1. HIPAA Security Rule

**Johns, Merida L., "Information Security", in Johns, Merida L. (ed.) Health Information Management Technology, an Applied Approach, AHIMA: Chicago, IL, 2nd ed. 2007, chapter 19, pp. 847 - 874**

1. The HIPAA Security Rule envisions that a covered entity's risk management activities and security measures will reduce the entity's data security risks and vulnerabilities to which of the following levels:
   a. reasonable and appropriate protection of electronic PHI
   b. reasonable and appropriate protection of electronic and non-electronic PHI
   c. absolute protection of electronic PHI from all threats and hazards, whether or not reasonably anticipated
   d. absolute protection of electronic PHI against any unauthorized use or disclosure, whether or not reasonably anticipated

2. Security policies must be in which of the following formats:
   a. Must be maintained in written format
   b. May be oral agreements between supervisors and employees
   c. May be written or oral
   d. May not be in an electronic form

3. The establishment by a covered entity of a defined security management process includes which of the following elements:
   a. Conducting a risk analysis
   b. Creating and maintaining security policies and practices
   c. Ongoing review of information system activity (e.g. audit logs, access reports, and tracking of security incidents)
   d. All of the above

4. According to HIPPA standards, the designated individual responsible for data security:
   a. Must be identified by every covered entity
   b. Is only required in large facilities
   c. Is only required in hospitals
   d. Is not required in small physician office practices

5. Workforce security awareness and training is required for which of the following:
   a. For all workforce members
   b. Only for workforce members who handle PHI
   c. Only for workforce members who handle electronic data
   d. Only for workforce members who handle electronic PHI

6. Which of the following ensures that procedures are in place to handle an emergency response in the event of an untoward event such as a power outage:

a. An audit control
b. A contingency plan
c. Employee training
d. Password protection

7. Written business associate agreements are required with which of the following:
a. Any company where work is outsourced
b. Any outside company that handles electronic data
c. Any outside company that handles electronic PHI
d. Every outside company

8. Which of the following ensure that a user has only the information needed to perform his or her job:
a. Audit controls
b. Access controls
c. Person identification forms
d. Workstation safeguards

9. A visitor sign-in sheet to a computer area is an example of which of the following controls:
a. Administrative
b. Audit
c. Facility access
d. Workstation

10. The process that encodes textual material, converting it to scrambled data that must be decoded, is which of the following:
a. An audit trail
b. An encryption
c. A password
d. A physical safeguard

**AMA Practice Management Center, "What you need to know about the new health privacy and security requirements"**

11. The HIPAA regulations implementing the HITECH Act, a part of the 2009 "stimulus bill", introduced which of the following patient rights that affect the content of a patient's clinical health record that may be disclosed by a covered entity to third parties, when a patient has paid the covered entity in full for a health care item or service:
a. the patient may restrict the disclosure of the PHI about the individual to a health plan for the purpose of carrying out payment or of health care operations
b. the patient may restrict the disclosure of the PHI about the individual to all other providers for any purpose, including for subsequent treatment of the same condition for which the patient had paid "out of pocket"

c. the patient may restrict the disclosure of the PHI about the individual to law enforcement authorities for any purpose
d. none of the above

12. The HIPAA regulations implementing the HITECH Act introduced which of the following compliance obligations upon a "business associate" (BA) of a covered entity:

a. the BA's compliance obligations are exclusively contained within the Business Associate Agreement(s) to which the BA is a party
b. the HIPAA requirements apply directly to BAs, regardless of the content of any Business Associate Agreement to which the BA is a party
c. the HIPAA requirements apply directly to BAs, subject to being reduced by a Business Associate Agreement containing a less restrictive requirement
d. none of the above

13. HHS has yet to adopt final regulations implementing which of the following patient rights envisioned by the HITECH Act:

a. a patient may receive from a covered entity with an EHR system an accounting of disclosures made by that covered entity of that patient's PHI, including disclosures that had been made for treatment, payment and healthcare operations purposes
b. a patient may receive from a covered entity an electronic copy of his/her medical record
c. a patient may restrict certain disclosures of PHI relating to services for which the patient has paid "out of pocket"
d. none of the above (all of the above patient rights have been incorporated into the final HIPAA regulations)

