***Anita Hakala Homework*** *due*Sunday, December 4 at 11:55 PM*(Required)*

1. Check your Understanding:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **10.1** | **10.2** | **10.3** |
| 1 | C | B | D |
| 2 | C | D | A |
| 3 | D | B | D |
| 4 | C | B | A |
| 5 | C | A | D |
| 6 | A | B | C |
| 7 | B | A | A |
| 8 | D | B | D |
| 9 | A | C | B |
| 10 | C | C | B |

2.

**Access control:** 1. Computer software program designed to prevent unauthorized use of an information source 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 right as specified in 164.304 9a0 940 (45 CFR 164.31202003)

**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:**

**Authentication: 1.** The process of identifying the source of health record entries by attaching a handwritten signature, the authors 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 is an access control system which limits users to accessing only 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 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:** 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 is 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 a continuum of care

**ITAD:** Information Technology Asset Disposition is a 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 tern use 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 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 combination of systems that provides 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 at 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 isa 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 is a security mechanism used to grant users of a system access 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 if 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; also called **private key infrastructure:**

**Single sign on:** a type of technology that allows a user access to all disparate applications though one authentication procedure, thus reducing the number of passwords a user must remember and enforcing and centralizing control

**Trigger events:** Review of access logs, audit trails, failed log-ins, and other reports generated to monitor compliance with the policies and procedures

3.  **Name and describe** 4 examples of malware. (I put more than 4 to familiarize myself)

Malware is a software application that can take over partial or full control of a computer and can compromise data security and corrupt both data and hard drives.

 Examples:

**Computer virus**: a program that reproduces itself and attaches itself to legitimate programs on the computer. It can change or corrupt data and frequently slows down performance on the computer system.

**Computer worm:** A program that copies itself and spreads throughout a network. It can execute and run itself.

**Trojan Horse:** A program that gains unauthorized access to a computer and masquerades as a useful function. It is capable of compromising data by copying confidential files to unprotected area of a computer system. It may also copy and send themselves email addresses in a user’s computer.

**Spyware:** A computer program that tracks an individual’s activity on a computer system. Cookies are a type of spyware. It can store authentication information such as an individual’s password.

**Backdoor programs:** A computer program that bypasses normal authentication process and allows access to computer resources, such as programs, computer networks, or entire computer systems.

**Rootkit:** A computer program designed to gain unauthorized access to a computer and assume control over the operating system and modify the operating system

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

**Role-based access control**

**RBAC:** Role-based access control isa control system in which access decisions are based on the roles of individual users as part of an organization

**User-based access control**

**UBAC:** User-based access control is a security mechanism used to grant users of a system access based on identity

**Context based access control**

**CBAC**: limits a user’s access based not only on identity and role, but also on a person’s location and time of access

**Access control**

**Access control** is the restriction of access to information and information resources to only those authorized, by role or other means.

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

 Policies and procedures that address management of computer resources.

 Examples: Logging off computers when not in use

 Automatic log-off after a certain period of time

 Updating passwords

Policy on **Information Technology Asset Disposition (ITAD)** that identifies how all data storage devices are destroyed and purged of data prior to repurposing or disposal