1. Check your Understanding:

10.1- 1. C 2. C 3. D 4. C 5. C 6. A 7. A 8. A 9. D 10. C

10.2- 1. B 2. D 3. B 4. B 5. C 6. A 7. B 8. D 9. A 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 that is designed to prevent unauthorized use of information.

Access safeguards – Identification of which employees should have access to what data. Employees should have access only to data they need for their job.

ARRA: American recovery and reinvestment act. To preserve and create jobs and promote economic recovery, to assist those most impacted by recession, provide investments needed to increase economic efficiency.

Authentication: The process of identifying the source of health record entries by attaching a handwritten signature, the authors, initials, or an e signature.

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

Encryption: The process of transforming text into 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 the 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. A security principle that keeps info from being modified or otherwise corrupted.

IDS: Intrusion detection system: a system that performs automated intrusion detection

ITAD: Information tech 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 Hippa

Impact analysis:

Decryption: Data decoded and restored to readable form

Security system: 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 the 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 proportion 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 activities intended to minimize the potential for injuries to occur in a facility and to anticipate and respond to ensuring liabilities for those injuries that do occur in a facility.

RBAC: role based access control: A technique used in performance improvement initiatives to discover the underlying causes of a problem. Analysis of a sentiment event from all aspects to identify how each contributed to the occurrence of the event and then prevent reoccurrence.

PKI: Public Key Infrastructure: In cryptography, an asymmetric algorithm made publicly available to unlock a coded message

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

e-PHI: electronic patient health information.

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: A type of tech that allows a user access to all disparate application through one authentication procedure.

Trigger events: Review of access logs, audit trails, failed logins, and other reports generated to monitor compliance with the policies and procedures

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

 1. A computer Virus: When a program reproduces itself, and attaches itself to “good” programs. A virus can even change or ruin data.

2. Computer Worm: A program that copies itself and spreads throughout a network. Computer worms don’t attach to another program. It runs itself.

3. A Trojan horse: A program that gains unauthorized access to a computer and masks itself as something useful/good. It damages data by copying files to unprotected areas of a computer system. Some will even send information via email.

4. Rootkit: a computer program that gains unauthorized access to a computer and takes over the operating system and modify the system.

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

 1. Identification: Identify an individual via username or user number. The methods should be robust to avoid imposters.

2. Authentication: verifying a claim of identity. For example, authenticating something you know, something you have, or something you are.

3. Passwords: something you know. It may be a PIN number, a password, mother’s maiden name, what school you graduated from, etc.

4. Biometrics: Something you are: Palm prints, finger prints, voice recognition, retinal eye scan

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

1. Workforce security: The covered entity must ensure appropriate clearance procedures to grant access to individually identifiable info to workforce members who need to use e-phi to perform duties. This is a way to prevent access to info to those who don’t need it and have clear procedures for terminated employees.

2. Information Access Management: This standard requires covered entities to implement a program of information access management. It ensures policies and procedures to determine who should have access to what information.

3. Evaluation: Periodically an evaluation is performed to respond to environmental or operational changes that affect security. Appropriate improvements that policies and procedures should follow.