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) d 6) c 7) a 8) d 9)b 10) b

2. Access control-a computerized 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.

Authentication- the process of identifying the source of health record entries by attaching a handwritten signature, the authors intials or an electronic signature.

CBAC-context based access control.am 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 into unintelligible string of characters that can be transmitted via communication 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 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.

IDS-integrated delivery system- a system that combines the financial and clinical aspects of healthcare and uses a group of healthcareproviders selected on the basis of quality and cost management criteria to furnish comprehensive health services across the continuum of care.

ITAD-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-a collective term used to refer to any study that determines the benefits of a proposed project, including cost-benefit analysis, return on investment benefit analysis, 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 the computer.

Firewall-a computer system or a combination of systems that provide 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 portions of a database.

Security breach-unauthorized data or system access.

Risk analysis-the process of identifying possible security threats to the organization data and identifying which risks should be practively 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.

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

PKI-in cryptography an asymetric algorithm made publicly available to unlock a coded message.

UBAC-a security mechanism used to grant users of a systemaccess based on identity.

e-PHI-unsecured electronic protected health information. That has not been made unusable unreadable or indecipherable to unauthorized persons.

Single - key encryption-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 elimanated.

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 complaince with the policies and procedures.

3.  **Name and describe** 4 examples of malware.Trojan Horse-disquises itself as a normal file or program to trick users into downloading and installing malware. Spyware- type of malware that functions by spying on user activity without their knowledge. Virus form of malware that is capable of copying itself and spreading to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Worm- most common type of malware. They soread over computer newtworks by exploiting operating systems vulnerabilities.Worms cause harm to their host networks by consuming bandwidth and overloading servers.

4. **Name  and describe** 4 Access Safeguards-identification- the basic block of access control if identifying the individual. Usually performed through a user name or number. Identification methods must be unique so imposters cannot successfully pose as legitimate users. Authentication- act of verifying a claim of identity. Something you know, something you have or something you are are the three types of information to authenticate an individual. Passwords- used in conjunction with username. Policies should be in place so passwords can not be compromised. Biometrics- palm prints,finger prints, voice prints and eye scans used for more security.

5. HIPAA Security provisions:  **Name and describe**   3 Administrative safeguards- Risk analysis. Process of identifying potential security risks, determine the probability of occurance and magnitude of risks. Risk Management.-Process used to identify and implement security measures to reduce risk to a reasonable and appropriate level within the covered entity.Sanction policy- appropriate sanctions must be in place so that the workforce members understandthe consquences of failing to comply with security ,policies,procedures to deter noncompliance.