product or service (or payment for such product or service) that's provided by, or included in a plan of benefits of, the covered entity making the communication
- As part of a provider's treatment of the patient and for the purpose of furthering that treatment.
- For conducting case management or care coordination for the individual.

**Topic C - Uses and disclosures: Public purposes**

1. List the permitted uses and disclosures under the Privacy Rule.

- Required by law
• Public health activities
• Health oversight activities
• Victims of abuse, neglect, or domestic violence (adult, elder, spouse)
• Judicial and administrative proceedings in response to court order or
• Law enforcement purposes
• About decedents to coroner, medical examiner, or funeral director
• Cadaveric organ, eye, or tissue donation
• Research
• To avert serious threat to health or safety
• For specialized government functions related to military, veterans, armed forces, and correctional
  institutions, and custodial situations
• Government programs providing public benefits
• Workers’ compensation

2. What's the rule for uses and disclosures required by law?

If there's a state or federal law that requires use or disclosure for any of the purposes above or for any
other purpose, then the covered entity must disclose. If there's no other law requiring that information be
used or disclosed, even for the permitted purposes listed above, covered entities must not disclose PHI
for these purposes without an Authorization.

3. What are public health officials' access rights to PHI?

The Privacy Rule allows disclosures that are required by law to public health officials to collect or receive
information for public health purposes regarding specific diseases. In order to do their job of protecting
the health of the public, public health officials frequently need to obtain information about the persons
affected by a disease. In some cases, they may need to contact those affected in order to determine the
cause of the disease to allow for actions to prevent further illness.
4. When are the conditions under which a covered entity is permitted to disclose PHI for abuse, neglect, or domestic violence?

If a covered entity discloses PHI about a person believed to be a victim of abuse, neglect, or domestic violence, the covered entity must promptly inform the individual of this disclosure except when the covered entity believes, in its professional judgment, that informing the individual would place him or her at risk of serious harm or, if informing a personal representative, when the covered entity believes, in its professional judgment, that the personal representative may be responsible for the abuse, neglect, or other injury, and that informing that person wouldn't be in the individual's best interest.

5. What are the rights and limitations of covered entities for use and disclose of PHI for research purposes?

In the course of conducting research, researchers may create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose PHI for research with individual Authorization, or without individual Authorization under limited circumstances set forth in the Privacy Rule.

6. Which two boards can grant a waiver of Authorization?

Privacy Board and Institutional Review Board (IRB)

7. What are the criteria for review for a waiver of authorization for a research study?

The following three criteria must be satisfied for an IRB or Privacy Board to approve a waiver of authorization under the Privacy Rule:

The use or disclosure of PHI involves no more than minimal risk to individual privacy based on the presence of the following:

- An adequate plan to protect identifiers from improper use and disclosure
• An adequate plan to destroy the identifiers at the earliest opportunity unless retention is justified or required by law
• Adequate assurances that PHI won’t be reused or disclosed other than as required by law, for authorized oversight of the research project, or for other research when the use or disclosure of PHI would be permitted by the Rule
• The research couldn’t practicably be conducted without the alteration or waiver
• The research couldn’t practicably be conducted without access to and use of the PHI

8. What are the differences in scope of responsibility between an IRB and a Privacy Board?

The scope of responsibility for an IRB review is much broader than that required under the Privacy Rule. The Common Rule requires IRB review for all research proposals under its purview, even if informed consent is to be sought. An IRB has the authority to approve, require modifications in (to secure approval), or disapprove research. An IRB review looks at the scientific benefit and validity of the research and assures, both in advance and by periodic review, that the rights and welfare of people participating in a research study are protected.

The Privacy Rule regulates only the content and conditions of the documentation that covered entities must obtain before using or disclosing PHI for research purposes. The Privacy Rule requirements are limited to evaluating requests for authorization waivers or authorization alterations for use and disclosure of PHI for a specific research project and assure adequate privacy protections are in place.

Review Questions

1. What are the conditions for uses and disclosures for treatment, payment, and health care operations under the Privacy Rule?

• Treatment Can share with any other provider (covered entity or not) to facilitate its own or the other provider's treatment activities. Minimum necessary doesn’t apply.
• Payment Can share with any other covered entity or any provider (covered entity or not) to facilitate its own or the other provider's payment activities. Minimum necessary does apply.
• Health care operations: Can share with any other covered entity to facilitate its own or the other covered entity’s health care operations when the individuals whose PHI is involved have relationships with both entities Minimum necessary does apply.

