Nicole Batchelder

MCO

12/04/2016

Chapter key term

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- computer software that was designed to prevent unauthorized use of an information resource

Access safeguards-identification of which employees should have access to which information

ARRA-american recovery and reinvestment act

Authentication-the process of identifying the source of health records entries

CBAC-context-based access control

Encryption-the process of transforming text into unintelligible string of characters that can be transmitted via communications media with a high degree of security

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 or wherever they are needed.

Data integrity-the extent to which healthcare data are complete, accurate, consistent and timely

IDS-integrated delivery system

ITAD-information technology asset disposition

HIPAA Security Rule-the federal regulation 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.

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 between a network and traffic outside of the network

Network controls-a method of protecting data from unauthorized change and corruption at rest and during trasmission among information systems

Password-a series of characters that must be entered to authenticate a user

Security breach-unauthorized data or system access

Risk analysis-the process of identifying possible security threats

Risk management-a program of activities intended to minimize the potential for injuries to occur

RBAC-role-based access control

PKI-public key infrastructure

UBAC-user-based access control

e-PHI-electronic protected health information

Single - key encryption-two or more computers share the same secret key to encrypt or decrypt messages

Single sign on-a type of technology that allows a user access to all disparate applications through one authentication procedure

Trigger events-review off access logs, audit trails, failed log ins, and other reports generated to monitor compliance

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

 -computer virus-a program that reproduces itself and attaches to legitimate programs on a computer

-computer worm-a program that copies itself and spread throughout a network

-trojan horse-a program that gains unauthorized access to a computer and masquerades as a useful function

-spyware-a computer program that that tracks an individual’s activity on a computer system

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

 Role-based access controls-identifying the access needed for a particular role to perform their job

User-based access controls-identifying the access needed for a particular employee to perform their job

Context-based access controls –limits users access based on their identity, role and location at time of access

Access controls-a restriction of access to information and information resources to only those who are authorized

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

-security management process-a process in place for creating, maintaining and overseeing the development of security policies

-assigned security responsibility-a designated security official who has been assigned security responsibility for the development and implementation of the policies

-workforce security-appropriate clearance procedure to grant access to individually identifiable information to workforce members

**Instructions:**