# Lab - Recommend Security Measures to Meet Compliance Requirements

## Objectives

**Part 1: Investigate compliance requirements**

**Part 2: Recommend compliance solutions**

## Background

Compliance with relevant security and privacy standards is a challenge for most businesses. Compliance is often complex, and the stakes are high. Businesses frequently outsource much of the burden of compliance to companies that specialize in providing solutions that have proven to meet compliance requirements and satisfy compliance audits.

In this lab, you will investigate compliance requirements and recommend measures to meet HIPAA requirements. The Health Insurance Portability and Accountability Act (HIPAA) is a set of regulations created in the United States to protect the privacy and rights of healthcare patients. It controls how patient healthcare information can be shared. It specifies detailed requirements that are designed to protect patient privacy and security.

All healthcare providers in the United States, from the smallest office to the largest hospitals, must comply with HIPAA. Many service providers have entered the market to assist healthcare providers in reaching HIPAA compliance.

## Scenario

Dr. Anthony Larouche, a dentist, has been working in a large dental office with other dentists. He has decided to open his own office. All the office-related IT systems were handled by his office staff. He knows little about computer networks and network security. He has hired your company as consultants to help him comply with the HIPAA technical security requirements.

You have been asked to create a list of specific requirements that will meet the Technical Safeguards under the Security Rule of the HIPAA compliance regulations.

## Required Resources

- Computer or other device with internet connection

## Instructions

### Part 1: Investigate compliance requirements

In this part, you will review the requirements for complying with the HIPAA security specifications. HIPAA regulations consist of two rules, the Privacy Rule and the Security Rule. We will focus on the Security Rule, which consists of safeguards, standards, and implementation specifications. There are five security standards in the technical safeguard. Some of the standards have several associated implementation specifications. Some standards have no implementation specifications.

### Step 1: Become familiar with HIPAA Safeguards

Search the web to learn more about the HIPAA Security Rule Safeguards. A good search for a general overview is **site:compliancy-group.com hipaa security rule**. Answer the following questions.

## **TASK 1**

1. **What are three examples of protected health information?**

**ANSWER**

Name, address, date of birth

2. **Summarize the four general rules that all healthcare organizations must follow as regards the Security Rule.**

**ANSWER**

1. Ensure confidentiality, integrity, and availability of all electronic protected healthcare information.
2. Identify and protect against cyber threats
3. Ensure all sensitive data are encrypted
4. Protect against impermissible uses or disclosures

3. **What are the three types of safeguards that make up the HIPAA security rule?**

**ANSWER**

Administrative, Physical and Technical

## **TASK 2**

### Step 2: Review Technical Safeguard documents

a. Please refer to this document for clarification regarding the Technical Security Standards 164.312 (a) - (e)(2)(ii) and the treatment of electronic protected health information (EPHI). Consult other internet sources for additional clarification. Quickly review the contents of the document.

b. Complete the table below with the standard names and implementation specifications for the standards, where applicable. Two of the standards have no implementation specifications.

****ANSWER****

| Technical Safeguards | | |
|---|---|---|
| **Section** | **Standard** | **Implementation Specifications** |
| 164.312(a)(1) | Access Control | 1. Unique User Identification (Required)<br>2. Emergency Access Procedure (Required)<br>3. Automatic Logoff (Addressable)<br>4. Encryption and Decryption (Addressable) |
| 164.312(b) | Audit Controls | N/A |
| 164.312(c)(1) | Integrity | 1. Mechanism To Authenticate Electronic Protected Health Information |
| 164.312(d) | Person or Entity Authentication | N/A |
| 164.312(e)(1) | Transmission Security | 1. Integrity Controls (Addressable)<br>2. Encryption (Addressable) |

****TASK 3****

## Part 2: Recommend compliance solutions.

The HIPAA technical security specifications should suggest security measures that will enhance or fulfill compliance with each requirement. Complete the table below with your recommendations. Use the knowledge that you have gained in the course so far and perform additional internet searches. You will find that there are many solutions available from companies that address each HIPAA standard.

