**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 3 – Option C**

Names of team members: Corey Cooley, Taylor Payne, Will Brown, & John Hopson

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

The Health Insurance Portability and Accountability Act (HIPAA) was designed to help keep the protected health information (PHI) of consumers private and secure. The HITECH Act, passed in 2009, broadened the PHI protections afforded by HIPAA and enforced data breach notification requirements on covered entities and business associates. The Omnibus Regulations further amended the protections of HIPAA and HITECH in 2013.

Resources for HIPAA are numerous online. A good collection of articles can be found at:

<https://datica.com/academy/> (a vendor site, so some pushing of their product is to be expected).

Follow the article sequence here and then answer the following:

[HIPAA 101](https://datica.com/academy/hipaa-101-a-primer/)

[What is PHI?](https://datica.com/academy/what-is-protected-health-information-or-phi/)

[The HIPAA Privacy Rule](https://datica.com/academy/the-hipaa-privacy-rule/)

[The HIPAA Security Rule](https://datica.com/academy/the-hipaa-security-rule/)

[HIPAA Risk Assessment and Management](https://datica.com/academy/hipaa-risk-assessment-and-management/)

[HIPAA and Encryption](https://datica.com/academy/hipaa-and-encryption/)

[HIPAA and Data Breaches](https://datica.com/academy/hipaa-and-data-breaches/)

1. What/who are *covered entities*? *Business associates*? (5 pts.)

***Covered entities*** *are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.*

***Business associates*** *are people or entities that for a covered entity will perform or help in performance of specific business activities that use or could disclose PHI.*

*Examples include: data analysis, claims processing or administration, utilization review, and quality assurance reviews.*

2. Describe two methods of de-identifying PHI. Do you think the 18 elements considered to uniquely identify an individual are sufficient? Why or why not? (5 pts.)

*There are two methods of de-identifying PHI, the first by expert determination to ensure a small/negligible risk of re-identification which is validated by the expert. The second is to remove the 18 elements that are given. The 18 elements should be enough to uniquely identify an individual due to the amount of information stored about that one person. Most of these identifying characteristics are repeatable by another person, but the combination of birthdays with their fingerprints as well as social security number and physical identifiers like pictures should be sufficient to identify an individual.*

3. Describe the three major categories of safeguards in the Security Rule. Which is the largest area? (8 pts.)

*The first major category is the* ***Administrative*** *category. This is the largest category of safeguards, accounting for more than 50% of the rule. The administrative category consists of the policies and processes that need to be followed to safeguard data. The most important area in this category is risk assessment. The second category is the* ***Physical*** *category. This is the physical aspect of securing systems that have access to ePHI. It consists of workstations, facilities, and different portable and mobile media. This category also contains office security and workstation security(locking doors, tracking visitors, using workstation firewalls, etc). The third category is the* ***Technical*** *category. This category consists of encryption, access controls, and auditing. Encryption keeps files safe from prying eyes, and access controls and logging is necessary in order to monitor and receive alerts depending on context.*

4. What should be the first step in the process of securing ePHI? Explain your reasons. (7 pts.)

*Encryption of data should be the first step in securing ePHI. ePHI should be encrypted during storage and transmission at a high level such as 256-bit. Encryption will ensure that even if data is taken or intercepted it cannot be accessed or viewed in plaintext. As stated in the second chapter, it is more important to ensure confidentiality of data rather than worry about whose possession the data is in. There are many tools and ways encryption can be implemented and many different encryption levels. Firewalls and other security measures beyond the safeguards in the security rule can be taken as well, but none will provide as much data protection as encryption will if you system is breached.*