HIPAA Compliance Training: Practice Questions

Chapter 1 – HIPAA Basics

A-1: Discussing HIPAA fundamentals

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. Business associates must also comply with all applicable provisions of the HIPAA privacy and security rules.

2 How does HIPAA impact covered entities?

HIPAA impacts covered entities by requiring the use of all applicable standard transactions while ensuring privacy and security wherever health information is stored, maintained, or transmitted. In summary, HIPAA requires covered entities to:

- Comply with standard transaction and code sets
- Use mandated national identifiers as required
- Use and disclose PHI only as required or allowed by law
- 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 establish safeguards and address availability, confidentiality, and integrity of protected health information (PHI)
• Train workforce members so that they understand the organization’s 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 individually identifiable health information so it isn’t readily available to those who don’t need it
• 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
• Ensure that patients and health plan members can exercise their rights regarding access to, amendment of, restriction of, use of, etc., their health information
• Follow breach assessment protocols when inappropriate disclosures occur and apply appropriate sanctions in all cases
• Document all compliance activities, policies, procedures, plans and actions
• Comply with all federal audits and investigations

Business associates are subject to many of the same requirements, although they are not required to comply with standard transactions unless their business function involves transactions. Business associates also tend to have little to no direct contact with patients for treatment purposes, so many of the individual rights provisions are less likely to apply. However, all provisions of the Security Rule and key elements of the Privacy Rule, such as adhering to appropriate uses and disclosures and to minimum necessary, are required for business associate compliance.

3 Outline the general HIPAA timelines for compliance.

The final HIPAA rules and regulations provide covered entities and business associates a specified period of time to reach compliance with the new provisions. Each published rule contains a timeline or timelines for compliance, with small health plans normally given a longer time to comply. While different provisions often have different time periods for coming into compliance, due dates are generally becoming shorter over time as the industry is expected to be fully in compliance at the time of the publication of new rule changes.

As HIPAA continues to evolve and provide more specific requirements and guidance, it is helpful to be aware of how rapidly changes to rules must be implemented. While the standard timeline is normally 180, the published timeline for each rule is the ultimate deadline, Enforcement provisions are usually immediately effective for any violations that occur after the final rule publication date.

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.
• Standardizes electronic, administrative, and financial health care transactions
• Creates unique health identifiers for employers, health plans, and health care providers, (likely not individuals)
• Sets industry security standards protecting the availability, confidentiality, and integrity of individually identifiable health information
• Ensures the privacy of protected health information with specific rules around how protected information can be used and shared
• Requires ongoing compliance project management, execution, testing, training, etc.
• Requires ongoing investment (staff, technology, resources, and fiscal) to maintain 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 reviewers
E HMOs
F Dentists
G Pharmacies

6 What’s a health care clearinghouse? Give some examples.

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
B-1: Discussing 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 Standards for Identifiers

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

Because health care business applications include a variety of functions such as patient scheduling, registration, clinical reporting, billing, and health insurance claims, which, when automated and seamlessly integrated, can improve both patient care and the bottom line. Healthcare business applications are also involved in the storage and movement of medical and claims information. The Administrative Simplification subtitle specifies standards for the electronic transmission of many common administrative and financial transactions previously performed on paper or using nonstandard electronic transactions. In addition, standards for protecting the privacy and security of patient and health plan member health information in electronic form are essential in an automated business environment.

To comply with HIPAA, all health care business applications must be secure and integrated into the health organization’s security infrastructure. These standards are the launch pad for e-business initiatives in health care. The HIPAA privacy rule, though, 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 common health care financial or administrative activities. Current transactions exist for the following types of 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
- Mobile device security
- Cloud computing

C-1: Discussing 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 $50,000 per violation and up to $1.5 million 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 $250,000 and/or imprisonment of not more than ten years.

D-1: Discussing HIPAA-related organizations

1 What’s the target audience of the NCPDP?

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 vendors
• 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 NCVHS 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)

E-1: Discussing 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. Business associates are also governed by and subject to many of the same obligations under HIPAA as covered entities.

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 personally 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 is a trading partner agreement?

A trading partner agreement is an agreement between two covered entities, usually a health plan and a provider, that governs exchanging standard transactions between the two entities. The
agreement may specify how to submit certain transactions. For example, the agreement may include specifics for submitting such as what situational information is required, whether to submit through a defined portal, whether to submit real-time vs. batch submission, whether to use a public or private health information exchange network, and other rules for processes necessary for exchanging standard transactions between the trading partners.

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 generally 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 needed access to PHI to perform the service. 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?

A business associate agreement is not normally required. However, if the hospital accesses PHI via a special Internet connection offered by the ISP in the course of its normal duties a business associate agreement may be prudent.

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

A business associate agreement is not normally required. 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 What are some exceptions to the business associate rules?

Exceptions involve conduits, 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, and may include some Accountable Care Organizations.

Review questions
1 The definition of the term workforce is important in the context 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 fits 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). Business associates are also directly subject to all of the HIPAA security provisions and several key privacy provisions.

3 What HIPAA rules have been finalized to date?

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
- National Health Plan Identifier Rule
- Enforcement Rule
- Breach Notification Rule
- Business Associate Privacy and Security Rules

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 intent and number of violations, ranging from $100 to $50,000 per violation with a maximum of $1.5 million 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 & code sets overview

A-1: Discussing transactions

1 What type of transactions do the transaction standards apply to? What’s the requirement for data storage and format?

The transaction standards apply only to electronic data exchange - 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 online, web-based transactions?

Internet transactions are being treated the same as other electronic transactions. However, while the format portion of the standard is often 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 is required under HIPAA.

A simple two-part test 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. If yes, the standard must 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 under HIPAA to conduct compliant transactions with entities that aren’t yet required to be in compliance because they aren’t conducting electronic transactions. However, other drivers, such as state law, insurer payment policy, and simplifying business processes to reduce costs, may require or strongly push a covered entity to conduct or require the
use of compliant transactions in all its business transactions. 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

A-1: Discussing ANSI ASC X12 standards

1 List the 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 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 disenrollment
• 270/271 – Eligibility inquiry and response
• 276/277 – Claims status inquiry and response
• 820 – Premium payment (can include EFT)
• 278 – Certification and authorization
Chapter 4 - Code sets & national identifiers

A-1: Discussing 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 sets.

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
- International Classification of Diseases, Clinical Modification (ICD-10-CM), Volumes 1 and 2
- Current Procedural Terminology, 4th Revision (CPT-4)
- Code on Dental Procedures and Nomenclature (CDT)
- ICD-9-CM, Volume 3
- ICD-10-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-10-CM Volumes 1 and 2
5 Which one of following code sets describes physician services or procedures?

A ICD-10-CM, Volume 3  
B CDT  
C CPT-4  
D HCPCS

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-10-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-10-CM, Volume 3  
D HCPCS

9 Which of the following organizations is responsible for maintaining the ICD-10-CM Volumes 1 and 2 code set?

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

A AMA
B ADA
C CMS
D FDA
E NCHS

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

A AMA
B ADA
C CMS
D FDA
E NCHS

12 Which of the following organizations is responsible for maintaining the ICD-10-CM Volumes 3 code set?

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

A AMA  
B ADA  
C CMS  
D FDA  
E NCHS

B-1: Discussing national health care identifiers

1 What are the different types of identifiers?

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

2 What’s the significance of identifiers? For example, what does every billing 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 requires:

- 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 (not required until 2016)  
- The employer identifier, as applicable

3 List the types of identifiers typically associated with a physician.
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 CMS contractor organizations that assign the NPIs, HPIDs, and OEIDs. The enumerators are also responsible for maintaining the NPPES and HPOES databases with the information sent by the providers, provider organizations (subparts), health plans, and sub health plans, and other entities that have completed the screening successfully and have been assigned the appropriate national identifier.

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

The NPPES database is a central electronic enumerating and data storage system that assigns the NPI and tracks information on providers with an NPI.

7 Describe the National Health Plan Identifier (HPID).

The National Health Plan Identifier is a number assigned by the CMS to the Health Plan and Other Entity Enumeration System (HPOES) to controlling health plans and sub health plans.

8 What issues are created by not having a national health identifier for individuals?

Lack of a national health identifier for individuals adds costs and complexity to matching up patient records from different providers, different payer networks, and from different states.

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 and ICD-10-CM) Volumes 1 and 2
- Current Procedural Terminology, 4th Revision (CPT-4)
- Code on Dental Procedures and Nomenclature (CDT)
- ICD-9-CM and ICD-10-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 are the national identifiers adopted under HIPAA?

