Chapter 9 Review Questions

1. What does Administrative Simplification include? Please mark all that apply.
   a. Privacy rule
   b. Code sets
   c. Security rule
   d. Electronic Transactions
   e. Identifiers
   f. Total accounts receivable

2. HIPAA was introduced in 1996. There are many facets to the law. Which includes the facets of HIPAA that have been implemented?
   a. Privacy, patient identifier, security, and transactions and code sets
   b. Privacy, security, transactions and code sets, provider identifiers
   c. Transactions and code sets, patient identifier, and provider identifier
   d. Privacy, security, patient identifier, and provider identifier

3. A patient has been injured at the work place and filed a workers' compensation claim. The employer requests the medical records specific to the claim. Can the provider send the medical records to the employer without authorization from the patient? If yes, why?
   a. No; patient permission is necessary to use or disclose to the employer
   b. No; medical records cannot be released to an employer under any circumstance; the records would need to be requested by the employers workers' compensation carrier.
   c. Yes, if the employee is a member of the workplace, and it is concerning a workplace injury, the records can be released
   d. Yes, the employer provides medical insurance and therefore is allowed to request a patient's PHI.

4. What does the HIPAA Privacy Rule require the average provider to do??
   a. Conduct training, appoint a privacy officer, implement safeguards to protect PHI and report HIPAA efforts to the OCR annually.
   b. Appoint a privacy officer, conduct periodic privacy audits and staff training, implement safeguards to protect PHI, and obtain the patient's signature before any use or disclosure of their record.
   c. Implement safeguards to protect PHI, have the patient sign a BAA to protect disclosures, and permit open access to all employees of the practice.
   d. Notify patient's of their privacy rights, implement policies and procedures to reasonably limit uses and disclosures to minimum necessary, appoint a privacy officer and conduct staff training, and implement safeguards to protect PHI.
5. Electronic data interchange (EDI) refers to the transmission of certain transactions electronically. What is the current version for HIPAA transactions?

a. X12 Version 4010, NCPDP Version 5.1, HL7
b. X12 Version 5010, NCPDP Version D.0.
c. HL7, NCPDP Version 5.1
d. HL7, X12 Version 4010

6. The HIPAA security rule adopts administrative, technical, and physical safeguards to prevent unauthorized access to protected health care information. What does the Security Rule apply to?

a. Written and oral communication, fax back systems, video teleconferencing
b. Paper-to-paper faxing, video teleconferencing, database storage
c. Database storage, information stored on desktops and laptops, electronically submitted faxes, telephone voice response systems
d. Telephone voice response systems, paper-to-paper fax machines, video teleconferencing, oral phone conversations, written documents stored on a shelf.

7. A billing office, who has signed a BAA with a provider, has used the electronic explanations of benefits (EOBs) in an education presentation to an association of billers. The presenter has not removed the names and IDs of the patients from the EOBs. Is this a violation of HIPAA? Why?

a. No; Business Associates are not required to protect the PHI of the patients.
b. No; PHI can be used for educational purposes
c. Yes; Business Associates are required by HIPAA and by their BAA agreement to protect PHI
d. Yes; both the provider who contracted the billing company and the billing company are in violation of HIPAA.

8. A breach of the PHI for 45 patients in your office has been discovered. According to HIPAA-HITECH how long do you have to notify the affected patient of the breach?

a. 14 days from the discovery of the breach
b. 30 days from discovery of the breach
c. 60 days from discovery of the breach
d. 90 days from discovery of the breach

9. You have an employee who performs the billing for the clinic out of her home. What would be a reasonable security safeguard to protect PHI?

a. Require the employee to log on to a remote server that has an automatic logoff feature set.
b. Require her to only work with paper charts so she will not fall under the HIPAA Security rule.
c. Have the employee sign a Business Associate Agreement to protect the practice from a breach of PHI.
d. HIPAA Security Rule does not allow for employees to work remotely.
10. Your office has received a subpoena accompanied by an order of the court to supply the medical records. According to HIPAA Administration Simplification, can you supply the records requested?

a. No; Records, even when ordered by a court, can not be released without the patient’s authorization.
b. No; Records cannot leave your office under any circumstance.
c. Yes; The provider has the option of whether or not to supply the records.
d. Yes; Records requested under court order may be provided without authorization from the patient.

