Moh. Samsul Hadi | SIB4C | 06 | KSI

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?

Medical records: This includes any information about an individual's health history, diagnoses, treatments, and medications.

Billing information: This includes any information related to the cost of medical services, such as insurance claims, patient statements, and payment history.

Health insurance information: This includes any information about an individual's health insurance coverage, such as **policy numbers, group numbers, and eligibility status.**

name, address, birthday

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

Protect against unauthorized access, use, disclosure, or modification of PHI. This includes implementing access controls, encryption, and physical security measures.

Ensure the integrity of PHI. This means protecting PHI from being altered or destroyed, and ensuring that it is accurate and complete.

Safeguard the confidentiality of PHI. This means protecting PHI from being disclosed to unauthorized individuals.

Protect against threats to the security of PHI. This includes implementing measures to prevent and detect security breaches..

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

Administrative safeguards: These are policies and procedures that help to ensure that PHI is protected. Examples of administrative safeguards include:

- Risk assessments
- Security awareness training
- Incident response plans
- Access controls

Technical safeguards: These are technological measures that help to protect PHI. Examples of technical safeguards include:

- Encryption
- Firewalls
- Intrusion detection systems
- Antivirus software

Physical safeguards: These are physical measures that help to protect PHI. Examples of physical safeguards include:

- Security cameras
- Access controls
- Locks
- Alarms

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.

The text provides an overview of the Security Series, a series of papers published by CMS to guide healthcare organizations in implementing the HIPAA Security Rule. The fourth paper in the series focuses on the Technical Safeguards standards and their implementation specifications.

The text explains the background of the Security Rule and the importance of technical safeguards in protecting electronic protected health information (EPHI). It also outlines the objectives of the paper, which include reviewing the standards and implementation specifications, discussing their purpose, and providing sample questions for covered entities to consider.

The text emphasizes that the sample questions are for consideration only and are not required for implementation. The purpose of the questions is to promote review of a covered entity's environment in relation to the requirements of the Security Rule.

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 identifiers* * Emergency access procedures* * Automatic logoff* * Encryption*
164.312(b)	Audit Controls	* Audit trail* * Review of audit logs*
164.312(c)(1)	Integrity Controls	* Data validation* * Data backup and recovery*
164.312(d)	Person Authentication	* Multiple authentication factors*

Technical Safeguards		
164.312(e)(1)	Work Station Controls	* Physical safeguards* * Screen savers* * Automatic logoff*

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 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

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 Identifiers	Active directory, employee database
164.312(a)(2)(ii)	Emergency Access Procedures	Alternate authentication methods, emergency contact list
164.312(a)(2)(iii)	Automatic Logoff	Session timeout settings, inactivity monitoring
164.312(a)(2)(iv)	Encryption	Data encryption at rest and in transit
164.312(b)	Audit Controls	Security information and event management (SIEM) solution, audit log analysis

Standard	Name	Control
164.312(c)(1)	**Integrity**	
164.312(c)(2)	Data Backup and Recovery	Regular backups, disaster recovery plan
164.312(d)	Person Authentication	Multi-factor authentication (MFA), biometric authentication
164.312(e)(1)	**Transmission Security**	
164.312(e)(2)(i)	Workstation Controls	Physical security measures, screen savers, automatic logoff
164.312(e)(2)(ii)	Security Procedures	Secure network configurations, vulnerability scanning

Blank Line, No additional information

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.
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**	

Standard	Name	Control
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.

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
Build and Maintain a Secure Network	1. Install and maintain a firewall configured to protect cardholder data. 2. Do not use vendor-supplied default passwords for system components. 3. Protect cardholder data on all systems within the cardholder data environment (CDE).
Protect Cardholder Data	4. Encrypt cardholder data transmitted across open public networks. 5. Protect cardholder data stored on any system by encrypting it. 6. Develop a process to protect cardholder data during transit.
Maintain a Program to Protect Cardholder Data	7. Develop, implement, and maintain a secure coding standard. 8. Assign unique IDs to each person with authorized access to the CDE. 9. Restrict access to cardholder data to authorized personnel.
Implement Strong Access Controls	10. Use strong passwords that are changed regularly. 11. Monitor access to cardholder data and review access logs regularly. 12. Assign unique IDs to each person with authorized access to the CDE.
Monitor and Test Networks	13. Perform internal and external vulnerability scans. 14. Implement a process to regularly test security systems and procedures.
Maintain a Secure Software Development Lifecycle	15. Develop and maintain a secure software development lifecycle (SDLC). 16. Accept only secure software components into the CDE.

Blank Line, No additional information

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.
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.

Blank Line, No additional information

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

Similarities:

- Data Protection: Both frameworks prioritize the protection of sensitive data, including personal information and payment card data.
- Access Controls: Both require strong access controls to prevent unauthorized access to sensitive data.
- Network Security: Both emphasize the importance of network security measures, such as firewalls and vulnerability scanning.
- Incident Response: Both require organizations to have a plan in place to respond to security incidents.

Differences:

- Scope: PCI-DSS is specifically focused on protecting cardholder data, while HIPAA applies to all protected health information (PHI).
- Requirements: While there are some overlaps, the specific requirements of PCI-DSS and HIPAA differ in certain areas. For example, HIPAA places a greater emphasis on the protection of patient privacy, while PCI-DSS focuses more on preventing fraud and data breaches.

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?

Major Challenges for Compliance of Smaller Organizations:

1. **Limited Resources:** Smaller organizations often have limited budgets and staff, making it difficult to allocate resources to compliance efforts.
2. **Lack of Expertise:** Smaller organizations may not have the in-house expertise to understand and implement compliance requirements.
3. **Complexity of Regulations:** Compliance frameworks like HIPAA and PCI-DSS can be complex and difficult to understand, especially for smaller organizations with limited resources.
4. **Cost of Compliance:** Implementing compliance measures can be expensive, especially for smaller organizations with limited budgets.
5. **Changing Regulations:** Compliance frameworks are constantly evolving, making it difficult for smaller organizations to stay up-to-date.
6. **Vendor Management:** Smaller organizations may rely on third-party vendors to process payments or store data, which can introduce additional compliance challenges.

To address these challenges, smaller organizations can:

- **Prioritize Compliance:** Make compliance a top priority and allocate resources accordingly.
- **Seek External Assistance:** Consider hiring a compliance consultant or outsourcing compliance functions to a third-party provider.
- **Leverage Technology:** Use technology to automate compliance tasks and reduce costs.
- **Stay Informed:** Stay up-to-date on the latest compliance requirements and industry best practices.
- **Build a Culture of Compliance:** Foster a culture of compliance within the organization, encouraging employees to take ownership of compliance responsibilities.

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.