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. D

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. D
6. C
7. A
8. D
9. B
10. B

2. Access control- A computer software program designed to prevent unauthorized use of an information resource.

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

ARRA- American Recovery and Reinvestment Act; To preserve and create jobs and promote economic recovery.

Authentication- The process of identifying the source of health record entries by attaching handwritten signatures, initials, or an electronic signature.

CBAC- Context-Based access control; 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- Transforming text into an unintelligible string of characters that can be transmitted via communications media with a high degree of security.

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

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

Data integrity- Extent to which healthcare data are complete, accurate, consistent, and timely.

IDS- Intrusion Detection System, system that performs automated intrusion detection.

ITAD- Information Technology Asset Disposition, policy that identifies how all data storage devices are destroyed and purged of data.

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

Impact analysis- Any study that determines the benefit of a proposed project, including cost-benefit analysis, return on investment, benefits realization study, or qualitative benefit study.

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

Firewall- Computer system or combination of systems that provides a security barrier or supports an access control policy between two networks.

Network controls- method of protecting data from unauthorized change and corruption at rest and during transmission among 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- identifying possible security threats to the organization’s data and identifying which risks should be proactively addressed.

Risk management- program of activities intended to minimize potential injuries to occur in a facility.

RBAC- Role-Based Access Control

PKI- Public Key Infrastructure, in cryptography an asymmetric algorithm made publicly avalible to unlock a coded message.

UBAC- User-Based Access Control, access granted based on identity.

e-PHI- Electronic Private Health Information

Single - key encryption – two or more computers share the same secret key to encrypt and decode messages.

Single sign on- technology that allows access to information on many applications through one authentication procedure.

Trigger events- Review of access logs, audit trails, failed log ins and other reports generated to monitor compliance.

3. Name and describe 4 examples of malware.

Virus-program that reproduces itself and attaches itself to legitimate computer programs.

Trojan Horse- Program that gains access to a computer and masquerades as a useful function.

Spyware- Program that tracks an individuals activity, cookies are a form of spyware.

Worm- Program that copies and spread throughout a computer network without piggybacking on another program.

4. Name and describe 4 Access Safeguards

Identification- username or code

Passwords- the use of characters and numbers to create a secret code

Biometrics- fingerprint scanner, retinal scans, and voice prints.

Smart Cards- The use of one time regenerated codes for access through the smart card or coin.

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

Door Locks- making sure computer with access to PHI or files with PHI are behind locked doors that require a key code or card.

Policies- Administrators can make policies with how to correctly deal with PHI and braches.

Automatic Logout- Program that automatically logs a user out after disuse for so many minutes.