11. What would be considered a proper notice of breach under the HITECH law when under 500 individuals were affected by the breach?

a. Post a breach notice to the clinic’s website including the date of the breach and when it was discovered, a list of names included in the PHI, suggested steps for individuals to take to protect themselves against any problems stemming from the breach.
b. Send a breach notice via U.S.P.S. with a date of the breach, when it was discovered, along with a copy of the information that was breached.
c. Publish a print advertisement of the breach in the local paper and include the date of the breach and when it was discovered, a brief description of incident that led to the breach, description of the unsecured PHI involved, and suggested steps for individuals to take to protect themselves against any problems stemming from the breach.
d. Call each individual affected by the breach and inform them of the date of the breach and when it was discovered, a list of names included in the PHI, suggested steps for individuals to take to protect themselves against any problems stemming from the breach.

12. You have referred a patient to an orthopedic provider. The Orthopedist has requested the patient’s medical records. According to HIPAA Administration Simplification, can you supply the records requested without a signed patient authorization?

a. No; the records can not be sent to another provider unless an authorization is signed by the patient.
b. No; medical records can only be shared between providers of the same practice.
c. Yes; providing records to a provider treating the patient falls under treatment, payment and operations.
d. Yes, medical records belong to the provider and the provider can share the records with anyone he wants.

13. When referring to HIPAA, what action would be reasonable when supplying “minimum necessary” standards to PHI?

a. The provider should go through each record shared and mark out all sentences that do not relate to the current condition being discussed.
b. All employees of a clinic should have access to all aspects of the patients’ records.
c. The medical records for the employees at the clinic should be locked up to maintain their privacy.
d. Limiting access to the medical records to only those employees who need it for a specific purpose.
14. Which parts of HIPAA Administration Simplification require policies and procedures to be established?

a. Privacy Rule, Security Rule, Code Sets, Electronic Transactions, and Identifiers  
b. Privacy Rule, Security Rule, Identifiers  
c. Privacy Rule, Electronic Transactions, Identifiers  
d. Privacy Rule, Security Rule

15. The Security Rule requires an entity to take administrative, technical, and physical safeguards to prevent unauthorized access to PHI. One of the technical safeguards includes access control. This is often done using passwords. Which password would be the most secure?

a. PAS123  
b. Pas132  
c. PAS&123  
d. Pas$132
Chapter 9 Review Questions Answer Key

1. What does Administrative Simplification include? Please mark all that apply.
   a. Privacy rule
   b. Code sets
   c. Security rule
   d. Electronic Transactions
   e. Identifiers


2. HIPAA was introduced in 1996. There are many facets to the law. Which includes the facets of HIPAA that have been implemented?
   b. Privacy, security, transactions and code sets, provider identifiers

   Rationale: Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans). Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans). Compliance for Transactions and code sets was required as of October 16, 2003. Compliance for National Provider Identifier (NPI) was required as of May 23, 2007 (May 23, 2008 for small health plans).

3. A patient has been injured at the work place and filed a workers' compensation claim. The employer requests the medical records specific to the claim. Can the provider send the medical records to the employer without authorization from the patient? If yes, why?
   c. Yes, if the employee is a member of the workplace, and it is concerning a workplace injury, the records can be released

   Rationale: Records can be released to the employer if the protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance (http://www.gpo.gov/fdsys/pkg/CFR-2002-title45-vol1/xml/CFR-2002-title45-vol1-sec164-512.xml)
4. What does the HIPAA Privacy Rule require the average provider to do??

d. Notify patient's of their privacy rights, implement policies and procedures to reasonably limit uses and disclosures to minimum necessary, appoint a privacy officer and conduct staff training, and implement safeguards to protect PHI.

Rationale: On average, the HIPAA Privacy Rule requires the average provider to have a Notice of Privacy Practices available for patients to read. This document informs the patient how a covered entity will use and disclose protected health information for treatment, payment, and operations. The notice must also clearly explain the patients’ rights under the privacy laws of HIPAA. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. The practice must appoint a privacy officer and conduct staff training. Incidental disclosures are permitted under the rule but only if the covered entity has taken “reasonable safeguards” to protect PHI and otherwise implemented the requirements of the minimum necessary rule.

5. Electronic data interchange (EDI) refers to the transmission of certain transactions electronically. What is the current version for HIPAA transactions?

b. X12 Version 5010, NCPDP Version D.0.

