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?

Answer
1. Name
2. Address
3. Birthday

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. 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?

Answer

1. Administrative
2. Physical
3. 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 Procedure - Automatic Logoff - Encryption and Decryption
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) - Encryption (A)

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 and password to each user
164.312(a)(2)(ii)	Emergency Access Procedure	Implement break-glass procedure for emergency access
164.312(a)(2)(iii)	Automatic Logoff	Configure automatic screen lock after period of inactivity

164.312(a)(2)(iv)	Encryption and Decryption	Use AES-256 encryption for stored EPHI
164.312(b)	Audit Controls	Implement system-wide logging and monitoring solution
164.312(c)(1)	**Integrity**	
164.312(c)(2)	Mechanism to Authenticate EPHI	Implement checksum verification for data integrity
164.312(d)	Person or Entity Authentication	Implement multi-factor authentication (MFA)
164.312(e)(1)	**Transmission Security**	
164.312(e)(2)(i)	Integrity Controls	Implement SSL/TLS for data in transit
164.312(e)(2)(ii)	Encryption	Use end-to-end encryption for email communication

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 - 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 or programs - 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?

Answer

Both PCI-DSS and HIPAA focus on protecting sensitive information, but they have different scopes. PCI-DSS is specifically for protecting cardholder data, while HIPAA protects electronic protected health information (EPHI). However, there are similarities in their approaches:

1. Both require strong access controls and unique user identification

2. Both emphasize the importance of encryption for data transmission
3. Both require regular monitoring and testing of security measures
4. Both stress the need for maintaining security policies and procedures

The main difference is that HIPAA has more specific requirements for healthcare-related processes, such as emergency access procedures, while PCI-DSS is more focused on financial transaction security.

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?

Answers

1. Limited resources (both financial and personnel) to implement and maintain complex security systems
2. Lack of dedicated IT security staff
3. Difficulty in keeping up with rapidly changing technology and threat landscapes
4. Balancing security measures with operational efficiency in a small-scale environment
5. Cost of regular security audits and assessments
6. Complexity of managing multiple compliance frameworks (e.g., both HIPAA and PCI-DSS for small medical practices that accept credit cards)
7. Limited bargaining power with vendors for security solutions tailored to their needs