## Nama : Mochammad Aldo Rizky

## NIM : 2141762002

## Kelas : SIB 4C

# 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

## 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.

What are three examples of protected health information?

Three examples of protected health information (PHI) are:

**Name, Address, Birthday**

**name, address, birthday**

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

Here's a summary of the four general rules that all healthcare organizations must follow regarding the Security Rule:

1. **Ensure Confidentiality, Integrity, and Availability**
2. **Identify and Protect Against Cyber Threats**
3. **Protect Against Impermissible Uses or Disclosures**
4. **Ensure Compliance of Workforce**

**1. Ensure confidentiality, integrity, and availability of all electronic protected healthcare information.**
**2. Identify and protect against cyber threats**
**3. Protect against impermissible uses or disclosures**
**4. Ensure compliance of workforce.**

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

The three types of safeguards that make up the HIPAA Security Rule are:

1. **Administrative Safeguards**
2. **Physical Safeguards**
3. **Technical Safeguards**

**Administrative, Physical, and Technical**

## 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.

**(R) = Required**

**(A) = Addressable**

| Technical Safeguards | | |
|---|---|---|
| **Section** | **Standard** | **Implementation Specifications** |
| 164.312(a)(1) | Access Control | - Unique User Identification (R)<br>- Emergency Access Procedure (R)<br>- Automatic Logoff (A)<br>- Encryption and Decryption (A) |
| 164.312(b) | Audit Controls | (No implementation specifications) |
| 164.312(c)(1) | Integrity | - Mechanism to Authenticate Electronic Protected Health Information (A) |
| 164.312(d) | Person or Entity Authentication | (No implementation specifications) |
| 164.312(e)(1) | Transmission Security | - Integrity Controls (A)<br>- Encryption (A) |

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

## 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 | - Assign unique username/ID to each user<br>- Prohibit shared logins/accounts<br>- Use employee ID numbers as unique identifiers<br>- Implement single sign-on (SSO) solution |

| Standard | Name | Control |
|---|---|---|
| 164.312(a)(2)(ii) | Emergency access procedure | - Create formal emergency access policy/procedure<br>- Designate emergency access roles/personnel<br>- Implement "break-glass" emergency access protocols<br>- Conduct regular emergency access testing/drills |
| 164.312(a)(2)(iii) | Automatic logoff | - Configure automatic logoff after period of inactivity<br>- Use screen locks on all devices<br>- Implement session timeouts for applications<br>- Deploy endpoint management solution |
| 164.312(a)(2)(iv) | Encryption and decryption | - Implement full-disk encryption on all devices<br>- Use TLS/SSL for all data transmissions<br>- Deploy key management system<br>- Encrypt data at rest in databases/storage |
| 164.312(b) | Audit controls | - Implement centralized logging and monitoring system<br>- Deploy security information and event management (SIEM) solution<br>- Conduct regular log reviews and audits<br>- Enable detailed audit logging on all systems |
| **164.312(c)(1)** | **Integrity** | |
| 164.312(c)(2) | Mechanism to authenticate electronic protected health information | - Implement digital signatures to verify data integrity<br>- Use checksums/hashing to confirm data has not been altered<br>- Regularly audit the systems for unauthorized data alteration<br>- Deploy data integrity monitoring tools to identify unauthorized changes<br>- Implement encryption mechanisms to protect data integrity during transmission |
| 164.312(d) | Person or entity authentication | - Implement multi-factor authentication (MFA) to verify users<br>- Utilize biometric authentication methods (e.g., fingerprint or facial recognition)<br>- Deploy strong password policies and complexity requirements<br>- Implement user identity proofing before granting access<br>- Use hardware tokens or smart cards for authentication |

| Standard | Name | Control |
|---|---|---|
| **164.312(e)(1)** | **Transmission Security** | |
| 164.312(e)(2)(i) | Integrity controls | - Implement message authentication codes (MACs) to detect data tampering<br>- Use digital signatures for data integrity verification<br>- Deploy secure file transfer protocols (SFTP, FTPS)<br>- Implement error-checking and data validation mechanisms<br>- Regularly monitor and audit data transmission logs |
| 164.312(e)(2)(ii) | Encryption | - Use strong encryption algorithms (e.g., AES) for data in transit<br>- Implement Transport Layer Security (TLS) for web-based transmissions<br>- Deploy Virtual Private Networks (VPNs) for secure remote access<br>- Use end-to-end encryption for email communications<br>- Regularly update and patch encryption software and protocols |

| 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. |
| 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 AAA accounting and document version tracking. |
| **164.312(c)(1)** | **Integrity** | |
| 164.312(c)(2) | Mechanism to authenticate electronic protected health information (EPHI) | Implement file integrity monitoring (FIM) |
| 164.312(d) | Person or Entity Authentication | Multi-factor authentication (MFA), questions for password reset, biometric authentication |

| Standard | Name | Control |
|---|---|---|
| **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. |