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

The two different types NPI are 1) the individual NPI, and 2) the subpart NPI. The individual NPI is assigned to providers and remains their permanent identifier for the life of their business. The subpart NPI, which identifies a component of an organization that offers separate types of services and that can bill as a separate entity. Providers can obtain one or more subpart NPIs, and they’re generally used in HIPAA-covered transactions to identify to whom the payment is to be made.
Chapter 5 - HIPAA Compliance and e-Health

A-1: Discussing HIPAA and e-business

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
- Train, 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?

During this phase, plan and develop your policies and procedures, implement new technologies, revise your business processes, and conduct other projects and activities to operationalize your compliance decisions. This step may require implementing or modifying a compliant transactions solution for business operations and the development of IT security and privacy solutions, including development of all policies, procedures and plans required.

Understand that HIPAA compliance requirements, and any other e-health initiatives, may cause significant changes in policies, procedures, and processes within the organization and potentially between business partners and business associates in the handling of all PHI and individual records. Therefore, preparations with your workforce, such as training, and with your business partners, such as negotiating new or revised agreements and notifications of changes in your exchange protocol, should be determined and made before you “flip the switch” on a new technology, process, or procedure.
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?
- Do any of these services require access to PHI?

3 What are the key steps for a small provider to comply with the Privacy Rule?

a Site assessment and inventory
b Gap analysis
c Remediation
d Documentation
e Compliance

C-1: Discussing planning for security compliance
1 What are some 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, systems, and technologies
- Applications
- Skills and competencies
- Plans, policies and procedures
D-1: Discussing a 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:

- An organizational business challenge
- A large business process challenge
- A major documentation challenge
- A technology challenge
Review questions

1 Review the requirements for the 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 or business associate establishes a contract for each organization that uses PHI to conduct business on its behalf, assuring that the HIPAA security and privacy protections follow the 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)
- Safeguards
- Assigned responsibility

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 or business associate. 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

A-1: Discussing privacy

1 In the context of the HIPAA guidelines, what is 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 is 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. Portions of the Privacy Rule also extend directly to Business Associates and to those who perform certain contracted functions for either covered entities or business associates.

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 $50,000 per year in fines with a cap of $1,500,000 per year in each category.

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 media 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.
Chapter 7 - Privacy Rule – Organizational and individual relationships, rights, and responsibilities

A-1: Discussing organizational responsibilities 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 cancelling 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.
8 Which of the following relationships would qualify as a business associate?

- A food services vendor runs the employee and visitor cafeteria in a large hospital. It does not serve patients and no food service employees ever see patient PHI.
- A food services vendor operates the food services kitchen serving patients in a large hospital. It uses patient PHI to develop individual meals for patients on special or restricted diets, calorie or nutrition specific diets, or diets for those who have difficulties eating normally. Food service employees sometimes bring food to patient rooms when the hospital is short staffed.

B-1: Discussing 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.
- Electronic copies. The individual has the right to request an electronic copy of any PHI maintained electronically.
- 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.
- Notice of Breach. The individual has the right to be notified of any breach of her/his PHI.
- Restrictions on Self Pay Services. The individual has the right to request restriction on disclosure of information on self-paid services to a health plan.

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 noncompetent 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. An example of an indirect treatment relationship is with a testing laboratory or imaging facility.

2 What is a Business Associate Contract?

It is a written arrangement between the covered entity and its business associate, or between a business associate and its subcontractor(s), to document that the covered entity or business associate has obtained satisfactory assurance that the business associate or subcontractor 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 a provider, as part of its standard business practices, discloses health information to its trading 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. Trading partners do not require any contractual arrangements under HIPAA, although the provider may have business contracts with its trading partners to enable smooth business operations.

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 used?

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

A-1: Discussing 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 is not 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 cannot 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 be protected by the Privacy rule

2 What is 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 disclosure of 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 their health information.
Chapter 9 - Privacy Rule – Uses and Disclosures of PHI

A-1: Discussing Uses and Disclosures

1 What is the difference between use and disclosure?

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

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

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 to an organization as well as externally with other entities.

2 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 only be used for research, public health, or other health care operations purposes, and requires a data use agreement prior to disclosure.

3 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 is 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
4 What is 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, unless required by law, must be authorized by an individual and, therefore, are exempt from the minimum necessary requirements.

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

- Minimum necessary
- Tracking disclosures
- Verification
- Agreements

6 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

B-1: Uses and disclosures for TPO

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 does not apply.
• Payment: Can share with any other covered entity, business associate 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, the covered entity’s business associate or your business associate 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:

• 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 is 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:

- If it’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 patients’ Authorization for selling or disclosing the PHI for marketing activities for example:

- Selling PHI to third parties for their use and re-use. Under the Privacy Rule, a hospital or other provider cannot 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 cannot 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 is not required if:

- Made to describe a health-related product or service (or payment for such product or service) that is 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.

C-1: Discussing permitted uses and disclosures

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 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

2 What is the rule for uses and disclosures required by law?

If there is 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 is 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 the 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, it is frequently necessary for public health officials 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. Public health authorities may also have law enforcement or other special powers under certain emergency circumstances where health risks can rise dramatically.

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 them 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 would not 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 will not be reused or disclosed other than as except 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 could not practicably be conducted without the alteration or waiver
• The research could not 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 does not 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
Chapter 10 - Privacy Rule – Safeguards

H-1: Discussing safeguards

1 What are the general requirements for safeguards?

- Covered entities and business associates must reasonably safeguard PHI—including oral information—from any intentional or unintentional use or disclosure that is in violation of the Privacy Rule.
- Covered entities and business associates must adopt and implement written 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. 20140213
- Encryption of all ePHI either at rest or in transition with particular attention paid to laptops, USB drives or other portable devices.

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 behaviours 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

4 It is not a HIPAA violation for an employee to post a patient image on social media provided the patient’s face is not shown.

a. True

b. False
5 What are the acceptable methods for destroying PHI?

- Paper, film, or other hard copy media must be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

6 If you were audited by OCR, describe how you would prove that your chosen safeguard are reasonable for your business environment.

We would provide documents describing our process for decision making and showing how they are appropriate for our organization’s risks as identified through a recent comprehensive risk assessment. We will show that cost was not a major factor in determining appropriate safeguards.
A-1: Discussing the scope of the 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
B-1: Discussing 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. Denial of service is a common way to disable targeted websites.

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, on customer and personal privacy and security, and on national security.

C-1: Discussing security terminology

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.

D-1: Discussing 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

Sanction policies also include carrying out and documenting appropriate sanctions in response to violations of the HIPAA security provisions.

E-1: Discussing 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.

F-1: Discussing 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.

G-1: Discussing 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 or a business associate and its subcontractor 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.

H-1: Discussing policies and procedures, and documentation standards

1 Can a covered entity or business associate change its security policies and procedures at any time?

A covered entity or business associate 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.

6 What two documents inform the HHS guidance on risk assessment?

NIST SP 800 66, An Introductory Resource Guide to Implementing the HIPAA Security Rule

NIST SP 800 30 Risk Management Guide for Information Technology Systems
A-1: Discussing security threats

1 What’s a denial of service (DoS) attack?

Denial of service (DoS) attacks can be disruptive for any organization. In a DoS attack, the attacker doesn’t gain unauthorized access to a resource; instead the hacker’s action leads to the loss of access to a resource. The resource may be the network, CPU, memory, or disk. A DoS attack results in overload of a resource, such as disk space, network bandwidth, internal tables of memory, or input buffers (buffer overflow). The overload causes the host or particular service to become unavailable for legitimate use. This could be anything from blocking access to a resource to causing a host to crash.

2 What’s DNS spoofing?

In DNS spoofing, the hacker compromises the Domain Name System (DNS) server and explicitly alters the hostname to IP address table.

3 What’s a Telnet type of an attack?

A Telnet attack captures and uses usernames and passwords for applications, such as Telnet and the File Transfer Protocol (FTP), that support username/password-based authentication.

B-1: Discussing security technology options

1 What are some examples of defence-oriented security technology solutions?

Examples of defence-based security technologies include:

- Firewall systems
- Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS)
2 What are some examples of trust-oriented security technology solutions?

Examples of security technologies that enable trust include:

Encryption
- Public Key Infrastructure (PKI)
- Device encryption

Strong Authentication
- Biometrics
- Authentication tokens
- Smart cards

3 What has impeded the health care industry with regard to security?

- Limited technology budgets
- Multiple proprietary systems
- Multiple legacy systems
- Paper-based processes

Review questions

1 What are some characteristics of a good password policy?

A good password policy typically requires:

- Passwords of a minimum length (six to eight characters)
- Combinations of alphanumeric characters and symbols
- Users to change their passwords every 30 to 60 days
- Users not to be able to select previously used passwords

2 Identify examples of strong authentication mechanisms.

The two addressable implementation specifications of the Transmission Security standard are integrity controls and encryption.
Chapter 13 - Advanced administrative safeguards

A-1: Discussing security awareness and training

1 What’s the objective of the Security Awareness and Training standard?

The objective of the Security Awareness and Training standard is to implement a security awareness and training program for all members of its workforce (including management).

