Chapter 10 Key terms

1. Check your Understanding:

10.1

1. c

2. c

3. d

4. c

5. c

6. a

7. b

8. d

9. a

10. c

10.2

1. b

2. d

3. b

4. b

5, a

6. b

7. a

8. b

9. c

10. c

10.3

1. d

2. a

3. d

4. a

5. b

6. c

7. a

8. d

9. b

10. b

2. Access control—restriction of access to information and information resources to only those who are authorized by role or other means.

Access safeguards .—fundamental security strategy means being able to id which employees should have access to what data

ARRA—American recovery and reinvestment act, moved the enforcement for hipaa security compliance from the cms office of electronic standards and security to the dhhs office fro civil rights.

Authentication—act of verifying a claim of identity

CBAC—context based access control limits a users access based not only on identity and role but also on a person’s location and time of access

Encryption—method of encoding data converting them to a jumble of unreadable scrambled characters and symbols as they are transmitted through a telecommunication network so that they are not understood by persons who do not have a key to transform the data into their original form.

Edit check—help to ensure data integrity by allowing only reasonable and predetermined values to be entered into the computer.

Data availability—making sure the organization can depend on the information system to perform as expected, and to provide information when and where it is needed

Data integrity—means that data are complete, accurate, consistent, and up to date so it is reliable

IDS—intrusion detection system a system that performs automated intrusion detection

ITAD—information technology asset disposition that identifies how all data storage devises are destroyed and purged of data prior to repurposing or disposal

HIPAA Security Rule—specify that covered entities must develop a security program that includes a range of security safeguards to protect individually identifiable health a9information maintained or transmitted in electronic form.

Impact analysis—estimate of the probability of threats occurring…is what the impact of threats or information assets might be.

Decryption—data can be decoded and restored back to their original readable form with a special algorithm.

Edit check—ensure data integrity by allowing only reasonable and predetermined valued to be entered in the computer.

Firewall—secure gateway is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.

Network controls—to prevent the threat of hackers

Password—part of authentication of who you are frequently used in conjunction with a username.

Security breach—unauthorized data or system access, by people from both inside and outside =the organization.

Risk analysis—iding security threats also includes identifying vulnerabilities, which are weaknesses in an organizations operations of which a threat can take advantage.

Risk management—encompasses the identification, evaluation and control of risks that are inherent in unexpected and inappropriate events.

RBAC—role-based access control one used most often in health care organizations

PKI—public key infrastructure uses both aq public and a private key which form a key pair

UBAC—user based access control based on a users individual id

e-PHI—electronic protected health informatin

Single - key encryption—two or more computers share the same secret key and that key is used to both encrypt and decrypt a message.

Single sign on—allows login to many separate, although related, software systems.

Trigger events

1. **Name and describe** 4 examples of malware.
2. **COMPUTER VIRUS—a program that reproduces itself and attaches itself to a legitimate program on a computer**
3. **Computer work—a program that copies itself and spreads throughout a network and does not need to attach itself to a legitimate program. It can execute and run on its own.**
4. **Trojan horse—a program that gains unauthorized access to a computer and masquerades as a useful function.**
5. **Spyware—computer program that tracks an individuals activity on a computer system.**

1. **Name  and describe** 4 Access Safeguards
2. **Identification—usually performed through the username or user number.**
3. **Authentication—act of verifying a claim of identity. Eg. Something you know, have or are.**
4. **Passwords—this is something you know frequently used in conjunction with user name.**
5. **Biometrics—something you are palm prints, fingerprints, voice prints and retinal scans.**

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

a. security management process—must have a defined security management process. Means that there is a process in place for creating, maintaining, and overseeing the development of security policies and procedures.

b. information access management- requires covered entities to implement a program of information access management

c. security incident procedures—requires the implementation of policies and procedures to address security incidents including responding to reporting and mitigating suspected or known incidents.