CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 3 – Option C

Names of team members: Danna Penaranda, Ben Spalding, James Ryg, and Maam Awa Ndaw

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://catalyze.io/learn (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
What is PHI?
The HIPAA Privacy Rule
The HIPAA Security Rule
HIPAA Risk Assessment and Management
HIPAA and Encryption
HIPAA and Data Breaches

1. What/who are *covered entities*?
   They are heavily associated health care actors such as providers, hospitals, health systems and insurers. For instance, Humana is a covered entity because it is provider of health insurance. Some clearinghouses that process payments for example a hospital is another example of a covered entities.

   Business associates? (5 pts.)
   Individuals and organizations that provide services and technology for the covered entities. If they conduct business and interact with Personal Health Information from these covered entities, then they are business associates under the Privacy Rule of HIPAA. For example, HP is a business associate for Humana by providing

customized software to process high volume documentation for all Humana's customers. The software, called HP Exstream software Humana, Inc., deals with HIPAA's Privacy Rule regarding PHI.[1]

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.)

   Personal Health Information contains uniquely identifiable pieces of data to recognize for instance a unique patient. The examples of unique identifiers that can reveal the identity of a patient/client are as name, SSN, e-mail address, phone number, medical records number, health claim beneficiary number, account numbers, certificate/license numbers, vehicle identifiers and serial numbers including license plates numbers, biometric identifiers, and full face photos.

   In the process of Safe Harbor, PHI can be de-identified by deleting some attributes from a record. The other method, called expert determination, uses the interpretation of an expert to decide which information in a data set is not individually identifiable.[2] In this last method, a company can assign an expert with data handling background in science, statistics, and mathematics PHI is unidentifiable. The capabilities of this individual is the only assurance to wipe PHI in databases.

   We think that these 18 elements are enough to identify anyone because these elements already exist in many other information systems. For instance, an e-mail address is used to open bank accounts. If a hacker gets access of an e-mail account, then it is very likely that he/she could imposture the bank account's owner and request a password reset.

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

The three main safeguards in the Security Rule are: (1) Administrative, (2) Physical, and (3) Technical.

1. Administrative safeguards are the largest area, and encompass policies regarding sensitive data. Examples include process and policy for employees and a focus on recognizing risk.

2. Physical safeguards are the tangible l aspects of securing systems that have access to ePHI. Some examples would be badges and metal detectors.

3. Technical safeguards are protection methods such as encryption, access controls, and auditing.

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 add encryption. Even though administrative safeguards are the biggest portion of the security rule, and they are the most important, a business must first ensure that if there is a breach of possession, then there will not be a breach of confidentiality.

Endnotes

[1] Case study. http://welcome.hp.com/country/us/en/prodserv/software/eda/pdf/Humana_Case_Study.pdf

[2] From the link provided at https://catalyze.io/learn/the-hipaa-privacy-rule