2 What implementation specifications are associated with this standard?

The implementation specifications for the Security Awareness and Training standard include:

- Security reminders (addressable)
- Protection from malicious software (addressable)
- Login monitoring (addressable)
- Password management (addressable)

3 What’s a virus? Identify the types of viruses.

A virus is a program that attaches itself to files on a target system. During attachment, the virus’ original code appends to victim files. This attachment is referred to as infection. At this point, when the file is infected, it’s converted from an ordinary file to a carrier. This infected file can infect other files, a process referred to as replication. The replication of files can spread across to the hard disk leading to systemic infection.

There are basically three types of virus:

- Master boot sector viruses
- Boot sector viruses
- File viruses

4 What’s a Trojan horse?
A Trojan horse performs functions unknown to the end user, as unauthorized code contained within a legitimate program. It may also be a legitimate program that has been altered by the placement of unauthorized code within it and performs functions unknown to the end user. The Trojan horse program does something more than what’s expected by the end user and typically results in some damage or transmission of information that’s sensitive, such as the e-mailing the password file.

5 What’s a worm?

A worm is a self-contained program that remotely uses security flaws, such as a buffer overflow, to compromise a system and then replicates itself to that system. Unlike viruses, worms don’t infect other executable programs, but instead install themselves on the victim system as a standalone entity that doesn’t require the execution of an infected application.

6 What’s phishing?

Phishing is the act of impersonating a trusted entity, such as a bank or health care system, to collect confidential or sensitive (usually personal) information via e-mail. Personnel should be warned that such trusted entities never contact them via e-mail, and that they should never provide any information other than by contacting the entity via trusted contact information (e.g., the Customer Support phone number on the back of a credit card).

B-1: Discussing security incident procedures

1 What’s the objective of the Security Incident Procedures standard?

The objective of the Security Incident Procedures standard is to implement policies and procedures to address security incidents. Security incident procedures are formal documented instructions for reporting security incidents.

2 Describe security incident response procedures.

Response procedures are documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report. The procedures are formal, documented instructions for reporting security incidents, so that security violations are reported and handled promptly.
3 What’s the key objective of perimeter security?

The key objective of perimeter security is to detect, prevent, and respond to threats. These capabilities are critical for a health care entity’s perimeter defense, especially detection and response.

C-1: Discussing contingency planning

1 What’s a contingency plan?

A contingency plan is one for responding to a system emergency. The plan includes performing backups and preparing critical facilities that can be used to facilitate continuity of essential business operations in the event of an emergency and recovery from a disaster.

2 What are the two key elements of a data recovery plan?

The two key elements of a data backup plan are recovery period and recovery point. The recovery period represents the time an organization needs to retrieve, load, and test backups and, potentially, to replace hardware and, therefore, to restore business operations. The recovery point represents the period of time that has transpired between the disaster and the most recent backup.

3 What’s a disaster recovery plan?

A disaster recovery plan is part of an overall contingency plan that contains a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. It’s important to invest in relatively realistic testing of a disaster recovery plan. Build this effort into budgets and schedules.

4 Describe emergency mode operations plan.

An emergency mode operations plan is part of an overall contingency plan that contains a process enabling an enterprise to continue to operate critical business functions in the event of fire, vandalism, natural disaster, or system failure.
5 What’s the key objective of testing and revision procedures?

These are procedures for the documented process of periodic testing of written contingency plans to discover gaps and weaknesses and the subsequent process of revising the documentation, if necessary. These written testing and feedback mechanisms are the key to successful testing.

D-1: Discussing the evaluation standard

1 What’s the objective of the Evaluation standard?

The objective of the Evaluation standard is to perform a periodic technical and nontechnical evaluation, based, initially, upon the standards implemented under this rule and, subsequently, in response to environment or operational changes affecting the security of EPHI, which establishes the extent to which an entity’s security policies and procedures meet the requirements of this subject.

2 Who would conduct such an evaluation?

The evaluation may be performed internally or by an external accrediting agency, which would be acting as a business associate. The evaluation would be of both technical and non-technical components of security.

E-1: Discussing BACs and other arrangements

1 Can a covered entity or business associate permit a business associate or subcontractor to process EPHI?

A covered entity or business associate can permit a business associate or subcontractor to create, receive, maintain, or transmit EPHI on the covered entity’s behalf only if the covered entity or business associate obtains satisfactory assurances that the business associate or subcontractor will appropriately safeguard the information.

2 What types of transmissions aren’t covered under the BACs and Other Arrangements standard?
This standard doesn’t apply to:

- The transmission by a covered entity of EPHI to a health care provider concerning the treatment of an individual.
- The transmission of EPHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor.
- The transmission of EPHI from or to other agencies providing the services when the covered entity is a health plan that’s a government program providing public benefits.

Review questions

1 Describe the objective of the Information System Activity Review implementation specification.

The Information System Activity Review implementation specification requires covered entities and business associates to implement procedures to review, regularly, records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2 Describe the Sanctions Policy implementation specification.

The Sanction Policy implementation specification requires covered entities and business associates to apply appropriate penalties against workforce members who fail to comply with the security policies and procedures of the entity. A sanction policy addresses statements regarding disciplinary actions that are communicated to all employees, agents, and contractors.

3 Describe a worm.

A worm is a self-contained program that uses security flaws, such as a buffer overflow, to compromise a system remotely and then replicate itself to that system. Unlike viruses, worms don’t infect other executable programs, but instead install themselves on the victim system as a standalone entity that doesn’t require the execution of an infected application.

4 Describe the Applications and Data Criticality implementation specification.

For the Applications and Data Criticality Analysis implementation specification, covered entities and business associates should assess the relative criticality of specific applications and data in support
of other contingency plan components. It’s an entity’s assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits. This procedure begins with an application and data inventory.

5 Identify the addressable implementation specifications of the Contingency Plan standard.

- Testing and Revision Procedures
- Applications and Data Criticality Analysis
Chapter 14 - Physical safeguards overview

A-1: Discussing Privacy Rule physical safeguards

1 Identify some policy requirements for workplace practices for paper records.

Some policy requirements for paper records include:

- Storing files and documents in locked rooms or storage systems
- Safeguarding confidential information by staff when lockable storage isn’t available
- Ensuring that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labelled and disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
- Ensuring that files and documents are shredded on a timely basis, consistent with record retention requirements.

2 When protecting oral confidential information, what types of locations have low risk, medium risk, or high risk for accidental disclosure?

- Low risk—interview rooms, enclosed offices, and conference rooms
- Medium risk—employee-only areas, telephones, and individual cubicles
- High risk—public areas, reception areas, and shared cubicles housing multiple staff where clients are routinely present

3 What does the safeguards plan identify?

The safeguards plan identifies the steps that must be taken to improve the work environment. Some important areas to address in this plan are:

- Reception
- Pedestrian traffic
- Electronic document storage
- Electronic document destruction
- Workstations, printers, monitors, and faxes
Chapter 15 - Advanced physical safeguards

A-1: Discussing requirements

1 What are physical safeguards?

Physical measures, policies, and procedures to protect a covered entity’s or business associate’s electronic information systems, and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

2 What are the physical safeguard standards?

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

3 What are the types of security questions addressed by physical safeguards?

- Is access to the building controlled?
- Is access to the computing facility controlled?
- Are there additional controls required for access after-hours?
- Is there an audit log that records the individual, the location of access, and the time of access?
- Are systems adequately protected from theft?
- Are procedures in place to dispose of confidential information adequately per HIPAA requirements?
- Are workstations secured after hours?
- Are the activities of the cleaning crew monitored?
- Has a plan been developed and tested for operating under an emergency?
- Are mobile devices (e.g. laptops, cell phones, flash drives, tablets) inventoried, tracked, and adequately secured in case of loss or theft?
- Are data backups sent to an offsite location for safe storage?
- Have procedures been developed for the testing and revision of applications and systems?
• Are members of the workforce trained on key security issues?

B-1: Discussing facility access controls

1 What’s the objective of the Facility Access Controls standard?

The objective of this standard is to implement policies and procedures to limit physical access to an entity’s electronic information systems and the facility or facilities in which they’re housed, while ensuring properly authorized access.

2 What are the implementation specifications for the Facility Access Controls standard and are they addressable or required?

