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-D9-B 10-B**

2. Access control **Computer software program to prevent unauthorized access of information HITECH covered entity must be in compliance to allow only authorized access**

Access safeguards . **practice where employees have access only to data they need to do their jobs**

**ARRA American recovery and reinvestment act**

Authentication **process of identifying source of health record by signature initials or electronic signature**

**CBAC Context based access control**

Encryption **process of putting text into an unintelligible string of chacters that can be transmitted with high degree of security and then decrypted**

Edit **check helps by ensure data integrity by allowing reasonable and predetermined values to be entered**

Data availability **extent that data is accessible when needed**

Data integrity **extent data is completely accurate consistent and timely, keeps info from beinging modified or corrupted**

IDS **intrusion detection system**

ITAD **information technology asset disposition**

HIPAA Security **Rule federal regulations created to implement security requirements of the HIPAA**

Impact **analysis term used to a study to determine benefit of project includes cost benefit ROI benefits realization or qualitative benefit study**

Decryption **data decoded and restored back to readable form**

Edit check **helps by ensure data integrity by allowing reasonable and predetermined values to be entered**

**Firewall a computer system that provides security barrier or supports access control policy between 2 networks or network and outside network**

Network controls **method of protecting data from unauthorized change and corruption at rest or during transmission**

Password **series of characters entered into computer to authenticate user and gain access to computer or database**

Security **breach unauthorized data or system access**

Risk analysis **process of identify security threats to data which need to be addressed which are higher or lower**

Risk management **program of activities to minimized the potential for injuries too occur in a facility and to anticipate and respond to ensuring liabilities also to evaluate and control risk of organization financial liability**

**RBAC role based access control**

**PKI public key infrastructure**

UBAC **user based access control**

e-PHI **unsecured electronic protected health information**

Single **- key encryption 2 o to or more computers share same key to encrypt and decrypt message key must be kept secret and if compromised data security may be breached**

Single sign **on user can sign on using one authentication for all access needing only 1 password**

Trigger events **review of logs audit trails failed logons and other reports to monitor compliance**

3.  **Name and describe** 4 examples of malware***. Computer virus* program the reproduces itself and attaches itself to legitimated programs *computer worm* program that copies itself and spreads throughout the network *trogan* *horse* program gains unauthorized access and masquerades as a useful function *spyware*  program that tracks activity on computer system cookies are ie**

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

**Physical safeguards are protecting information physicialy from fire or theft floods loss of power and other disasters**

**Firewalls bocks unauthorized access a program that filters info between 2 networks blocks malicious hackers**

**Applications safeguards controls in applications software or computer programs to protect the security and integrity of information**

**Administrative safeguards policies and procedures that are put in place to address the management of computer resources**

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

Instructions:

***Physical safeguards* include protection of electronic systems from natural and environmental hazard and intrusion**

***Technical safeguards* consist of 5categories access controls, audit controls, integrity person or entity authentication, transmission security guarding of** **data**

***Policies and procedures is* a rule that entities’ and BA must have policies and procedures in writing to comply with hippaa rules documation must be retained for 6 years from date of creation must be reviewed and updated as needed**