2. What are some of the permitted disclosures under the Privacy Rule?

• Required by law
• Public health activities
• Health oversight activities
• Victims of abuse, neglect, or domestic violence (adult, elder spouse)
• Judicial and administrative proceedings in response to court order or subpoena
• Law enforcement purposes
• About decedents to coroner, medical examiner, or funeral director
• Cadaveric organ, eye, or tissue donation
• Research
• To avert serious threat to health or safety
• For specialized government functions related to military, veterans, armed forces, and correctional institutions, and custodial situations
• Government programs providing public benefits
• Workers compensation

3. What are considered reasonable safeguards under the Privacy Rule?

Reasonable safeguards require security safeguards that provide administrative, physical, and technical safeguards that address the confidentiality, integrity, and availability of PHI. This applies to all PHI, no matter the form.

4. What's the difference between reasonable security safeguards under the Privacy Rule versus the Security Rule?
The Privacy Rule requires that reasonable security safeguards be implemented that protect all PHI, no matter the form. The Security Rule requires only that security safeguards be implemented for electronic PHI.
Chapter 10: Privacy Rule - Safeguards

Topic A - Safeguards

1. What are the general requirements for safeguards?

   - Covered entities must reasonably safeguard PHI—including oral information—from any intentional or unintentional use or disclosure that's in violation of the Privacy Rule.
   - Covered entities must have policies and procedures that reasonably limit access to and use of PHI to the minimum necessary given the job responsibilities of the workforce and the nature of their business.
   - Many health care providers already make it a practice to ensure reasonable safeguards—for instance, by speaking quietly when discussing a patient's condition with family members in a waiting room or other public area, and by avoiding using patients' names in public hallways and elevators.

2. What are the three types of safeguards?

   Administrative, physical, and technical.

3. What are some examples of administrative safeguards?

   Policies, procedures, and practices that minimize the likelihood of inappropriate use or disclosure of PHI. Administrative practices also include workforce training, monitoring workforce behaviors for compliance, the application of sanctions for failing to follow the policies and procedures, and mitigating harm to individuals impacted when a privacy breach occurs.

4. What are the minimum required standards for medical charts, X-ray light boards of empty prescription vials?

   The minimum necessary standards don't require that covered entities prohibit the maintenance of medical charts at bedside or that empty prescription vials be shredded or that X-ray light boards be
isolated. Covered entities must, in accordance with other provisions of the Privacy Rule, take reasonable precautions to prevent inadvertent or unnecessary disclosures.

Review Questions

1. What are the three types of safeguards that covered entities are required to implement to protect the privacy of protected health information (PHI)?

The three types of safeguards that must be implemented are administrative, physical, and technical.

2. What does the covered entity need to consider when establishing appropriate privacy safeguards?

The covered entity needs to consider the following when adopting appropriate safeguards:

- Reasonably safeguarding PHI from any intentional or unintentional use or disclosure that's in violation of the Privacy Rule, state law, and other federal law and adopted policies, procedures, and practices that may be more stringent than the Privacy Rule
- Drafting and implementing policies and procedures that reasonably limit access to and use of PHI to the minimum necessary given the job responsibilities of workforce members (employees, temporaries; contractors, and volunteers) and the nature of their business
- Establishing safeguards that address potential areas of exposure by requiring workforce members to speak quietly when discussing a patient's condition with family members in a waiting room or other public area and to avoid using patients' names in public hallways and elevators.
- Implementing safeguards to protect patient confidentiality.

3. The minimum necessary standard doesn't apply when exchanging PHI for what activity that doesn't require patient, health plan member consent or authorization?

Minimum necessary isn't required when PHI is exchanged for treatment purposes
4. The Privacy Rule allows for what are called incidental disclosures, as long as the appropriate safeguards have been established to keep them to a minimum. What are types of incidental disclosures?

Incidental disclosures of PHI include:

- Oral coordination of services by health care staff at hospital nursing stations
- Nurse’s and other health care professional's discussion of a patient's condition over the phone with the patient or a provider
- Health care professional's discussion of lab test results with a patient or other provider in a joint treatment area
- Health care professional's discussion of a patient's condition during training rounds in an academic or training institution
- Health plan customer service representative's and case manager’s conversations with plan members about claims, appeals, pre-authorization requirements, etc

5. What are considered appropriate physical safeguards?

Physical safeguards include applying physical barriers and controls to enhance protections, key management practices, assignment of workforce identification badges, secure (not visible or accessible to the public) placement of faxes, photocopiers, records, and computers used to process or display PHI, prohibiting taking paper or electronic records off site, facility contingency plan to be followed in the event of a disaster, and security guidelines when transporting laptops or other portable devices.
Chapter 11 - HIPAA Security Rule - Overview

Topic A - Scope of HIPAA Security Rule

1. What’s the scope of information that must be protected as a result of the final Security Rule?


2. What are the major sections of the Security Rule?

- Administrative safeguards
- Physical safeguards
- Technical safeguards

3. What are some factors guiding the philosophy behind HIPAA’s Security Rule?

The security standards are designed to be:

- Comprehensive — They cover all aspects of security safeguards.
- Technology-neutral — Standards can be implemented using a broad range of off-the-shelf and user-developed technologies and security solutions.
- Scalable — The goals of the regulations can be achieved by entities of all sizes from single practitioners to large multinational health care organizations.