- Contingency operations (addressable)
- Facility security plan (addressable)
- Access control and validation procedures (addressable)
- Maintenance records (addressable)

C-1: Discussing workstation use and security

1. What’s the objective of Workstation Use standard?

The objective of the Workstation Use standard is to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.

2 What’s the objective of the Workstation Security standard?

The objective of the Workstation Security standard is to implement physical safeguards for all workstations that access EPHI and restrict access to authorized users only.
1 What is the objective developing a sound physical security program?

The objective of developing a sound physical security program is to reasonably ensure physical assets and access to those assets are protected from inappropriate use or access. Also, it establishes a plan to address operations and recovery in the event of a disaster.

2 What represents the greatest threat to the physical security of a covered entity or business associate?

The workforce represents the greatest risk to the physical security of a covered entity or business associate.

3 What are the types of access control?

The two types of access control are role-based and time-based access control.

4 What does HIPAA require in the event of a disaster where a facility is unusable or partially unusable?

HIPAA requires the creation of a contingency plan that covers disaster recovery (returning the operation to normal operations as soon as feasible) and the ability to perform mission critical operations during the recovery process (emergency mode operations).

5 Why are maintenance records important?

Maintenance records are important because they provide documentation that appropriate maintenance is being performed, documents maintenance has been authorized and completed appropriately, documents related policies and procedures (key and lock changes, alarm maintenance, maintaining secure locations within the organization, etc.) are followed/enforced.
Chapter 16 - Physical safeguards – Device and Media Management

A-1: Discussing Device and Media Controls

1 What is the objective of the Device and Media Controls standard?

The objective of the Device and Media Controls standard is to implement policies and procedures that govern the receipt and removal of hardware and electronic media and devices that contain EPHI into and out of a facility, and the movement of these items within the facility.

2 What are the implementation specifications of the Device and Media Controls standard?

The implementation specifications of the Device and Media Controls standard are:

- Disposal (Required)
- Media Re-use (Required)
- Accountability (Addressable)
- Data Backup and Storage (Addressable)

3 Discuss data back up and its objectives.

Continual and consistent backup of data is required as one cannot be sure when an organization may experience some disaster that will require access to data that has been backed up to be back in operations. Data may also be lost or corrupted—as a result, a good data backup plan is important.

The objective of a data backup plan is to be able to retrieve an exact copy of information. Also, the testing of data recovery processes is an integral part of the data backup process. If the data cannot be recovered from backup medium, it renders the whole data backup process ineffective.

4 What are some examples of questions addressed by data storage?

Data storage addresses questions such as:
- Where will the media be stored?
- What is the media-labelling scheme?
- How quickly will data need to be recovered in the event of an emergency?
- How long will data be retained?
- What is the appropriate media type used for backup?
Chapter 17 - General technical safeguards

A-1: Discussing requirements

1 What is the purpose of technical safeguards?

Technical safeguards refer to the technology and the policy and procedures for its use that protect e-PHI and control access to it.

2 Identify the Technical Safeguard standards.

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

3 What types of permissions are typically supported by operating systems for access control?

Operating systems support Access Control Lists (ACLs) to determine permissions to specific files, directories and applications such as:

- Read
- Write
- Execute
- No access

4 How can information be secured between a client system and a Web site?

When information needs to be encrypted between a client and a Web site, a Secure Sockets Layer (SSL) session can be established between the two ends to ensure encryption of information transmitted over the channel.
5 What is the benefit of using a PKI with a VPN?

A PKI can generate certificates for Virtual Private Network (VPN) devices. This ensures a solution that supports encryption and authentication—both working together.

B-1: Discussing Access Control

1 What is the objective of the Access Control standard?

The objective of the Access Controls standard is to implement technical policies and procedures for electronic information systems that maintain e-PHI to allow access only to those persons or software programs that have been granted access rights.

2 Identify the Access Control implementation specifications.

The implementation specifications of the Access Control standard are:

- Unique User Identification (required)
- Emergency Access Procedure (required)
- Automatic Logoff (addressable)
- Encryption and Decryption (addressable)

3 What is the objective of Encryption and Decryption?

The objective of Encryption and Decryption is to implement a mechanism to encrypt and decrypt electronic protected health information. The use of file encryption is an acceptable method of denying access to information in files or directories. Encryption provides confidentiality, which is a form of control. The use of encryption for the purpose of access control of data at rest should be based upon an entity’s risk analysis.

C-1: Discussing Audit Controls

1 What is the objective of the Audit Controls standard?
The objective of the Audit Controls standard is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI.

2 What are some reasons to generate log entries or alerts?

There are at least three (and possibly a fourth) reasons to generate log entries or alerts:

- Legal mandate / fiduciary responsibility
- In support of a broader risk management program
- In support of monitoring and capacity management activities and, depending on overall system architecture
- Transaction rollback or back out

3 What are some examples of audit control events?

Audit control events include (but are not limited to):

- Traffic passing inbound through the external firewall is logged whenever it is directed at the VPN server
- All attempts (unsuccessful or successful) to communicate with the VPN server
- Notice and details of all successful VPN tunnel session establishment
- All “new” communications from the VPN server that attempt to communicate across the internal firewall
- All details of all attempts (unsuccessful or successful) to communicate with the authentication server
- High-level details of all attempts to communicate with the LDAP directory server
- All server platform local user and remote user logons
- All server platform local user and remote user session command details
- All server platform configuration changes

D-1: Discussing the Integrity standard

1 What is objective of the Integrity standard?
The objective of the Integrity standard is to implement policies and procedures to protect e-PHI from improper alteration or destruction.

2 What is the implementation specification for the Integrity standard?

The implementation specification defined for the Integrity Standard is: Mechanism to Authenticate Electronic PHI (addressable).

E-1: Discussing Person or Entity Authentication

1. What is the objective of the Person or Entity Authentication standard?

The objective of the Person or Entity Authentication standard is to implement procedure to verify that a person or entity seeking access to e-PHI is the one claimed.

2 Identify authentication solution options.

Fast emerging authentication solutions include:

- Tokens
- Smart cards
- Biometrics

3. What are some examples of biometrics technologies?

- Fingertips
- Facial recognition
- Retina scanning
- Iris scanning
- Hand geometry
- Voice patterns

Review questions
1. The objective of the ___________ Control standard is to implement technical and administrative policies and procedures for electronic information systems that maintain e-PHI to allow access only to those persons or software programs granted access rights.

Access

2. The objective of the ___________ Controls standard is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI.

Audit

3. Which standard is meant to protect e-PHI from improper alteration or destruction inside the organization and when data is transmitted?

A. Audit control
B. Transmission security
C. Integrity
D. Access control

4. Which type of access control places users in groups based on what actions they need to perform on the system?

A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Context-based access control

5. True or false? It is required that every user have a unique number or name for the purpose of tracking system use.
6 For the Automatic ______________ implementation specification, covered entities should address implementing electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Logoff

7 Typing a username and a password is an example of _____________ an individual or an entity as an authorized user on the network.

Authenticating
Chapter 18 - Advanced technical safeguards

A-1: Discussing Transmission Security

1 What is the objective of the Transmission Security standard?

The objective of the Transmission Security standard is to implement technical security measures to guard against unauthorized access to e-PHI that is being transmitted over an electronic communications network.

2 Identify the Transmission Security implementation specifications.

The Transmission Security standard includes the following implementation specifications:

- Integrity Controls (addressable)
- Encryption (addressable)

B-1: Discussing TCP/IP network infrastructure

1 What are the layers in the TCP/IP architecture?

There are four layers in the Internet (TCP/IP) architecture:

- Network Access
- Internet
- Transport
- Session

2 Identify the key lower layer TCP/IP protocols.

Lower layer protocols include:

- IP
- TCP
C-1: Discussing firewalls

1 What's a firewall system?

A firewall is one or more systems that may be a combination of hardware and software and that serve as a security mechanism to prevent unauthorized access between trusted and untrusted networks. Firewall systems are typically the first line of defense between an organization's internal network and its connection to the Internet.

2 Describe a firewall proxy.

A firewall proxy accepts traffic destined for the other side of the firewall and examines the higher-level details of specific application communications, then either passes valid traffic along to the intended destination or drops (or rejects/denies) malicious or otherwise inappropriate activity.

D-1: Discussing Virtual Private Networks (VPNs)

1 What are some key elements that need to be considered for securing a VPN?

Securing a VPN must include the following key elements:

- Authenticity of end points: Security of the VPN tunnel requires that its end points are authentic. This implies accuracy within the authentication mechanism employed.
- Data integrity: Must ensure that data aren't modified while in transit from one location to another.
- Secure management of tunnel: Must be able securely to manage the establishment and operation of a VPN tunnel.