## 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 cardholder data<br>• Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data | • Protect stored cardholder data<br>• Encrypt transmission of cardholder data across open, public networks |
| Maintain a vulnerability management program | • Use and regularly update anti-virus software or programs<br>• Develop and maintain secure systems and applications |
| Implement strong access control measures | • Restrict access to cardholder data by business need-to-know<br>• Assign a unique ID to each person with computer access<br>• Restrict physical access to cardholder data |
| Regularly monitor and test networks | • Track and monitor all access to network resources and cardholder data<br>• Regularly test security systems and processes |
| Maintain an information security policy | • Maintain a policy that addresses information security for all personnel |

| PCI-DSS Objectives | PCI-DSS Requirements |
|---|---|
| Build and maintain a secure network. | = Install and maintain a firewall configuration to protect card holder data.<br>= Do not use vendor-supplied defaults for system passwords and other security parameters. |

| PCI-DSS Objectives | PCI-DSS Requirements |
|---|---|
| Protect cardholder data. | = Protect stored cardholder data.<br>= Encrypt transmission of cardholder data across open, public networks. |
| Maintain a vulnerability management program. | = Use and regularly update anti-virus software.<br>= Develop and maintain secure systems and applications. |
| Implement strong access control measures. | = Restrict access to cardholder data by business need-to-know.<br>= Assign a unique ID to each person with computer access.<br>= Restrict physical access to cardholder data. |
| Regularly monitor and test networks. | = Track and monitor all access to network resources and cardholder data.<br>= Regularly test security systems and processes. |
| Maintain an information security policy. | = Maintain a policy that addresses information security for all personnel. |

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

   You're right that there are many similarities between the PCI-DSS requirements I provided earlier and the HIPAA compliance requirements outlined in these search results. Both frameworks focus on protecting sensitive data through administrative, physical, and technical safeguards. However, there are some key differences in scope and specifics:

   1. Scope:
      - PCI-DSS is specifically focused on protecting credit card data and applies to businesses that handle card payments.
      - HIPAA is broader, covering all protected health information (PHI) and applies to healthcare providers, insurers, and their business associates.
   2. Specific Requirements:
      - PCI-DSS has more prescriptive technical requirements, like specific firewall configurations and encryption standards.
      - HIPAA is more flexible, allowing organizations to determine appropriate security measures based on their size, complexity, and risk analysis.
   3. Privacy Focus:
      - HIPAA has a strong emphasis on patient privacy rights and consent for data sharing, which isn't present in PCI-DSS.
      - PCI-DSS is primarily concerned with data security rather than privacy.
   4. Breach Notification:
      - HIPAA has specific requirements for notifying patients and authorities in case of data breaches.

- PCI-DSS focuses more on prevention and doesn't have the same level of breach notification requirements.

5. Risk Analysis:
   - While both require risk assessments, HIPAA places a stronger emphasis on ongoing risk analysis and management.
6. Training:
   - HIPAA explicitly requires workforce training on privacy and security, which is not as prominent in PCI-DSS.

While there is significant overlap in the general security principles (like access control, encryption, and monitoring), the specific implementation and focus areas differ between the two frameworks due to the different types of data and industries they cover.

**They are very similar. Most of them are common sense security requirements that are familiar.**

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?

   Based on the research results provided, some of the major challenges for compliance of smaller organizations with frameworks like HIPAA and PCI-DSS include:

   1. Limited resources and expertise: Small businesses often lack dedicated IT or compliance staff to fully understand and implement complex requirements. As noted in the search results, "small businesses often run with the mentality that since they are too small, they don't need to be compliant".
   2. Cost of implementation: Implementing necessary security measures, software, and systems can be expensive for small organizations with limited budgets. The search results mention that "the average cost of PCI compliance for the affected small businesses went over USD 300,000 annually".
   3. Ongoing maintenance and updates: Compliance is not a one-time event but requires continuous monitoring, updates, and training. As stated, "Compliance is not a one-time event but an ongoing process".
   4. Complexity of requirements: Understanding and interpreting the specific requirements applicable to their business can be challenging for small organizations. The search results note that "PCI DSS rules may seem complex, technical, and more than a bit daunting".
   5. Legacy systems and technology: Older systems may not meet current compliance standards and can be difficult or costly to upgrade. The research mentions challenges with "legacy systems fit[ting] the current regulations".
   6. Employee training and awareness: Ensuring all staff members understand and follow compliance procedures can be difficult for small businesses. The need for "annual compliance training" is highlighted.
   7. Risk assessment and management: Conducting thorough risk assessments and implementing appropriate controls may be challenging without specialized knowledge.
   8. Documentation and reporting: Maintaining detailed records and producing required compliance reports can be time-consuming for small organizations with limited staff.
   9. Keeping up with regulatory changes: Staying informed about updates to compliance requirements and adapting accordingly can be challenging for small businesses focused on day-to-day operations.
   10. Balancing compliance with business operations: Small organizations may struggle to integrate compliance measures without disrupting their core business activities.

These challenges highlight the need for small organizations to carefully plan their compliance strategies, potentially seeking external expertise or leveraging technology solutions to manage compliance effectively.

**Answers will vary. There are many. One of the big ones is assessment of compliance. Organizations must not only implement the measures that are required, but must also prove that they comply by passing security audits, undergoing vulnerability assessments, and compiling reports to support compliance.**