CIS 481 – Intro to Information Security

Understanding HIPAA and its Effects on Information Security and the Business Environment by Danna Penaranda

"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." Dr. Wright, Assistant Professor, University of Louisville, Computer Information Systems, College of Business

HIPAA's 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. In essence, they are direct providers.

HIPAA's Business associates

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] In short, they have operations with direct providers.

In discussing the two methods of de-identifying PHI and the 18 elements to uniquely identify an individual.

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. This expert's skills are the only assurance to wipe PHI in databases.

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.

HIPAA's Security Rule and its three main safeguards: (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.

The first step in the process of securing ePHI

Risk assessment is the first step before deciding what to encrypt. 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] https://catalyze.io/learn/the-hipaa-privacy-rule
Personal Health Information found here

What is PHI?
HIPAA Privacy Rule
HIPAA Security Rule
HIPAA Risk Assessment and Management
HIPAA and Encryption