Martha Herz
HIT I
Chapter 10

1. Check your Understanding:

10.1

1. C. Availability.

2. C. They originate within an organization

3. D. Malware

4. C. Integrity

5. C. Employees

6. A. Computer Worm

7. B. Assisting in workforce data access clearances

8. D. Patient, employee, and organizational information.

10.2

1. B. People

2. D. Access Controls

3. B. Encryption

4. B. Annually

5. A. Include mandatory scheduled password changes

6. B. Filters information between networks

7. A. Risk analysis

8. B. Writing a policy regarding automatic computer logoffs

9. C. Two-Factor

10. C. Edit Checks

10.3

1. D. Assigning passwords that limit access to computer-stored information

2. A. Six years

3. D. Someone inside the organization must be responsible for data security

4. A. The employee and patient have the same last name

5. D. Data integrity

6. C. General rules

7. A. Must be identified by every covered entity

8. D. Data at rest, in motion and disposed

9. B. If not implemented, the organization must document why it is not reasonable and appropriate to do so.

10. B. Potential business associate liability was increased under HIPPA

2. Access control

Access safeguards- Identification of which employees should have access to what date; the general practice is that employees should have access sonly to data they need to do their jobs.

ARRA- American Recovery and Reinvestment Act- The purposes of this act include the following: to preserve and create jobs and promote economic recovery. To assist those most impacted by the recession, to provide investments needed to increase economic efficiency by spurring technological advances in science and health, to invest in transportation, environmental protection and other infrastructure that will provide long-term economic benefits, to stabilize state and local government budgets, in order to minimize and avoid reductions in essential services and counterproductive state and local tax increases.

Authentication- the process of identifying the source of health records entries by attaching handwritten signature, the author’s initials or and electronic signature. Proof of authorship that ensures as must as possible, that log-ins and message from a user originate from and authorized source.

CBAC- Context-based access control- an access control system which limits users to accessing information not only in accordance with their identity and role but to the location and time in which they are accessing the information.

Encryption- The process of transforming text in an unintelligible string of characters that can be transmitted via communications media with a high degree of security and then decrypted when it reaches a secure destination.

Edit check- Helps to ensure data integrity by allowing only reasonable and predetermined values to be entered into a computer.

Data availability- The extent to which healthcare data are accessible whenever and wherever they are needed.

Data integrity- the extent to which healthcare data are complete accurate, consistent and timely. Also a security principle that keeps information from being modified or otherwise corrupted either maliciously or accidently.

IDS- Intrusion detection system- a system that performs automated intrusion detection procedures should be outline in the organizations data security plan to determine what actions should be taken in response to a probable intrusion.

ITAD- Information technology asset disposition- policy that identifies how all data storage devices are destroyed and purged of data prior to repurposing or disposal.

HIPAA Security Rule- The federal regulations created to implement the security requirements of HIPAA.

Impact analysis- A collective term used to refer to any study that determines the benefit of a proposed projects, including cost benefit of a proposed project, including cost benefit analysis, and return on investment, benefits realization study, or qualitative benefit study.

Decryption-Data decoded and restored back to original readable form.

Edit check- Helps to ensure data integrity by allowing only reasonable and predetermined values to be entered into a computer.

Firewall- A computer system or a combination of systems that provides a security barrier or supports an access control policy between two networks or between a network and any other traffic outside network.

Network controls-A method of protecting data from unauthorized change and corruption at rest and during transmission among information systems.

Password-A series of characters that must be entered to authenticate user identity and gain access to a computer or specified portions of a database.

Security breach- Unauthorized data or system access

Risk analysis- The process of identifying possible security threats to the organization’s data and identifying which risks should be proactively addressed and which risks are lower in priority.

Risk management- A comprehensive program of activates intended to minimize the potential for injuries to cur in a facility and to anticipate and respond to ensuring liabilities for those injuries that do occur. The processes in place to identify evaluate and control risk, defined as the organization’s risk of accidental financial liability.

RBAC- Role-based access control- a control system in which access decisions are based on the roles of individual users as part of an organization.

PKI- Private key infrastructure- two or more computers share the same secret key and that key is used to both encrypt and decrypt a message; however the key must be kept secret and if it is compromised in any way the security of the data is likely to be eliminated.

UBAC- User-based access control – a security mechanism used to grant users of a system access based on identity.

e-PHI- Electronic protected health information.

Single - key encryption- more computers share the same secret key and that key is used to both encrypt and decrypt a message; however the key must be kept secret and if it is compromised in any way the security of the data is likely to be eliminated.

Single sign on- a type of technology that allows a user access to all disparate applications through one authentication procedure, thus reducing the number and variety of passwords a user must remember and enforcing and centralizing access control.

Trigger events-review of access logs, audit trails, failed logins, and other reports generated to monitor compliance with the polices and procedures.

1. **Name and describe** 4 examples of malware.

**Computer virus- a program that reproduces itself and attaches itself to legitimate programs on a computer. Computer viruses and change or corrupt data and often slow down the computer system.**

**Computer worm- a program that copies itself and spreads throughout a network but does no need to attach itself to a legitimate program.**

**Trojan horse- a programs that gains unauthorized access to a computer and masquerades as a useful function. A Trojan horse virus is capable of compromising data by copying confidential files to unprotected areas of the computer system, it may also copy and send themselves to e-mail address in a user’s computer.**

**Rootkit- a computer program designed to gain unauthorized access to a computer and assume control over the operating system and modify the operating system.**

1. **Name  and describe** 4 Access Safeguards

**Identification- The most basic access safeguard. Usually identification is performed through the username or user number. Identification methods must be robust so that imposters cannot successfully pose as a legitimate user and enter a system illegitimately.**

**Authentication- is the act of verifying a claim of identity. There are three different types - something you know (passwords), something you have (smart cards or tokens), or something you are (biometrics)**

**There is also two factor authentication- which is stronger than one type of authentication by requiring the user to provide two of the different types like a password and a token, a password and a fingerprint, or a token and a fingerprint.**

**Authorization- is a right or permission to an individual to use a computer resource such as a computer or to use specific applications and access specific data.**

5. HIPAA Security provisions:  **Name and describe**   3 Administrative safeguards.

Adminstrative safeguards include policies and procedures that address the management of computer resources. These safeguards may include polices such as

1. Requiring users log off the computers system when they are not using it or employ automatic logoffs after a period of inactivity.
2. Having password security requirements that include inappropriate sharing, minimum password requirements and changing and frequency of updating passwords and failed login monitoring and timely removal of terminated employee’s system access.
3. Prohibiting employees from accessing the internet for purposes that are not work related.