**Nama : Sasmita Rachmawati**
**Absen : 15**

## 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 of 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.

Questions:

What are three examples of protected health information?

1. Medical records: Any documentation related to a patient's medical history, diagnoses, or treatments.
2. Billing information: Financial data related to healthcare services, such as insurance details or patient payment records.
3. Communication records: Any data shared between a healthcare provider and a patient, including appointment reminders and test results sent via email or phone.

Show Answer

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

1. Ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI
2. Protect against any reasonably anticipated threats
3. Protect against any reasonably anticipated impermissible uses or disclosures:
4. Ensure compliance by the workforce

Show Answer

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

1. **Administrative Safeguards**: Policies and procedures designed to clearly show how the entity will comply with the act.
2. **Physical Safeguards**: Measures to protect electronic systems, equipment, and the data they hold from threats, environmental hazards, and unauthorized intrusion.
3. **Technical Safeguards**: The technology and the policies for its use that protect ePHI and control access to it.

Show Answer

**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.

| **Technical Safeguards** | | |
|---|---|---|
| **Section** | **Standard** | **Implementation Specifications** |
| 164.312(a)(1) | Access Control | Unique user identification, emergency access procedure, automatic logoff, encryption and decryption |
| 164.312(b) | Audit Controls | No specific implementation required |
| 164.312(c)(1) | Integrity | Mechanism to authenticate ePHI |
| 164.312(d) | Person or Entity Authentication | Verify that persons or entities seeking access are who they claim to be |
| 164.312(e)(1) | Answer Transmission Security | Integrity controls, encryption |

Click **Show Answer** to a sample answer table.

Show Answer

**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.

| **Standard** | **Name** | **Control** |
|---|---|---|
| **164.312(a)(1)** | **Access Control** | |
| 164.312(a)(2)(i) | Unique User Identification | Ensure each user has a unique login ID and track system access using detailed audit logs. Assign unique credentials for identification. |
| 164.312(a)(2)(ii) | Emergency Access Procedure | Establish and document an emergency access protocol for authorized personnel to access ePHI during critical situations or system failures. |
| 164.312(a)(2)(iii) | Automatic Logoff | Implement session timeouts that automatically log users out after a period of inactivity to prevent unauthorized access. |
| 164.312(a)(2)(iv) | Encryption and Decryption | Encrypt ePHI both at rest and in transit using modern encryption standards like AES-256 and SSL/TLS for transmission. |
| 164.312(b) | Audit Controls | Set up automated logging systems that track and record user activities related to ePHI. Regularly review audit logs for suspicious or unauthorized access. |
| **164.312(c)(1)** | **Integrity** | |
| 164.312(c)(2) | Mechanism to Authenticate ePHI | Implement mechanisms that verify data integrity, such as integrity validation tools or file integrity monitoring systems. |
| 164.312(d) | Person or Entity Authentication | Require biometric verification, smart cards, or token-based authentication to confirm the identity of any individual attempting to access ePHI. |
| **164.312(e)(1)** | **Transmission Security** | |
| 164.312(e)(2)(i) | Integrity Controls | Implement cryptographic integrity checks to prevent ePHI from being altered during transmission. Employ TLS and other encryption methods. |
| 164.312(e)(2)(ii) | Encryption | Encrypt all ePHI transmitted over public or unsecured networks. Ensure encryption keys are managed securely to protect against unauthorized access. |

Click **Show Answer** to a sample answer table.

Show Answer

**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:

| PCI-DSS Objectives | PCI-DSS Requirements |
|---|---|
| Build and Maintain a Secure Network | Install and maintain a firewall configuration to protect data |
| Protect Cardholder Data | Encrypt transmission of cardholder data across open networks |
| Maintain a Vulnerability Management Program | Use and regularly update anti-virus software or programs |
| Implement strong access control measures | Restrict access to cardholder data on a need-to-know basis |
| Regularly Monitor and Test Networks | Track and monitor all access to network resources and data |
| Maintain an information security policy | Maintain a policy that addresses information security for all personnel. |

Click **Show Answer** to a sample answer table.

Show Answer

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

- HIPAA and PCI-DSS share many similarities, especially in their focus on protecting sensitive data through encryption, access controls, and regular audits. Both frameworks require that organizations maintain strict security policies, use encryption to protect data in transit and storage, and monitor user access. However, HIPAA is specific to healthcare data (ePHI), while PCI-DSS is focused on protecting payment card information.

Show Answer

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?

- Smaller organizations often face significant challenges in compliance due to limited financial and technical resources. Some of the major hurdles include:
  1. **Cost of compliance**: Implementing encryption, audit systems, and maintaining secure networks can be expensive.
  2. **Lack of expertise**: Smaller organizations may not have dedicated IT staff with expertise in security standards.

3. **Administrative burden**: The effort required to continuously monitor and update systems, conduct audits, and train employees can strain limited staff resources.

Show Answer