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?

[Answer]

1. Name
2. Address
3. Birthday

Protected Health Information (PHI) encompasses any information that can identify an individual and relates to their health status, provision of healthcare, or payment for healthcare.

name, address, 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 health information (ePHI).

   This requires measures to keep ePHI secure, complete, and accessible only to authorized individuals.

2. Identify and protect against cyber threats.

   Implement policies and procedures to detect and defend against potential cyber threats.

3. Protect against impermissible uses or disclosures.

   Implement safeguards to ensure that ePHI is not improperly used or disclosed.

4. Ensure compliance of workforce.

   Train employees and ensure that they adhere to security measures that comply with HIPAA standards.

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 Safeguards: Policies and procedures designed to manage the selection, development, and implementation of security measures.
2. Physical Safeguards: Physical measures to protect electronic systems and data from unauthorized access.
3. Technical Safeguards: Technology-based measures to secure ePHI and control access.

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.

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 for login, as well as to track who has created, edited, or accessed ePHI.
164.312(a)(2)(ii)	Emergency access procedure	Implement mirrored HDD storage, data backups, and use of secure cloud-based data storage and retrieval for emergency situations.
164.312(a)(2)(iii)	Automatic logoff	Configure all systems to automatically log off after a period of inactivity. This should apply to both workstations and relevant applications.
164.312(a)(2)(iv)	Encryption and decryption	Encrypt sensitive data at rest and in transit. Implement software-based encryption or use auto-encrypting drives for servers and databases.
164.312(b)	Audit Controls	Implement AAA (Authentication, Authorization, and Accounting) logging to track access to ePHI. Use version tracking for documents to monitor changes.
164.312(c)(1)	**Integrity**	
164.312(c)(2)	Mechanism to authenticate ePHI	Implement File Integrity Monitoring (FIM) systems to ensure that unauthorized changes to ePHI are detected and flagged.

Standard	Name	Control
164.312(d)	Person or Entity Authentication	Implement multi-factor authentication (MFA) to secure access. Include password reset security questions and consider biometric authentication.
164.312(e)(1)	**Transmission Security**	
164.312(e)(2)(i)	Integrity controls	Implement hashing algorithms for secure communications. Secure deletion policies should be enforced for emails and documents containing ePHI.
164.312(e)(2)(ii)	Encryption	Use WPA2 or stronger encryption for wireless communication, VPNs for remote access, encrypted email for sending ePHI, and HTTPS for web-based access.

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. - 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 HIPAA and PCI-DSS requirements focus on fundamental security principles such as data encryption, access control, vulnerability management, and audit logging. They emphasize protecting sensitive data, whether it's cardholder information (PCI-DSS) or protected health information (HIPAA). The overlap includes the use of firewalls, encryption, multi-factor authentication, and audit trails. Overall, they share a common goal of safeguarding sensitive information but are tailored to different industries and data types.

   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?

   [Answer]

   Smaller organizations often face challenges such as limited resources, both in terms of budget and staff, which can make implementing comprehensive security measures difficult. They may lack the technical expertise required to assess and maintain compliance, and the costs of security audits, vulnerability assessments, and software tools needed for compliance can be prohibitive. Furthermore, staying up to date with evolving regulations and security threats while managing day-to-day business operations can overwhelm smaller teams. Lastly, proving compliance by compiling reports and preparing for audits is a significant burden, especially if the organization lacks a dedicated compliance officer.

   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.