Nama : Yusufa Haidar

Kelas : SIB-3C

Absen : 21

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?

1. Patient Name
2. Medical Records
3. Social Security Numbers

name, address, birthday

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

a. **Ensure confidentiality, integrity, and availability of ePHI**: Healthcare organizations must safeguard electronic Protected Health Information (ePHI) to ensure that it is not accessed or altered by unauthorized individuals and that it is available to authorized users when needed.

b. **Identify and protect against cyber threats**: Organizations must implement measures to identify and defend against potential cyber threats that could compromise ePHI, such as malware, hacking, or data breaches.

c. **Protect against impermissible uses or disclosures**: Organizations must prevent unauthorized access or sharing of ePHI, ensuring that data is only used or disclosed in compliance with HIPAA regulations.

d. **Ensure workforce compliance**: Healthcare organizations must train and monitor employees to ensure they follow security protocols, avoid breaches, and adhere to HIPAA requirements.

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?

a. **Administrative Safeguards**: Policies and procedures designed to manage the selection, development, and implementation of security measures. These include risk analysis, workforce training, and contingency planning to ensure protection of ePHI.

b. **Physical Safeguards**: Measures to protect the physical equipment and facilities where ePHI is stored. This includes controlling access to buildings, workstations, and devices, as well as implementing policies for device disposal and reuse.

c. **Technical Safeguards**: Technology and procedures used to secure ePHI and control access to it. Examples include encryption, secure access controls, audit controls, and authentication systems to prevent unauthorized access to electronic health information.

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	- **Required:** Unique User Identification - **Required:** Emergency Access Procedure - **Addressable:** Automatic Logoff - **Addressable:** Encryption and Decryption
164.312(b)	Audit Controls	None (requires recording and examining system activity)
164.312(c)(1)	Integrity	- **Addressable:** Mechanism to Authenticate Electronic Protected Health Information
164.312(d)	Person Or Entity Authentication	None (requires verifying the identity of those accessing ePHI)
164.312(e)(1)	Transmission Security	- **Addressable:** Integrity Controls - **Addressable:** 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	Assign each user a unique identifier to ensure tracking of user access and activity related to ePHI.
164.312(a)(2)(ii)	Emergency Access Procedure	Establish procedures for obtaining access to ePHI in emergency situations, such as during a system failure.
164.312(a)(2)(iii)	Automatic Logoff	Implement automatic logoff or equivalent measures to prevent unauthorized access after periods of inactivity. This helps protect unattended systems from misuse.
164.312(a)(2)(iv)	Encryption and Decryption	Use encryption to protect ePHI both at rest and in transit, based on the entity's risk assessment. Encryption ensures data confidentiality.
164.312(b)	Audit Controls	Implement hardware, software, and procedural mechanisms to record and examine system activity related to ePHI. Audit logs should track access and changes to sensitive data.
164.312(c)(1)	**Integrity**	
164.312(c)(2)	Mechanism to Authenticate ePHI	Implement a system that verifies that ePHI has not been altered or tampered with. For example, use of hash functions can help ensure data integrity.
164.312(d)	Person or Entity Authentication	Ensure that users or entities seeking access to ePHI are properly identified before access is granted. This may involve the use of passwords, tokens, or biometrics.
164.312(e)(1)	**Transmission Security**	
164.312(e)(2)(i)	Integrity Controls	Implement measures to ensure that ePHI is not improperly modified during transmission. Examples include encryption and secure hashing algorithms.
164.312(e)(2)(ii)	Encryption	Encryption should be applied to ePHI when transmitted, ensuring confidentiality and protection against interception.

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.

Standard	Name	Control
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
1. Build and maintain a secure network	a. Install and maintain a firewall configuration to protect cardholder data. b. Do not use vendor-supplied defaults for system passwords and other security parameters.
2. Protect cardholder data	a. Protect stored cardholder data using encryption, truncation, or masking techniques. b. Encrypt transmission of cardholder data across open, public networks.

PCI-DSS Objectives	PCI-DSS Requirements
3. Maintain a vulnerability management program	a. Use and regularly update anti-virus software or programs to protect against malware. b. Develop and maintain secure systems and applications by applying security patches in a timely manner.
4. Implement strong access control measures	a. Restrict access to cardholder data by need-to-know. b. Assign a unique ID to each person with computer access to ensure accountability. c. Restrict physical access to cardholder data, including using access controls and monitoring systems.
5. Regularly monitor and test networks	a. Track and monitor all access to network resources and cardholder data by reviewing logs and using automated systems. b. Regularly test security systems and processes, including vulnerability scans and penetration tests.
6. Maintain an information security policy	a. Maintain a policy that addresses information security for all personnel, ensuring regular updates and employee training on security practices.

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.

PCI-DSS Objectives	PCI-DSS Requirements
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 **HIPAA** and **PCI-DSS** share common security objectives, such as protecting sensitive data, ensuring access controls, and regularly monitoring system activity. The primary difference lies in their scope—HIPAA focuses on healthcare data, while PCI-DSS is centered on payment card information.

   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 face a distinct challenge in balancing security and regulatory compliance with limited resources and expertise. To address these, smaller entities often turn to managed service providers, consultants, or specialized compliance software to help ensure adherence to both HIPAA and PCI-DSS while still focusing on their primary operations.

   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.