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 computer software program designated to prevent unauthorized use of information, a safeguard that a covered entity must implement technical polocies 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

Access safeguards – identification of which employees should have access to what data

ARRA – American Recovery and Reinvestment Act – to preserve and create jobs and promote economic recovery, assist those most impacted by the recession, provide investments needed to increase economic efficiency by spurring technological advances in science and health, invest in transportation, environmental protection, to stabilize local and state government budgets

Authentication – process of identifying the source of health record entries by attaching a handwritten signature, initials, or electronic signature

CBAC – Context-based 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 – process of transforming text into an unintelligible string of characters that can be transmitted through communications with a high degree of security 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 – extent to which healthcare data are complete, accurate, consistant, 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 prior to repurposing or disposal

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

Impact analysis – term used to refer to any study that determines the benefit of a proposed project including cost benefit analysis, return n investment, benefits realization study, or qualitative benefit study

Decryption – data decoded and restored back to original readable form

Edit check – helps 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

RBAC – Role – based access control – a control system in which access decisions are based on the 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

Single sign on – a type of technology that allow the user access to all disparate applications through one authentication procedure

Trigger events – review of access logs, audit trails, failed logins, and other eports generated to monitor compliance with the polocies and procedures

3. Name and describe 4 examples of malware.

Computer Worm – program that copies itself and spreads throughout a network, it can execute and run itself

Spyware – computer program that tracks an individual’s activity on computer system

Computer virus – program that reproduces itself and attaches itself to legitimate programs on the computer

Trojan horse – program that gains unauthorized access to a computer and masquerades as a useful function

4. Name and describe 4 Access Safeguards

Identification – basic building block of access control is identification of an individual

Biometrics – palm prints, fingerprints, voice prints, and retinal scans

Single sign on – allows a user to sign on one time and have access many systems

Authorization – permission given to an individual to use a computer resource

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

Assigned security responsibility – each covered entity must designate a security official who has been assigned security responsibility for the development and implementation of the polocies and procedures required by the HIPAA Security rule

Information access management – this standard requires covered entities to implement a program of information access management

Security incident procedures – this standard requires entities to provide security training for all staff