Nama : M. Daffa Farrell. A

Kelas : SIB-4C

No : 07

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.

What are three examples of protected health information?

name, address, birthday

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

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?

Administrative, Physical, and Technical

Answer

- Administarive : Covered entities are required to implement administrative safeguards, which are policies and procedures that describe how the organization intends to protect ePHI and ensure compliance of the Security Rule. Examples include preparing a data backup plan and password management processes, among other things. These standards are laid out in §164.308 of the Security Rule.
- Physical : These safeguards refer to both the physical structure of an organization and its electronic equipment.
- Technical : This component includes the policies and procedures that determine how technology protects ePHI as well as who controls access to that data. Typically, due to the level of technical literacy needed to understand this regulation, it is the most difficult for entities to understand.

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 Control	None
164.312(c)(1)	Integitry	Mechanism to Authenticate ePHI
164.312(d)	Person or Entity Authentication	None
164.312(e)(1)	Transmission Security	Integrity Controls, Encryption

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	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 • 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	All users should have unique usernames to track who accessed or modified ePHI.
164.312(a)(2)(ii)	Emergency Access Procedure	Use backup storage, secure cloud systems, and ensure procedures for accessing records in emergencies.
164.312(a)(2)(iii)	Automatic Logoff	Configure automatic logoff policies for systems after a period of inactivity.
164.312(a)(2)(iv)	Encryption and Decryption	Encrypt sensitive data at rest and in transit using modern encryption methods (e.g., AES, TLS).
164.312(b)	Audit Controls	Implement logging of access and activity, audit trails, and regular review of access logs.
164.312(c)(1)	**Integrity**	
164.312(c)(2)	Mechanism to Authenticate ePHI	Use digital signatures and checksums to verify ePHI integrity.
164.312(d)	Person or Entity Authentication	Implement Multi-Factor Authentication (MFA), biometrics, and strict password policies.
164.312(e)(1)	**Transmission Security**	
164.312(e)(2)(i)	Integrity Controls	Use secure email services and encrypt communication channels to ensure data integrity.
164.312(e)(2)(ii)	Encryption	Secure email, WPA2 or better wireless encryption, and remove ePHI from unencrypted email threads.

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

Maintain a vulnerability management program.	• Use and regularly update anti-virus software. • Develop and maintain secure systems and applications.
Implement strong access control measures.	• Restrict access to cardholder data by business need-to-know. • Assign a unique ID to each person with computer access. • Restrict physical access to cardholder data.
Regularly monitor and test networks.	• Track and monitor all access to network resources and cardholder data. • 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?

   Both frameworks focus on similar security fundamentals, such as access control, encryption, and monitoring. They share common goals, including the protection of sensitive data, whether it's health-related (HIPAA) or financial (PCI-DSS).

   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?

   Smaller organizations may face challenges in terms of resources—both in terms of staff expertise and financial capacity. Compliance requires continuous monitoring, regular audits, and security updates, which can be difficult for small teams to maintain. Additionally, proving compliance through reports, audits, and vulnerability assessments can be a significant burden for organizations without dedicated IT staff.

   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.