14. In the HIPAA regulations the concept of limiting the scope and quantity of PHI to the "minimum necessary to accomplish the intended purpose" applies to:

a. requests by a covered entity for the receipt of PHI
b. disclosures by a covered entity of PHI in response to a request for PHI
c. both of the above
d. none of the above

15. In the HITECH Act the exercise of discretion by a covered entity to determine the "minimum necessary" information to be released pursuant to a request was limited (other than for purposes of treatment, among other exceptions). A default presumption was established, unless the releasing entity determines otherwise, that the "minimum necessary" is constituted of which of the following:

a. the legal record/ a designated record set
b. a de-identified data set
c. a limited data set
d. none of the above

16. The HIPAA regulations implementing the HITECH Act introduced which of the following patient rights with regard to marketing materials sent to the patient by a covered entity:

a. covered entities must provide patients an opportunity to opt-out of receiving fundraising communications
b. covered entities must obtain prior written authorization from a patient to send a communication from a third party for which the covered entity receives direct or indirect payment
c. both of the above
d. none of the above

**Mosquera, Mary, "8 tactics for mobile data privacy and security", Government Health IT, July 20, 2011**

17. The exponential growth in the use by healthcare professionals of mobile devices (e.g., smartphones, tablets, laptops) that provide access to a provider's electronic health record (EHR) system poses which of the following data security threats:

a. Loss of a device without password protection enabled could provide a third party the means of unauthorized access to the EHR system and its PHI
b. Loss of a device without encryption of the data stored on the device could provide a third party unauthorized access to the PHI "at rest" on the mobile device
c. Us of the mobile device to access and transmit PHI to or from the EHR system over an unsecured WI-FI network could enable a third party's unauthorized access to the PHI "in motion" to or from the mobile device
d. All of the above

## 5. Breach Notification

**AMA, "HIPAA Violations and Enforcement"**

18. HIPAA provides for all of the following enforcement options in the event of a violation of the HIPAA regulations, except:

a. a civil monetary penalty ranging from $100 to $50,000 per violation, determined by the HHS Secretary
b. a criminal fine of up to $250,000 and imprisonment for up to ten years, determined by a court of law as a result of a prosecution initiated by the US Department of Justice
c. damages awarded by a court of law as a result of a law suit (private cause of action) initiated by a private sector entity seeking to sanction a violation of HIPAA
d. none of the above (all of the above are provided for in HIPAA)

19. The HIPAA regulations implementing the HITECH Act established several levels of increasing civil and criminal penalties for violations of HIPAA based upon:

a. the number consumers directly affected by the violation

b. the size of the violator covered entity
c. increasing levels of culpability of the violator
d. none of the above

20. The HIPAA regulations implementing the HITECH Act provide for the greatest potential civil monetary penalty for which of the following categories of culpability:

a. unintentional violation caused by factors beyond the violator's knowledge or control
b. gross negligence
c. willful neglect followed by correction of the violation within 30 days of discovery
d. willful neglect without correction of the violation

21. The HIPAA regulations implementing the HITECH Act provide for a maximum potential civil monetary penalty (CMP) for identical violations during a calendar year, in the amount of which of the following:

a. $50,000
b. $10,000
c. $1.5 million
d. none of the above

## 6. FTC Data Breach Enforcement

**FTC, "Complying with the FTC's Health Breach Notification Rule", April 2010**

22. The FTC's Health Breach Notification Rule applies to which of the following entities:

a. HIPAA covered entities
b. vendors of personal health records
c. Business Associates of HIPAA covered entities
d. none of the above

23. The timing of the reports to be submitted to the FTC following a breach of the FTC's Health Breach Notification Rule varies depending on which of the following:

a. the number consumers directly affected by the violation
b. the size of the violator
c. increasing levels of culpability of the violator
d. none of the above

24. The Federal Trade Commission (FTC) can penalize an entity that has violated the FTC's Health Breach Notification Rule by reason of which of the following authorities of the FTC;

a. power to enforce compliance with HIPAA
b. power to prosecute violations of the Fourth Amendment to the US Constitution
c. power to prosecute unfair or deceptive act or practices in interstate commerce
d. none of the above