2 What are some examples of VPN tunnelling protocols?

The major tunnelling protocols for VPNs are:
• Point-to-Point Tunnelling Protocol (PPTP)
• Layer 2 Tunnelling Protocol (L2TP)
• IP Security Protocol (IPSec)

E-1: Discussing wireless transmission security

1 What functions are supported by handheld devices?

Handheld devices facilitate at least three activities in the area of mobile health care (m-health) applications. These are:

• Accessing information
• Recording information
• Transmitting/communicating information

2 What are two key areas of risk with wireless networks?

• Access control
• Privacy

3 What’s a possible solution for physicians and medical professionals that want to use handhelds?

A possible solution for physicians and medical professionals using handhelds is to design an architecture for wireless communications where the handhelds function as dumb terminals. In this scenario, a series of Web servers, which take data from all the hospital’s computer systems, handling tasks, such as billing and test results, and convert the information into standard Web pages. The Web servers also store the digital patient files as Web documents. The digital files may include photos and videos of procedures. Further, the bedside information is entered on PDAs using a combination of on-screen forms and either a small add-on keyboard or a shorthand handwriting program that works with PDAs.

Using this architecture of wireless organizers that link with the servers substantially reduces the vulnerability of information on PDAs. The PDAs, acting as dumb terminals, immediately send the information to servers for storage. In this solution, the memory of the PDAs must be then cleared so that there’s no possibility of that information being used in an unauthorized manner.
4 What are some factors to consider before deploying wireless technology for a health care infrastructure?

- Operating platforms vary considerably. Carefully research and determine if the Mobile Healthcare Computing Device (MHCD) for your organization needs to be a Palm, an iPad, or a BlackBerry handheld type solution.
- Consider your data security needs before you deploy. The default settings might not be adequate for companies that handle confidential information.
- Consider the HIPAA Proposed Security Rule requirements for physical safeguards, technical security services, and mechanisms, and especially review closely authentication- and access control-related specifications.
- Don’t install access points without investigating whether they’re properly placed. Plan on extensive testing.
- Don’t assume your IT staff are knowledgeable about wireless networking. Make sure that the people who install and manage your networks are aware of wireless networking’s unique configuration issues.

F-1: Discussing encryption

1 Describe symmetric cryptography.

Symmetric cryptography is an encryption system that uses the same key to encrypt and decrypt. The secrecy of encrypted data depends solely on the secrecy of the secret key, also referred to as the private key.

2 What are some examples of symmetric key algorithms?

Examples of symmetric key algorithms are:

- Advanced Encryption Standard (AES)
- Triple DES (3DES)
- International Data Encryption Algorithm (IDEA)

3 Describe asymmetric cryptography.
Asymmetric key encryption is an encryption system that uses a linked pair of keys—a public key and a private (secret) key. What one pair of keys encrypts, the other pair decrypts. The public key is publicly available and is usually embedded in digital certificates.

4 What are some examples of asymmetric key algorithms?

Examples of asymmetric key algorithms are:

- RSA
- Elliptic Curve Cryptosystem (ECC)
- Diffie-Hellman

5 Describe a message digest.

A message digest takes a message of any size input and outputs a short, fixed-length code. The output is typically 16 to 20 characters, depending on the type of message digest algorithm used. The message digest is unique to the message. The message digest depends on every bit of the message and its attachments. A message digest is like a fingerprint of the message. Message digests are also referred to as digital fingerprints, cryptographic hashes, or cryptographic checksums.

6 What are some commonly used message digests?

Commonly used message digest-generation programs are:

- MD4 and MD5 from RSA Security (128 bits or 16 characters)
- SHA-1 (Secure Hash Algorithm) from the National Institute of Standards and Technology (NIST) (160 bits or 20 characters)

G-1: Discussing Kerberos authentication

1 What are the three heads of Kerberos?

- Key Distribution Center (KDC)
- Client user
- Server with desired service to access
2 In a Windows 2000 environment, what services are performed by the Kerberos KDC?

The KDC is installed as part of the domain controller in Windows 2000 and performs two service functions:

- The Authentication Service (AS)
- The Ticket-Granting Service (TGS)

H-1: Discussing Windows XP security

1 What are the ways to use software restriction policies in an XP environment?

There are two ways to use software restriction policies.

- If administrators have identified all the software that should be allowed to run, they can use a software restriction policy to limit execution to only that list of trusted applications.
- If administrators don’t know about all the applications their users will run, they’ll have to be reactive and restrict inappropriate applications as they’re identified.

2 What security templates does Security Configuration Manager support in an XP environment?

The Security Configuration Manager (SCM) set of tools allows security administrators to define these security templates:

- Password policies
- Lockout policies
- Kerberos policies
- Audit policies
- Event log settings
- Registry values
- Service startup modes
- Service permissions
- User rights
- Group membership restrictions
- Registry permissions and file system permissions
3 Describe the main purpose of the Internet Connection Firewall (ICF) from Microsoft? Can you selectively protect specific ports or protocols?

The main purpose of the Internet Connection Firewall (ICF) is to protect standalone systems with broadband Internet connections. ICF is ideal protection for telecommuters and corporate remote-access solutions. ICF is either on or off; you can’t selectively protect specific ports or protocols.

4 What are some advantages of NTFS?

- Encrypted File System (EFS) technology, which provides a high level of protection from hackers and data theft by transparently encrypting files with a randomly generated key.
- EFS encryption of offline data means new options for sharing encrypted files of disabling data recovery agents.
- EFS management through Group Policy and command-line utilities.
- Better compression for storage and support for larger partitions and file sizes.
- Windows XP Professional supports NTFS, FAT16, and FAT32 file systems.

Review questions

1 DES is an example of:

   A Symmetric algorithm
   B Asymmetric algorithm
   C Message digest hashing program
   D None of the above

2 ECC is an example of:

   A Symmetric algorithm
   B Asymmetric algorithm
   C Message digest hashing program
   D None of the above
3 SHA-1 is an example of:

A Symmetric algorithm
B Asymmetric algorithm
C Message digest hashing program
D None of the above

4 Blowfish is an example of:

A Symmetric algorithm
B Asymmetric algorithm
C Message digest hashing program
D None of the above

5 What are the two mechanisms for providing access control and privacy on wireless LANs defined in the IEEE 802.11b standard?

- Service Set Identifiers (SSIDs)
- Wired Equivalent Privacy (WEP)

6 Describe the auto logoff implementation specification.

For the Automatic Logoff implementation specification, covered entities should address implementing electronic procedures that terminate an electronic session after a predetermined time of inactivity.

7 Describe context-based access control.

Context-based access is based upon the context of a transaction—not on the attributes of the initiator. The external factors might include time of day, location of the user, or strength of user authentication.
Chapter 19 - Digital signatures and certificates

A-1: Discussing electronic signature requirements

1 What’s an electronic signature (specifically defined as a digital signature in the proposed Security Rule)?

An electronic signature is the attribute affixed to an electronic document to bind it to a particular entity or individual.

2 What are the appropriate implementation features of digital signatures?

The required features are:

- Message integrity
- Non-repudiation
- User authentication

3 What are the optional implementation features of digital signatures?

If an entity uses electronic signatures, the entity may also use, among other things, any of the following implementation features:

- Ability to add attributes
- Continuity of signature capability
- Countersignatures
- Independent verifiability
- Interoperability
- Multiple signatures
- Transportability of data

B-1: Discussing digital signatures
1 What’s a digital signature?

A digital signature is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and parameters, so that the identity of the signer and the integrity of the data can be verified.

2 What keys does Alice need for a digital signature and encrypted message exchange with Bob?

Alice needs these keys:

- Alice’s private key
- Alice’s public key
- Bob’s public key (Alice obtains this.)
- Alice’s random session key (Alice generates this.)

3 What keys does Bob require for a digital signature and encrypted message received from Alice?

Bob needs these keys:

- Bob’s private key
- Bob’s public key
- Alice’s public key (Bob obtains this.)
- Bob’s random session key (Bob generates this.)

4 What are the steps involved on Alice’s side to sign and send an encrypted message to Bob?

The steps involved on Alice’s side are:

a Alice writes her e-mail message, and this is used to create a message digest.

b The message digest is encrypted with Alice’s private key. The result is Alice’s digital signature.

c The original message is encrypted with a random session key.

d The session key is encrypted with Bob’s public key.

e5 The entire packet (digital signature + session key encrypted message + session key encrypted with Bob’s public key) is sent to Bob.
5 What are the steps involved on Bob’s side to decipher the signature and encrypted message received from Alice?