4. Describe the major category areas covered by the final Security Rule under HIPAA that their organization needs to address for compliance.

The final Security rule outlines the requirements in three major categories:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
Topic B - Threats to business information

1. What’s a passive threat?

Passive threats are those that, if realized, don't result in any modification to any information contained in the system(s) and where neither the operation nor the state of the system changes.

2. What's an active threat?

Alteration of information or changes to the state or the operation of the system is defined as an active threat to a system. An example is modification of the routing tables of a system by an unauthorized user.

3. Describe a denial of service threat.

Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions. The attack may involve suppressing traffic or generating extra traffic. The attack may also disrupt the operation of a network, especially if the network has relay entities that make routing decisions based on status reports received from other relay entities.

4. Why is it important to understand and be aware of security threats?

Threats today have a real and immediate impact on business revenue and costs.

Topic C - Security terminology and categories

1. Define the term security.

Security is generally defined as having controls, countermeasures, and procedures in place to ensure the protection of information assets and control access to valued resources. Security is how an entity decides to protect its information assets.
2. What's the goal of security?

Generally, the goal of security is to counter identified threats and to satisfy relevant security policies and assumptions.

3. Define authentication.

Authentication is the process of proving your identity. A system needs to authenticate users to a degree appropriate for the level of risk/threat that an authenticated user represents.

4. Define access control.

Access control is assuring that only authorized users access a system, and that all unauthorized users are rejected.

5. Describe data confidentiality.

Data confidentiality is assuring the privacy of data on the system, and network data confidentiality protects your data from passive threats.

6. Describe data integrity.

Data integrity is the assurance that data hasn't been altered or destroyed in any unauthorized manner. Data integrity provides protection against active threats.

7. What's the objective of security mechanisms?

Both types of security mechanisms (specific and pervasive) implement security services.

8. What are some factors guiding the philosophy behind HIPAA's Security Rule?

The security standards are designed to be:
• Comprehensive—They cover all aspects of security safeguards.
• Technology neutral—Standards can be implemented using a broad range of off-the-shelf and user-developed technologies and security solutions.
• Scalable—The goals of the regulations can be achieved by entities of all sizes from single practitioners to large multinational health care organizations.

9. Describe the major category areas covered by the final Security Rule under HIPAA that an organization needs to address for compliance.

The final Security Rule outlines the requirements in three major categories:

• Administrative safeguards
• Physical safeguards
• Technical safeguards

10. What are the central principles of security?

Confidentiality, integrity, and availability.

Topic D - Administrative Safeguards

1. What are the nine standards defined within administrative safeguards?

• Security management process
• Assigned security responsibility
• Workforce security
• Information access management
• Security awareness and training
• Security incident procedures
• Contingency plan
• Evaluation
• Business Associate Contracts and other arrangements
2. **What’s a contingency plan?**

A contingency plan is one designed to respond to a system emergency. The plan includes performing backups, preparing critical facilities that can be used for the continuity of operations in the event of an emergency, and recovering from a disaster.

3. **What do sanction policies and procedures address?**

Sanction policies and procedures address statements regarding disciplinary actions that are communicated to all employees, agents, and contractors. Examples include:

- Verbal warning
- Notice of disciplinary action placed in personnel files
- Removal of system privileges
- Termination of employment
- Contract penalties

**Topic E - Physical Safeguards**

1. **What are the physical safeguard standards?**

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

2. **What are the implementation specifications of device and media controls?**

- Disposal
- Media re-use
- Accountability
- Data backup and storage
3. **What's the objective of accountability?**

The objective of accountability is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

**Topic F - Technical Safeguards**

1. **Describe technical safeguards.**

Technical safeguards refer to the technical solutions and the related policies and procedures for their use that protect EPHI and control access to it.

2. **Identify the five technical safeguard standards.**
   - Access control
   - Audit controls
   - Integrity
   - Person or entity authentication
   - Transmission security

3. **What's audit control?**

Audit control is about mechanisms employed to record and examine system activity.

