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 Area

1. Patient Name
2. Medical Records
3. Address

Show Answer

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

Answer Area

and availability of all electronic protected health information (ePHI). Protect against threats to the security of the ePHI.

Show Answer

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

Answer Area

analysis)
Physical Safeguards (e.g., facility access controls, workstation security)
Technical Safeguards (e.g., access

Show Answer

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)	Answer Area: Access Control	Answer Area: - Unique User Identification, Emergency Access Procedure, Automatic Logoff, Encryption and Decryption
164.312(b)	Answer Area: Access Control	Answer Area: None

Technical Safeguards		
164.312(c)(1)	Answer Area Integrity	Answer Area - Mechanism to Authenticate ePHI
164.312(d)	Answer Area Person or Entity Authentication	Answer Area None
164.312(e)(1)	Answer Area Transmission Security	Answer Area - Integrity Controls, Encryption

Blank Line, No additional information

Click **Show Answer** to a sample answer table.

Show Answer

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 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)	Answer Area: Unique user identification	Answer Area: All users should have unique usernames not only for login but also to identify who has created, edited,
164.312(a)(2)(ii)	Answer Area: Emergency access procedure	Answer Area: Mirrored HDD storage of records, backups, use of secure cloud for data storage and retrieval.
164.312(a)(2)(iii)	Answer Area: Automatic logoff	Answer Area: All computers should be set with security policies to logoff after an idle period. Configure relevant
164.312(a)(2)(iv)	Answer Area: Encryption and decryption	Answer Area: Identify information to be encrypted, encrypt server HDD, either in software or with auto-encrypting drives.
164.312(b)	Answer Area: Audit Controls	Answer Area: Implement AAA accounting and document version tracking.
164.312(c)(1)	**Integrity**	
164.312(c)(2)	Answer Area: Mechanism to authenticate ePHI	Answer Area: Implement file integrity monitoring (FIM)
164.312(d)	Answer Area: Person or Entity Authentication	Answer Area: Multi-factor authentication (MFA), questions for password reset, biometric authentication
164.312(e)(1)	**Transmission Security**	
164.312(e)(2)(i)	Answer Area: Integrity controls	Answer Area: communications security hashing on transmitted documents, secure deletion of emails and other EPHI documents
164.312(e)(2)(ii)	Answer Area: Encryption	Answer Area: Secure transmission WPA2 or better wireless, VPN for remote access, encrypted email, HTTPS, removing EPHI

Blank Line, No additional information

Click **Show Answer** to a sample answer table.

Show Answer

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-DSS control objectives**. Each objective has one or more requirements. From your searches, complete that table below:

PCI-DSS Objectives	PCI-DSS Requirements
Answer Area Build and maintain a secure network.	Answer Area Install and maintain a firewall configuration to protect card holder
Answer Area Protect cardholder data.	Answer Area = Encrypt transmission of cardholder data across open, public networks.
Answer Area Maintain a vulnerability management program.	Answer Area = Develop and maintain secure systems and applications.
Answer Area Implement strong access control measures.	Answer Area = Restrict physical access to cardholder data.
Answer Area Regularly monitor and test networks.	Answer Area = Regularly test security systems and processes.
Answer Area Maintain an information security policy.	Answer Area Maintain a policy that addresses information security for all personnel.

Blank Line, No additional information

Click **Show Answer** to a sample answer table.

Show Answer

Blank Line, No additional information

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

Answer Area

Both frameworks require strict access controls, encryption, audit controls, and data integrity measures. They focus on protecting sensitive data (HIPAA focuses on health information, while PCI-DSS focuses on credit card data).
Both require regular monitoring and testing of security systems to ensure compliance.
The main difference is the type of data each framework covers (ePHI for HIPAA, cardholder data for PCI-DSS).

Show Answer

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 Area

Smaller organizations may struggle with the financial burden of implementing advanced security solutions (e.g., encryption, auditing tools).
Lack of in-house expertise: Small organizations might not have dedicated security staff to ensure compliance.
Regular assessments and documentation required to prove compliance can be challenging due to limited resources and personnel.

Show Answer

End of document

Show All Answers

Clear My Responses