**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 3 – Option C**

Names of team members: **Trisia Baltazar, Adrian Boone, Savanah Kennedy, Ryan Smith**

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 health systems, payers, and clearinghouses. Business associates are entities that provide services to covered entities and through those services access, transmit, process, or store PHI (protected health information).**

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.)

**De-identification occurs when data has been stripped from common identifiers by two methods.**

**One method of de-identifying PHI is removing the eighteen elements. The elements are a core set of data elements that individually or in combination uniquely identify an individual. It is not sufficient because it is considered a bit outdated, such as fax numbers being an element instead of social media. The other method occurs when another approach is used. One must ensure a statistically small / negligible risk of re-identification which is validated by a statistics expert.**

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

**The three major categories of safeguards in the Security Rule are administrative, physical, and technical. Administrative is the largest category of safeguards, as it accounts for more than 50% of the rule. The administrative category covers the processes and policies needed to safeguard data. Risk assessments are the most important component of this category. Documenting architecture identifying risks related to PHI protecting, and mitigating those risks are all covered in risk assessments. Workforce security, contingency planning, and training are also covered in the administrative category.**

**The physical category covers the physical aspect of securing systems that have access to ePHI. Securing physical objects such as data centers, workstations, facilities, and different mobile and portable media are covered in this category. Complaint Infrastructure-as-a-Service (IaaS) vendors help organizations cover this category of HIPAA. Office security and workstation security are physical areas that need to be secured. Policies such as locking doors and not allowing cleaning stuff in offices unsupervised are policies that could be taken to help the physical category, although these are not hard safeguards.**

**The technical category covers the technical aspects of securing ePHI. Encryption, access controls, and auditing are included in this category. Encryption must be end to end and at rest. High performance SSD drives help improve issues with encrypting at rest data. Access controls mean that all server activity should be logged and those logs should be monitored. Appropriate alerting should be possible with monitoring the logs. The logs should include what was accessed, by whom, and when.**

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

**The first step in the process of securing ePHI should be to educate employees on the importance of securing ePHI and provide guidelines on how to do that. The reasoning for this is that the vast majority of ePHI data breaches comes from hardware breaches, not software. These breaches are usually due to employee carelessness. An unencrypted employee laptop that stores ePHI could be lost or stolen for example. Actual software or “hacking” breaches account for a much smaller number of breaches. An organization can reduce the chance of hardware breaches simply through employee training and there ePHI will be much more secure. It is an easy and cheap way to begin the process of securing ePHI.**