IK-RARS'JATI PRAMESTI
2141762003
SIB-4C

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?

name, address, birthday

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

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?

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

Blank Line, No additional information

IK-RARS'JATI PRAMESTI
2141762003
SIB-4C

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 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.

Standard	Name	Control
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.

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.	• 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.

PCI-DSS Objectives	PCI-DSS Requirements
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?

Fokus Perlindungan

1. **PCI-DSS:**
   - **Dirancang khusus untuk melindungi data pemegang kartu kredit dari akses tidak sah dan penipuan. Ini mencakup transaksi pembayaran elektronik dan pengelolaan data sensitif terkait kartu pembayaran.**
   - **Contoh data yang dilindungi: nomor kartu kredit, data otentikasi, dan informasi kartu lainnya (UpGuard)(PCI Security Standards Council).**
2. **HIPAA Security Rule:**
   - **Fokus pada perlindungan Protected Health Information (PHI) yang berkaitan dengan kesehatan pasien, baik secara elektronik maupun fisik. HIPAA dirancang untuk industri kesehatan.**
   - **Contoh PHI yang dilindungi: nama pasien, nomor jaminan sosial, dan catatan medis(Compliancy Group)(Compliancy Group).**

Tujuan Kontrol Utama

- **PCI-DSS memiliki enam tujuan kontrol utama:**
  1. **Membangun dan memelihara jaringan yang aman.**
  2. **Melindungi data pemegang kartu.**
  3. **Memelihara program manajemen kerentanan.**
  4. **Menerapkan kontrol akses yang kuat.**
  5. **Memantau dan menguji jaringan secara rutin.**
  6. **Memelihara kebijakan keamanan informasi(PCI Security Standards Council).**
- **HIPAA Security Rule berfokus pada tiga perlindungan utama:**
  1. **Administrative Safeguards: Mengelola risiko dan akses untuk memastikan keamanan PHI.**
  2. **Physical Safeguards: Melindungi akses fisik ke perangkat dan lokasi yang menyimpan PHI.**
  3. **Technical Safeguards: Menggunakan teknologi untuk mengontrol akses dan memastikan integritas serta kerahasiaan data elektronik(Compliancy Group)(Compliancy Group).**

Perbandingan Konkretnya:

1. **Perlindungan Data dalam Transit dan Saat Disimpan:**
   - **PCI-DSS dan HIPAA sama-sama menuntut perlindungan data yang dienkripsi saat dikirimkan dan saat disimpan. Namun, PCI-DSS lebih ketat dalam hal perlindungan data kartu kredit dan metode otentikasi.**
2. **Manajemen Akses:**
   - **Kedua kerangka kerja menuntut pembatasan akses berdasarkan "need-to-know" basis, menggunakan ID unik untuk melacak pengguna yang memiliki akses ke sistem. Namun, HIPAA juga menekankan pembatasan akses untuk menjaga privasi pasien, sementara PCI-DSS lebih menekankan aspek keamanan keuangan.**
3. **Pemantauan dan Pengujian Sistem:**
   - **PCI-DSS secara eksplisit meminta pengujian dan pemantauan rutin terhadap sistem keamanan dan transaksi pembayaran. HIPAA juga mewajibkan audit dan pemantauan sistem, tetapi fokusnya pada PHI dan memastikan sistem kesehatan tetap aman dan patuh.**

Perbedaan Cakupan dan Industri

- **PCI-DSS hanya berlaku untuk bisnis yang menangani kartu pembayaran, sehingga lebih sempit dibandingkan HIPAA, yang mencakup berbagai aspek industri kesehatan(UpGuard)(PCI Security Standards Council).**
- **HIPAA memiliki lingkup yang lebih luas dalam melindungi data pasien di seluruh organisasi kesehatan, termasuk klinik, rumah sakit, dan penyedia layanan kesehatan lainnya.**

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?

   Ada banyak. Salah satu yang besar adalah penilaian kepatuhan. Organisasi tidak hanya harus menerapkan langkah-langkah yang diperlukan, tetapi juga harus membuktikan bahwa mereka mematuhi dengan lulus audit keamanan, menjalani penilaian kerentanan, dan menyusun laporan untuk mendukung kepatuhan.