The steps involved on Bob’s side are:

a Bob receives the entire packet (digital signature + session key encrypted message + session key encrypted with Bob’s public key).

b Bob decrypts the session key with his private key. (He now has the session key used by Alice.)

c Bob decrypts the encrypted message with the session key to get the original message.

d He then decrypts the message digest with Alice’s public key. (He now has the message digest that was created by Alice.) He takes the original message (from his Step 3) and creates a message digest.

e He compares the message digest he received from Alice with the one he created. If the two match, it indicates that the message wasn’t modified in transit.

6 Explain how Alice uses the various keys.

On Alice’s side, the keys are used as follows:

- The message digest is encrypted with Alice’s private key.
- The plaintext message is encrypted with Alice’s session key.
- Alice’s session key is encrypted with Bob’s public key.

7 Explain how Bob uses the various keys.

On Bob’s side, the keys are used as follows:

- Alice’s encrypted session key is decrypted by Bob’s private key.
- The encrypted message is decrypted with Alice’s session key.
- The encrypted message digest (digital signature) is decrypted with Alice’s public key.

8 Describe PGP.

Pretty Good Privacy (PGP) enables each user to issue and manage a digital certificate. In a PGP-based PKI, there’s no Certificate Authority (CA). PGP cryptographic methods and keys compare well with those used in X.509-based PKI solutions. In a PGP solution, each user signs his or her digital
certificate. The issuer and subject fields are identical. Thus, all PGP certificates are initially self-signed.

PGP supports RSA, DSS, and Diffie-Hellman for public-key encryption. For conventional encryption, PGP supports International Data Encryption Algorithm (IDEA) and Triple Data Encryption Standard (3DES). The hash-coding algorithm supported is Secure Hash Algorithm -1 (SHA-1).

9 Describe S/MIME.

The Secure Multipart Internet Message Extensions (S/MIME) protocol uses public keys that comply with the X.509 standard. S/MIME is a specification for securing e-mail. S/MIME supports both encryption and signing. S/MIME supports digest and hashing algorithms MD5 and SHA-1. It also supports digital signature algorithms DSA and RSA. The key encryptions algorithms supported include Diffie-Hellman and RSA, while data encryption algorithms include RC2/40-bit-key, RC2/128-bit key, and 3DES.

C-1: Discussing digital certificates

1 What’s a digital certificate?

Digital certificates are digital documents attesting to the binding of a public key to an individual, another entity, or another entity’s Web site. They allow verification of the claim that a specific public key does, in fact, belong to a specific individual, or the Web site provides adequate transmission protections. Certificates help prevent someone from using a phony key to impersonate someone else, and they also help prevent Web site users from unknowingly sending confidential information openly through a Web site. In some cases, it may be necessary to create a chain of certificates, each one certifying the previous one until the parties involved are confident in the identity in question.

In their simplest form, certificates always contain a public key with the associated name. Additionally, a certificate containing an expiration date, the name of the certification authority that issued the certificate, a serial number, and perhaps other information is also common. Most importantly, it contains the digital signature of the certificate issuer.

2 What’s the most widely accepted format for certificates?
The most widely accepted format for certificates is defined by the ITU-T X.509 international standard, which enables certificates to be read by any X.509 compliant application.

3 What entities are involved in a certificate and why?

The entities involved in a digital certificate include:

- Issuer
- Subject
- Consumer

The issuer creates and signs the certificate. The subject sends the issuer his or her public key directly or uses it to validate the security of a Web site. The consumer uses the subject’s public key (in the certificate) and/or is reasonably assured that information transmitted via a secure Web site is, in fact, secure when transmitted to the entity maintaining the web site.

4 What’s the relationship between a digital certificate and a digital signature?

Certificates are typically used to generate confidence in the legitimacy of a public key. Certificates are essentially digital signatures that protect public keys from forgery, false representation, and alteration. The verification of a signature, therefore, can include checking the validity of the certificate for the associated public key.

D-1: Discussing Public Key Infrastructure (PKI)

1 Why is IPSec emerging as a protocol of choice for VPN systems?

IPSec is fast emerging as the protocol of choice to build the best VPN system, because it supports:

- Strong security
- Encryption
- Authentication
- Key management

2 Identify some common PKI functions.
Common PKI functions are:

- Registration
- Certificate issuance
- Certificate revocation
- Key recovery
- Lifecycle management

3 What are the features supported by Microsoft’s Windows XP and Vista?

Microsoft’s Windows XP and Vista operating systems provide built-in support for PKI. This support includes features such as:

- A number of public key-enabled applications and services—Internet Information Server, Internet Explorer, Microsoft Outlook and Outlook Express, Encrypted File System (EFS), IPSec, and smart card logon.
- Active Directory, which can be used as a publication point for Microsoft certificates and CRLs.
- Microsoft Certificate Services, which enable an organization to issue its own certificates and implement its own PKI. This is the CA service in Windows XP and Vista. Its job is to accept certificate requests, issue certificates, and publish the CRL.
- Support for smart cards in Windows XP and Vista, which may be used for key storage and cryptographic operations, in addition to logons.
- Commercial CA certificates preloaded in Windows XP and Vista, which enable users and computers to participate in existing PKIs on the Internet.
- Public Key policies in the Group Policy, which enable administrators to control the external CAs that users and computers, can trust.

These features are implemented on industry standards, such as X.509, LDAP, SSL/TLS, S/MIME, IPSec, and the public key extensions of Kerberos, enabling interoperability with third-party applications and PKIs.

Review questions

1 Describe a countersignature.
A countersignature is the capability to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where a party signs a document that’s already been signed by another party.

2 Describe the Serial Number field in a X.509 certificate.

The CA that issued the certificate assigns a unique serial number to each certificate.

3 Describe key recovery in a PKI.

Key recovery is an advanced PKI function that allows the recovery of data or messages when a key is lost.

4 Describe lifecycle management in the context of a PKI.

Lifecycle management is the routine maintenance of certificates in a PKI, including updating, backing up, and archiving keys. These functions are performed on a periodic basis, not in response to a specific request.
A-1: Discussing threats, risk management, and policy

1 What’s risk? What’s a safeguard? What are the options to defend an enterprise?

Risk is the combination of a threat exploiting some vulnerability that could cause harm to some asset. Safeguards counter threats. To defend an enterprise, you can reduce the value of the assets and/or take measures that reduce vulnerabilities.

2 What’s residual risk?

What remains after implementing risk-reducing measures is called residual risk.

3 What does the area of risk management address?

The area of risk management addresses:

- System security management
- Security service management
- Security mechanism management

4 Describe security service management.

Security service management addresses the management of such security services as authentication management, intrusion detection management, use access management, etc. Security service management focuses on protecting an organization’s infrastructure, data exchange, etc., by service area rather than by general security management or, say, network management.

5 What does security mechanism management address? Identify security mechanism management functions.
Security mechanism management addresses the management of security mechanisms. Security mechanism management functions include:

- Key management
- Encipherment management
- Digital signature management
- Access control management
- Data integrity management
- Authentication management
- Traffic padding management
- Routing control management
- Notarization management

6 How do policies, procedures, and practices differ?

Policies are high-level requirements adopted by the organization and apply to workforce members and external entities. Procedures are specific, step-by-step instructions defining how policy is implemented. Processes are activities that occur and are defined in policy and procedure, such as the data backup and recovery process.

7 How does a sound risk management program relate to policies, procedures, and practices?

A sound risk management program should include responsibility to ensure that policies, procedures, and practices are current, accurate, easy to communicate, and enforced. Such a program includes oversight of policies and procedures and practices for administrative, physical, and technology safeguards.

B-1: Discussing ISO-27002 security standards

1 Identify the fifteen major sections of the ISO-27002 standard.

   1. Framework,
   2. Acceptable Use of Information Technology Resources,
   3. Information Security Definition & Terms
4. Risk assessment

5. Security policy – management direction

6. Organization of information security – governance of information security

7. Asset management – inventory and classification of information assets

8. Human resources security – security aspects for employees joining, moving and leaving an organization

9. Physical and environmental security – protection of the computer facilities

10. Communications and operations management – management of technical security controls in systems and networks

11. Access control – restriction of access rights to networks, systems, applications, functions and data

12. Information systems acquisition, development and maintenance – building security into applications

13. Information security incident management – anticipating and responding appropriately to information security breaches


15. Compliance – ensuring conformance with information security policies, standards, laws and regulations

2 What’s the purpose of asset classification and control?

The objectives of the asset classification and control section are:

- Accountability of assets: To maintain appropriate protection of corporate assets
- Information classification: To ensure that information assets receive an appropriate level of protection

3 What’s the purpose of physical and environment security within ISO 27002?

The objectives of the physical and environmental security section are:
• Secure areas: To prevent unauthorized access, damage, and interference to business premises and information
• Equipment inventory: To prevent loss, damage, and compromise of assets and interruption to business activities

4 What are the objectives of the computer and network management section of ISO 27002?

The objectives of the computer and network management section are:

• Operational procedures and responsibilities: To ensure the correct and secure operation of information processing facilities
• System planning and acceptance: To minimize the risk of systems failures
• Protection from malicious software: To protect the integrity of software and information
• Housekeeping: To maintain the integrity and availability of information processing and communication
• Network management: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
• Media handling and security: To prevent damage to assets and interruptions to business activities
• Data and software exchange: To prevent loss, modification, and misuse of information exchanged between organizations

5 What are the objectives of the compliance section?

The objectives of the compliance section are:

• Compliance with legal requirements: To avoid breaches of any criminal or civil law, statutory, regulatory, or contractual obligations, and security requirements
• Security review of IT systems: To ensure compliance of systems with organizational security policies and standards
• System audit considerations: To maximize the effectiveness of and to minimize interference to/from the system audit process

C-1: Discussing security policy considerations
1 What are some characteristics of a well-written policy?