Rationale: On January 16, 2009, HHS published it was adopting X12 Version 5010 and NCPDP Version D.0 for HIPAA transactions. In this rule, HHS also adopts a new standard for Medicaid subrogation for pharmacy claims, known as NCPDP Version 3.0. For Version 5010 and Version D.0, the compliance date for all covered entities was January 1, 2012.

6. The HIPAA security rule adopts administrative, technical, and physical safeguards to prevent unauthorized access to protected health care information. What does the Security Rule apply to?

c. Database storage, information stored on desktops and laptops, electronically submitted faxes, telephone voice response systems

Rationale: Security safeguards apply to any PHI stored electronically before it is transmitted. Paper-to-paper faxing and video teleconferencing are not considered e-PHI because the information being exchanged did not exist in electronic form before the transmission. Telephone voice response systems are operated from electronic systems where the information is stored, which makes them covered by the Security Rule.

7. A billing office, who has signed a BAA with a provider, has used the electronic explanations of benefits (EOBs) in an education presentation to an association of billers. The presenter has not removed the names and IDs of the patients from the EOBs. Is this a violation of HIPAA? Why?

c. Yes; Business Associates are required by HIPAA and by their BAA agreement to protect PHI
Rationale: The Privacy Rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. PHI in electronic form is designated as electronic PHI (e-PHI).

8. A breach of the PHI for 45 patients in your office has been discovered. According to HIPAA-HITECH how long do you have to notify the affected patient of the breach?

c. 60 days from discovery of the breach
Rationale: A breach of notice must be within 60 days of the discovery of the breach.

9. You have an employee who performs the billing for the clinic out of her home. What would be a reasonable security safeguard to protect PHI?

a. Require the employee to log on to a remote server that has an automatic logoff feature set.
Rationale: The HIPAA Security Rule does not prevent employees from working remotely; however, the necessary security requirements are expected to be in place as if they were in the office, or even more strict. The automatic logoff specification is one that would apply regardless of the location of the employee. Business Associate Agreements are for Business Associates, not employees.

10. Your office has received a subpoena accompanied by an order of the court to supply the medical records. According to HIPAA Administration Simplification, can you supply the records requested?

d. Yes; Records requested under court order may be provided without authorization from the patient.
Rationale: Title 45 - Public Welfare. SUBCHAPTER C - ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS. PART 164 - SECURITY AND PRIVACY. Subpart E - Privacy of Individually Identifiable Health Information.
(e) Standard: Disclosures for judicial and administrative proceedings.
(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:
(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order;...
11. What would be considered a proper notice of breach under the HITECH law when under 500 individuals were affected by the breach?

c. Publish a print advertisement of the breach in the local paper and include the date of the breach and when it was discovered, a brief description of incident that led to the breach, description of the unsecured PHI involved, and suggested steps for individuals to take to protect themselves against any problems stemming from the breach.

Rationale: The method of notification will vary depending on the number of individuals involved. Notice to individuals must include:
The date of the breach and when it was discovered
A brief description of the incident that led to the breach
Description of the unsecured PHI involved
Suggested steps individuals should take to protect themselves against any problems stemming from the breach
The notice must be received within 60 days of the breach. The notice can be sent regular mail or alternative method of notice such as Web posting or print advertisement.

12. You have referred a patient to an orthopedic provider. The Orthopedist has requested the patient’s medical records. According to HIPAA Administration Simplification, can you supply the records requested without a signed patient authorization?

c. Yes; providing records to a provider treating the patient falls under treatment, payment and operations.

Rationale: Medical records may be shared when done so for treatment, payment, or operations. An example of TPO includes Doctors and/or hospitals (that are covered entities) may share information freely with one another for treatment reasons.

13. When referring to HIPAA, what action would be reasonable when supplying “minimum necessary” standards to PHI?

d. Limiting access to the medical records to only those employees who need it for a specific purpose.

Rationale: The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.
14. Which parts of HIPAA Administration Simplification require policies and procedures to be established?

d. Privacy Rule, Security Rule

Rationale: Both the Privacy Rule and Security Rule require policies and procedures to be established. The Privacy Rule requires a covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. The Security Rule, Administration Safeguards require assigning responsibility to someone for security and having policies and procedures in place to direct your security efforts.

15. The Security Rule requires an entity to take administrative, technical, and physical safeguards to prevent unauthorized access to PHI. One of the technical safeguards includes access control. This is often done using passwords. Which password would be the most secure?

d. Pas$132

Rationale: Using a combination of upper and lower case letters, non-sequential numbers, and special characters reduces the risk another person might be able to re-create your password.