****ANSWER****

| Standard | Name | Control |
|---|---|---|
| **164.312(a)(1)** | **Access Control** | |
| 164.312(a)(2)(i) | Unique User Identification | All users should have unique usernames not only for login but also to identify who has created, edited, or accessed EPHI. |
| 164.312(a)(2)(ii) | Emergency Access Procedure | Mirrored HDD storage of records, backups, use of secure cloud for data storage and retrieval. |

| Standard | Name | Control |
|---|---|---|
| 164.312(a)(2)(iii) | Automatic Logoff | All computers should be set with security policies to logoff after an idle period. Configure relevant applications to automatically log users off after an idle period as well. |
| 164.312(a)(2)(iv) | Encryption And Decryption | Identify information to be encrypted, encrypt server HDD, either in software or with auto-encrypting drives. |
| 164.312(b) | **Audit Controls** | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. |
| **164.312(c)(1)** | **Integrity** | |
| 164.312(c)(2) | Mechanism To Authenticate Electronic Protected Health Information | Implement file integrity monitoring (FIM) |
| 164.312(d) | **Person or Entity Authentication** | Multi-factor authentication (MFA), questions for password reset, biometric authentication |
| **164.312(e)(1)** | **Transmission Security** | |
| 164.312(e)(2)(i) | Integrity Controls | communications security hashing on transmitted documents, secure deletion of emails and other EPHI documents |
| 164.312(e)(2)(ii) | Encryption | Secure transmission WPA2 or better wireless, VPN for remote access, encrypted email, HTTPS, removing EPHI from unencrypted email such as forwards and responses. |

****TASK 4****

## Reflection Questions

1. There are many compliance frameworks that impose requirements on network security. The relevance of these frameworks depends on the type of business and the business activities that are conducted. PCI-DSS is a compliance framework for businesses that accept credit cards for

payment. Search the web for **PCI-DSS control objectives**. Each objective has one or more requirements. From your searches, complete that table below:

****ANSWER****

| PCI-DSS Objectives | PCI-DSS Requirements |
|---|---|
| Establish and maintain a secure network. | • Install firewalls and web filtering to protect cardholder data.<br>• Change default or vendor-supplied device security configurations. |
| Protect payment card and cardholder data. | • Protect cardholder data stored on company servers or networks.<br>• Encrypt and protect cardholder data transmitted over open and public networks. |
| Maintain a vulnerability management program. | • Use and keep up-to-date antivirus and malware software to protect cardholder data.<br>• Develop and maintain secure systems and applications. Use secure protocols in all applications. |
| Implement strong access control measures. Protect identity and access management. | • Restrict access to cardholder data by need-to-know.<br>• Restrict all access to cardholder data to authenticated users and assign a unique ID to each person with access.<br>• Limit physical access to cardholder data through physical hardware and devices. |
| Monitor and test networks and network traffic regularly and regularly evaluate their effectiveness. | • Monitor all access to network resources and especially cardholder data.<br>• Regularly evaluate and test the effectiveness of existing security systems and processes. |
| Maintain a personnel-wide information security policy. | • Maintain a policy that addresses information security, is accessible, and appealing to all personnel. |

2. **How do these compliance requirements compare to the HIPAA requirements that you supplied above?**

****ANSWER****

I think they are very much similar. These requirements both aims to protect data and information from unauthorize use and access. The only difference is that HIPAA is specifically for healthcare

centers and medical professionals while PCI-DSS is for the businesses that uses credit cards information.

3. **Compliance frameworks such as HIPAA and PCI-DSS pertain to not only large organizations, but also small ones. For example, all medical professionals must comply with HIPAA. All businesses that take credit cards must comply with PCI-DSS. In fact, medical practices that accept credit cards must comply with both. From your experience researching in this lab, what do you see as the some of the major challenges for compliance of smaller organizations?**

   ****ANSWER****

   The major challenges I can see here is limited resources. Unlike larger companies, small businesses often operate with tight budgets and cannot afford proper compliance teams that would help them to adhere to the industry standards and laws. Additionally, the cost of implementing necessary safeguards such as data encryption, secure storage, regular audits, and employee training can be overwhelming. With minimal financial and human resources, small organizations struggle to balance day-to-day operations with the demands of regulatory compliance, making it difficult to meet the required standards consistently.