A well-written policy should:

- Be technology-neutral
- Be short, simple, and written in a manner that’s easily understood
- Require change infrequently
- Require formal approval and support from senior-level management
- Be effectively communicated to all employees, agents, and contractors within the enterprise on a regular basis
- Not be tested

2 What are some characteristics of procedures?

A well-written procedure should:

- Apply to the department or unit in a vertical manner
- Be technology-specific
- Be sufficiently detailed to document every step in a process from start to finish
- Be able to walk a novice through the successful completion of a task
- Be updated whenever a step in the procedure changes
- Not require formal approval from senior-level executive management
- Be communicated on a need-to-know basis to employees, agents, and contractors
- Be tested

D-1: Discussing sample security policy documents

1 What’s the purpose of an acceptable use policy?

The purpose of an acceptable use policy is to outline the acceptable use of technology and data across a health information exchange or between entities involved in the exchange of PHI. These rules are in place to protect exchange members. Inappropriate use exposes the exchange to risks, including virus attacks, compromise of network systems and services, breach of privacy and/or security, regulatory action, legal issues, etc.

Review questions
1 What’s the purpose of an information system activity review?

The purpose of the information system activity review is to ensure that users comply with access control procedures. The covered entity should maintain, and periodically review, audit logs.

2 Identify examples of strictly prohibited system and/or network activities.

Examples of strictly prohibited system and/or network activities are:

- Introducing a malicious program into the network or server.
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a health care organization computing asset to engage actively in procuring or transmitting material that’s in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any health care organization account.
Chapter 21 - HITECH Act and Red Flag Rule

A-1: Discussing HITECH fundamentals

1 What is the purpose of HITECH?

HITECH is the section of the 2009 American Recovery and Reinvestment Act (ARRA) that provided economic stimulus to help the nation out of a deep recession. HITECH is designed to accelerate the computerization of the entire health care industry, facilitate electronic health information exchange, and expand and further define privacy and security protections to build greater trust among industry players and with consumers as well. These changes are expected to improve the efficiency and coordination of care, improve the timeliness of care, and reduce the overall costs of care.

2 What areas does HITECH address?

The HITECH provisions address the following areas:

- National framework for HIT coordination
- Promote HIT implementation
- Provide grants and loan funding to encourage HIT adoption
- Expand and clarify HIPAA privacy and security provisions

3 How are HITECH and HIPAA related?

Part of the provisions of HITECH expand and clarify elements of HIPAA that have caused confusion or barriers to compliance in the health care industry. HITECH strengthened many of the privacy and security requirements and also expanded the coverage of HIPAA to new entities to create a broader scope of protection and build greater trust among industry players and the public in moving to digital technologies.

4 Name three HITECH programs and briefly describe the purpose for each.
• The Beacon Community Cooperative Agreement Program funds innovative community-based demonstration programs that use HIT to move health systems towards patient-centered care
• EHR incentive programs to speed up the installation and use of EHRs among eligible Medicare and Medicaid providers.
• Health Information Technology Regional Extension Centers (RECs) which offer technical assistance, guidance and information to support and accelerate health care providers’ efforts to implement and use EHRs
• The State HIE Cooperative Agreement Program funded state efforts to rapidly build or expand health information exchange networks both within and across states to move toward nationwide interoperability.

5 Name three areas addressed in the HITECH Act

• Breach Notification
• Enforcement
• Expands HIPAA privacy and security to Business Associates and other entities
• Modifies individual rights
• Modifies HIPAA Privacy for genetic information

6 What four key Security Rule safeguards must Business Associates now comply with?

• Administrative
• Technical
• Physical
• Policies and Documentation

7 Under what three circumstances can a covered entity directly or through a business associate engage in a marketing communication with a patient?

• If the communication is about the individual’s current treatment and/or a medication already prescribed; or
• If communication is made by the covered entity who has obtained an authorization from the individual; or
• If the communication is made by the business associate in compliance with the preceding and under specific contract with the covered entity.
8 When accounting for disclosures of PHI from an EHR/EMR what is a covered entity required to do?

Covered entities implementing or using electronic health records (EHR) or electronic medical records (EMR) will be required to include all PHI disclosed from the EHR/EMR for whatever purpose including disclosures for treatment, payment and healthcare operations (TPO) and disclosures made by covered entities’ business associates, made within the three years prior to the request for an accounting. Disclosures for TPO not captured from the EMR/EHR do not need to be included in the accounting.

B-2: Discussing Red Flags Rule fundamentals

1 What is the purpose of the Red Flags Rule?

The Red Flags Rule was enacted because Congress wanted to stop the alarming growth of identity theft and its adverse effects on victims and service providers. Stopping identity theft all together is not realistic; however Congress felt its impact could be mitigated by setting processes and procedures to detect the fraud as soon as possible after it occurred and to help victims mitigate damages that result without unnecessary delay.

2 What are three ways a health care provider could become a “creditor”?

- Obtain or use consumer reports, directly or indirectly, in connection with a credit transaction;
- Furnish information to consumer reporting agencies in connection with a credit transaction;
- Advance funds to or on behalf of a person, based on a person’s obligation to repay the funds or on repayment from specific property pledged by or on the person’s behalf.

3 What are three similarities between the Red Flags Rule and HIPAA?

- Both require an ongoing risk assessment and risk management/mitigation process
- The requirement that Red Flags be formally identified and addressed and the requirement that written privacy and security policies and procedures be developed and implemented;
The requirement that workforce members and patients be educated and trained in Red Flags Rule identification and mitigation and the HIPAA training requirements for both workforce members and patients (through the Notice of Privacy Practices).

4 Why does stolen MII sell for up to 50 times more than a stolen credit card?

Few if any of the security protections built into credit cards are used in health insurance identification cards issued. Once a thief takes possession of MII, the submission of a false claim leaves few if any traces of the thief’s identity. For security purposes, credit cards have low limits and issuers scrutinize purchases in real time. Health insurers on the other hand contract for lifetime coverage limits as high as one million dollars and no means of identifying and tracing potentially fraudulent bills before they are submitted for payment.
Chapter 22 - Omnibus Rule

A-1: Discussing Omnibus fundamentals

1 What three items are yet to come following the Omnibus Rule?
   - Accounting for disclosures and access
   - Guidance regarding the minimum necessary rule
   - Distribution of penalties to persons harmed by rule violations

2 Breach Notification rules have changed. In determining whether or not to report a breach what test was replaced and what is the new test?
   - The “risk of harm” test was replaced
   - The new test is the “low probability of risk” standard based on a thorough risk assessment

3 Under the new standard, are there likely to be more breach notifications or fewer breach notifications?
   - More

4 Discuss the four mandatory factors that must be addressed in a documented breach risk assessment
   - Nature and extent of PHI involved
   - The unauthorized person who used PHI or to whom the disclosure was made
   - Whether the PHI was actually acquired
   - The extent to which the risk to PHI has been mitigated

5 Discuss the categories of PHI that may be used or disclosed for fundraising under the Omnibus Rule
   - Department of Service
6 Discuss how the Omnibus Rule changed regarding authorization for future research

Under the old rule, authorization had to be study-specific. The new rule allows a prior authorization to govern future research provided the person is put on reasonable notice of the potential for future research.

7 Discuss a new exception to the definition of marketing

Marketing does not include subsidized refill reminders about a drug that is currently prescribed and reimbursement must be reasonably related to the cost of the communication.

