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 – 1. A computer software program designed to prevent unauthorized use of an information resource 2. As amended by HITECH, a technical safeguard that requires a covered entity must in accordance with 164.306(a)(1) implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4) (45 CFR 164.312 2003)

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: The purposes of this act include the following: (1) To preserve and create jobs and promote economic recovery. (2) To assist those most impacted by the recession. (3) To provide investments needed to increase economic efficiency by spurring technological advances in science and health. (4) To invest in transportation, environmental protection, and other infrastructure that will provide long-term economic benefits. (5) 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 – 1. The process of identifying the source of health record entries by attaching a handwritten signature, the author’s initials, or an electronic signature 2. Proof of authorship that ensures, as much as possible, that log-ins and messages from a user originate from an authorized source 3. As amended by HITECH, means the corroboration that a person is the one claimed.

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 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 into the computer.

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

Data integrity – 1. The extent to which healthcare data are complete, accurate, consistent, and timely 2. A security principle that keeps information from being modified or otherwise corrupted either maliciously or accidentally

IDS – Integrated Delivery System: A system that combines the financial and clinical aspects of healthcare and uses a group of healthcare providers, selected on the basis of quality and cost management criteria, to furnish comprehensive health services across the continuum of care

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 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

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 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 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 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. 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 roles of individual users as part of an organization

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 – Unsecured electronic protected health information: e-PHI 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 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 policies and procedures

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

a) Computer Virus: A program that reproduces itself and attaches to legitimate programs on your computer.

b) Rootkit: A program which is designed to gain access to a computer and take over control of the computers operating system.

c) Trojan horse: A program which gains access to a computer and masks itself as a useful function. This program moves confidential information to unprotected areas of the computer.

  d) Spyware: A program that tracks activity on a computer, usually storing passwords.

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

  a) Role-based access control-This is when a person’s access is determined by the role they are in. For this method, everyone in the same role has the same access.

b) User-based access control-This is when a person’s access is set up at the user level. This method allows each individual employee to have unique access.

c) Context-based access control-This access takes role-based access or user-based access and refines it by utilizing time and location. For example, this form of access would allow you to define down to the unit where someone has access.

d)

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

a) A policy that instructs an employee to log off of their computer when they step away from their computer. This policy might also state that computers will automatically log off after a pre-set amount of time.

b) A policy which addresses password security, for instance password requirements, frequency of password changes or setting how many log in attempts before the system locks.

c) A policy in place that restricts employee access to the internet, only allowing access to perform work related functions.