4. **Define entity authentication.**

Entity authentication is a communications or network mechanism to identify, irrefutably, authorized users, programs, and processes and to deny access to unauthorized users, programs, and processes.
Topic G - Organizational requirements

1. Identify the required implementation specifications associated with the organizational requirement standard.
   - Business Associate Contracts
   - Other arrangements

2. What must the Business Associate Contract provide for?
   - The contract between a covered entity and a business associate must provide that the business associate:
     - Restricts access to and use by workforce performing plan administration functions
     - Establishes the uses and disclosures permitted and required by the plan sponsor and restricts further uses and disclosures
     - Reports to the covered entity any security incident of which it becomes aware
     - Authorizes termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract
     - Ensures that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it

3. What must the Group Health Plan provide for?
   - Ensure that the adequate separation required between the group health plan and the plan sponsor is supported by reasonable and appropriate security measures
   - Report to the group health plan any security incident of which it becomes aware
   - Reasonably ensure that no members of the workforce not directly involved in plan management have access to plan member information. This exclusion would cover human resources, business management, hiring managers, etc.
Topic H - Policies and procedures

1. Can a covered entity change its security policies and procedures at any time?

A covered entity may change its policies and procedures at any time, provided that the changes are documented and implemented in accordance with Security Rule requirements.

2. What are the implementation specifications of the documentation standard?

- Time limit (required)
- Availability (required)
- Updates (required)

3. What are some characteristics of a well-written security policy?

Well-written security policies:

- Are technology neutral
- Are relatively short, simple, and easily understood
- Should be high-level and not require frequent modifications
- Require formal approval and support from senior level management

4. What are some characteristics of a well-written procedure?

Well-written procedures:

- Can be technology specific
- Are sufficiently detailed to document every step in a process from start to finish
- Can walk a novice through the successful completion of a task
Review Questions

1. **What's the difference between vulnerability and a threat?**

Vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.

2. **What's data confidentiality?**

Data confidentiality protects data from passive threats and provides for the protection of data from unauthorized disclosure.

3. **The final Security Rule identifies security requirements in three major categories.**

Identify these categories.

- Administrative safeguards
- Physical safeguards
- Technical safeguards

4. **Identify the security principals that guided the development of the HIPAA security standards.**

The Security Rule consists of security standards that a health care entity must address to safeguard the confidentiality, integrity, and availability of its electronic data.

5. **Describe availability.**

Availability prevents the disruption of service and productivity.
Chapter 21

1. Which of the following is a Business Associate type added by ARRA?
   a. Data Aggregation services
   b. Security Management Outsource
   c. Electronic Pharmacy
   d. EMR/HER/Personal Health Record (PHR) vendors

2. Define “unsecured PHI”. (Both are required)
   a. Unencrypted electronic PHI, whether in motion or at rest.
   b. Paper-based PHI not shredded by cross-cut/diamond-cut device

3. What from the consumer’s point of view would be the most important aspect of Breach Notification communications?
   a. A brief synopsis of the event, including the date the event occurred and the date it was discovered
   b. What information was disclosed and to whom
   c. What the consumers affected should do for self-protection
   d. What the Covered Entity is doing about the event

4. A new audit program is expected from CMS OCR. When is it to be effective?
   a. 1Q of 2011
   b. 2Q of 2010
   c. 4Q of 2010
   d. 2Q of 2012

5. How far back will the EMR system be required to store disclosures prior to requests received from patients for accounting reports?
6. Personal health record (PHR) vendors:
   a. Are considered business associates if they provide PHRs or support PHRs on behalf of a covered entity
   b. Are now required to adhere to the HIPAA security rule and the use and disclosure provisions of the privacy rule
   c. Will be subject to new security rule to be developed by the Federal Trade Commission (FTC)
   d. None of the above

7. Disclosure accountings:
   a. Must include disclosures made for all purposes included treatment, payment and healthcare operations
   b. Only need to be documented for a three year period rather than a six year period
   c. Must be made available to individuals upon request and must be electronic
   d. From electronic health or medical records will need to include disclosures for all purposes

8. Marketing is considered healthcare operations as long as:
   a. The product or service marketed is the same as the patient is already taking or using
   b. Is of nominal value and provided in a face-to-face encounter
   c. Any compensation received by the covered entity is less than $1,000
   d. Marketing of services to patients or health plan members with certain conditions as determined from data analysis and through an appropriate vendor

9. There are four tiers of civil penalties associated with violations of increasing severity and the penalties are specifically set for each level of security or privacy rule violation.
   a. True
   b. False