8 Discuss which entities are now specifically identified as Business Associates under the Omnibus Rule

- Health Information Organizations
- e-Prescribing Gateways
- A provider of data transmission services (value-added)
- Offer of Personal Health Records on behalf of covered entities

9 Subcontractors are Business Associates under the Omnibus Rule. Discuss what makes a subcontractor a business associate

- A person to whom a business associate has delegated a function, activity or service
- The person is not a member of the business associate’s workforce
- The function, activity or service involves PHI

10 Which of the following statements is true with respect to rules governing business associates under the Omnibus Rule

- The rules are essentially the same as rules that have always applied to covered entities (True)
The rules that apply to business associates are substantially different from those that apply to covered entities.

11 Which of the following statements is true with respect to Patient Rights under the Omnibus Rule

- Patient rights remained about the same.
- Patient rights decreased
- Patient rights increased (True)

12 What OCR must do if preliminary analysis indicates “willful neglect” on the part of the covered entity or business associate? and this is ultimately confirmed.

- OCR must open a formal investigation

13 What must OCR do if its investigation establishes “wilful neglect” on the part of a covered entity or business associate?

- OCR must impose a penalty if “willful neglect is established.
A-1: Discussing HITECH fundamentals

1 Describe the purpose of the EHR incentive programs.

The Medicare and Medicaid EHR incentive programs were developed to encourage eligible hospitals and health professionals to purchase, install and use EHR technologies, with the goal of helping to automate the health care industry and improve health care in the United States.

2 Identify three differences between the Medicaid and Medicare EHR incentive programs.

Differences between the Medicare and Medicaid incentive programs include:

- Different provider and hospital types are eligible for each
- The Medicare program is run through CMS, and the Medicaid program is through the states
- Medicare providers will see deductions from their payments beginning in 2015 if they do not meet meaningful use

3 What is certified EHR technology?

Certified EHR technology is electronic health record software, applications, modules or systems that have been reviewed against national standards, implementation specifications, and certification criteria and provide capabilities that support eligible providers in meeting the meaningful use objectives and measures.

4 What is meaningful use and why is it important?

“Meaningful use” measures the use of certified EHR technology by eligible providers to perform selected business functions, such as e-prescribing, transmitting lab results, and clinical summary exchange. Meaningful use measures the progress of the health care industry in automating key business functions, which will enable better patient care and coordination.
5 Describe the difference between meaningful use objectives and meaningful use measures.

Meaningful use objectives describe the key business functions that eligible professionals must provide and the key capabilities that a certified EHR should support.

Meaningful use measures describe the threshold percentage that eligible professionals must achieve for each of the key business functions to demonstrate increasing use of certified EHR technologies.

6 What do clinical quality measures (CQMs) measure?

Clinical quality measures measure and track the quality of healthcare services, and measure many aspects of patient care including health outcomes, clinical processes, patient safety, care coordination, patient engagement and clinical guidelines.
Chapter 24 - HIPAA Compliance and Enforcement

A-1: Discussing HIPAA compliance and enforcement issues

1 Describe several changes in compliance and enforcement requirements with the enactment of the Omnibus Rule.

- Substantial increases have been made in civil monetary penalties.
- States’ Attorney Generals have the authority to bring civil actions for violation of federal privacy rules.
- Compliance actions must now be brought whenever investigations produce evidence of possible willful neglect on the part of Covered Entities or Business Associates.
- Business associates may be liable for violations of its agents, including a workforce member or subcontractor, regardless of whether a compliant business associate agreement is in place.

2 What are possible ways that an OCR audit can be triggered?

- Random
- Complaints
- Notification of breaches
- Awareness of potential violations or non-compliant activities

3 Which methods comply with HHS guidance on de-identifying PHI?

- Safe harbor
- Redaction
- Expert determination
- None of the above

4 Describe which workforce sanctions may be imposed under the Privacy and Security Rules.

- Verbal warnings
- Suspension or limitation of access to information systems, repositories, files and
• areas that contain PHI
• Required re-training
• Letters of warning
• Reassignment or suspension from work
• Termination

5 In regard to the Omnibus Rule’s enforcement provisions which of these statements is true?

• A Covered Entity or business associate can be liable for penalties of more than $1.5M in any given year
• Civil monetary penalties must be imposed for violations due to willful neglect
• In certain circumstances, a Business Associate’s constructive knowledge of a violation can be imputed to the Covered Entity, even when the business associate fails to notify the Covered Entity.
• Civil monetary penalties can be imposed on Business Associates regardless of whether a compliant business associate agreement is in place.

6 Is this statement True or False?

• OCR can impose a civil monetary penalty for an underlying Privacy or Security rule violation even where all the breach notifications were properly provided. True

7 Describe several of the findings from the OCR pilot audits of Covered Entities and Business Associates

• Security compliance issues were more common than those for privacy compliance
• Smaller entities had more problems with compliance than larger entities
• Conducting regular risk assessments was one of the most neglected compliance activities
• Many organizations failed to fully consider business associate compliance and risks

8 Describe several of the major security issues found

• User activity monitoring (audit logs)
• Contingency planning (disaster recovery, business disruption, backup)
• Authentication and integrity (strong user credentials)
9 Describe several of the major privacy issues found

- PHI uses and disclosures related to deceased individuals and personal representatives
- Disclosures for judicial and administrative proceedings
- Verification of the identity of an individual requesting PHI
- Business associate contracts

10 Describe some of the advice OCR gave Covered Entities and Business Associates to help ensure that documented proof of compliance is available in the course of an audit.

- Conduct a robust HIPAA compliance review and risk assessment on a regular basis
- Identify and document all lines of business and business functions affected by HIPAA
- Map PHI flows within the organization as well as flows to and from third parties
- Identify and document all PHI created, transmitted, stored, received, or handled by the organization, both internally and with external parties
- Seek guidance available on the OCR website
Chapter 25 - Social Media, Mobile Technology, and Big Data

A-1: Discussing social media, mobile technology and big data issues

1 Describe several benefits of social media for health care.
   - Allows for the creation of patient communities around specific health conditions, which can be support groups, treatment resources, research fundraisers, and advocates for research on the disease
   - Brings researchers together from around the world to share knowledge, accelerate research and the development of new and better treatments
   - Has the potential for near real time monitoring of the spread of outbreaks of contagious diseases
   - Has the potential for more accurate analysis of health issues affected by human behaviour, such as diet, exercise, smoking and drinking.

2 Describe some of the risks and challenges in using mobile devices to capture store, access or transmit ePHI.
   - Mobile devices do not normally have good security features
   - Mobile devices are often lost or stolen
   - Smart mobile devices may operate using cloud computing, which is not inherently secure.
   - Using personal mobile devices for business use make security more difficult to manage

3 What is big data?

Massive amounts of information on what people do and say each day is being created, captured and stored electronically, and this data is growing by leaps and bounds over a very short time period. With the right analysis tools, this information can be used for studies, statistics, research, and to answer basic and complex questions about people’s interactions with the health care systems.

4 What privacy risks are common with use of digital media and devices?
   - Risks to privacy: the right to control information about you
• Risk of being tracked: many personal devices capture your location, movements, and behaviors.
• Risk of loss of anonymity, as public spaces are also increasingly being monitored, so more and more of our daily lives and actions are being recorded and saved

5 What two key issues must be addressed in mobile/digital device policy?

• Securing all devices that capture store, access or transmit ePHI
• Securing company ePHI that will be captured, stored, accessed or transmitted, preferably using encryption

6 Name three recommended technical solutions for securing mobile technologies.

• Enabling or requiring strong user passwords or public/private keys with strong passphrases.
• Securing remote connectivity via encryption or other secure portal technologies.
• Requiring all personal devices used to connect to a company’s networks meet baseline security requirements.
• Conducting periodic risk assessments that include assessing risks related to mobile device use
• Establishing adequate backup capabilities to support mobile technologies
• Utilizing remote and device tools where possible to secure, monitor and lock devices and prevent data breaches

7 Name three recommended policy solutions for securing mobile technologies.

• Prohibit use of and access to company-owned devices and networks by non-workforce members; and prohibit access to those company assets on workforce member owned devices by non-workforce members.
• Company employees must never provide their company login or email password to anyone, not even family members.
• Company employees and contractors using mobile devices for business purposes must not use non-company email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct company business.
• Workforce members must store mobile devices in locked areas such as offices or car trunks whenever possible when not in use.
• Workforce members must avoid storing ePHI or passwords on the device.
• Workforce members using personal devices for business purposes should inform their supervisor and the IT department and ensure that the device is appropriately secured prior to use.

8 Identify three things a covered entity should never do using the internet, social media, or mobile devices.

• Post detailed information about a patient on Facebook without the patient name
• Share X-ray, ultrasound, or MRI images on a public social media site
• Discuss a patient’s health issues on a mobile phone on the subway
• Use PHI on a laptop or smartphone on a airplane
• Use a public email account to transmit PHI to another provider