Lab - Recommend Security Measures to Meet ComplianceRequirements

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 isoften complex and the stakes are high. Businesses frequently outsource much of the burden of complianceto 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 healthcareinformation can be shared. It specifies detailed requirements that are designed to protect patient privacy andsecurity.

All healthcare providers in the United States, from the smallest office to the largest hospitals, must complywith 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 knowslittle about computer networks and network security. He has hired your company as consultants to help himcomply with the HIPAA technical security requirements.

You have been asked to create a list of specific requirements that will meet the Technical Safeguards underthe 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 generaloverview is **site:compliancy-group.com hipaa security rule**. Answer the following questions.

Questions:

What are three examples of protected health information?

- Social Security Number
- Medical History
- Family Contact Information

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

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI).
2. Identify and safeguard against potential cyber threats.
3. Protect against unauthorized uses or disclosures.
4. Ensure that the workforce complies with security policies and procedures.

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

- Administrative
- Physical
- 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.

Technical Safeguards		
Section	**Standard**	**Implementation Specifications**
164.312(a)(1)	Access Control	Unique User Identification, Emergency Access Procedures, 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

Blank Line, No additional information

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 ElectronicProtected Health Information
164.312(d)	Person Or Entity Authentication	N/A
164.312(e)(1)	Transmission Security	● Integrity Controls ● Encryption

Blank Line, No additional information

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 findthat 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 ID for login and activity tracking.
164.312(a)(2)(ii)	Emergency Access Procedure	Use mirrored HDD storage, regular backups, and secure cloud storage for data retrieval.
164.312(a)(2)(iii)	Automatic Logoff	Implement policies to automatically log off users after a specified period of inactivity.
164.312(a)(2)(iv)	Encryption and Decryption	Encrypt server hard drives and use encryption software or self-encrypting drives.
164.312(b)	Audit Controls	Implement tracking of access and version control for changes.
164.312(c)(1)	**Integrity**	
164.312(c)(2)	Mechanism to Authenticate EPHI	Use file integrity monitoring (FIM) to verify the authenticity of data.
164.312(d)	Person or Entity Authentication	Implement multi-factor authentication (MFA), password reset questions, and biometric methods
164.312(e)(1)	**Transmission Security**	
164.312(e)(2)(i)	Integrity Controls	Use hashing for transmitted documents and ensure secure deletion of emails containing EPHI.
164.312(e)(2)(ii)	Encryption	Use WPA2 or better for wireless transmission, VPN for remote access, encrypted email, and HTTPS for secure communication.

Blank Line, No additional information

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-DSScontrol objectives**. Each objective has one or more requirements. From your searches, complete that tablebelow:

PCI-DSS Objectives	PCI-DSS Requirements
Build and maintain a secure network	Install and maintain a firewall, avoid using default passwords from vendors.
Protect cardholder data	Protect stored cardholder data, encrypt data during transmission.
Maintain a vulnerability management program	Use and regularly update anti-virus software, secure systems and applications.
Implement strong access control measures	Restrict access based on need-to-know, assign unique IDs, restrict physical access.
Regularly monitor and test networks	Track and monitor access to network resources and cardholder data, test security systems regularly.
Maintain an information security policy	Maintain a policy that addresses information security for all personnel.

Blank Line, No additional information

2. How do these compliance requirements compare to the HIPAA requirements that you supplied above?
   - They are quite similar as they both focus on key aspects of data security such as confidentiality, integrity, and controlled access. Both frameworks emphasize the importance of tracking, auditing, and testing systems to ensure they remain secure.

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 complianceof smaller organizations?
   - Smaller organizations often face challenges such as limited budgets for implementing and maintaining security systems, as well as difficulties in meeting audit and vulnerability assessment requirements. They may lack the internal resources needed to manage compliance effectively and may need to seek external assistance.

End of documen