Security Assessment and Management on Small Health Care Clinic

We perform a security assessment and management on Cedarville Family Clinic.

Story of Cedarville Family Health Risk

Cedarville Family Health has provided healthcare services to the small town of Cedarville Family Health, Rhode Island, for over 40 years. The clinic was founded by Dr. Thomas Smith, a dedicated medical professional committed to providing quality care to the community. Mabel Johnson joined him in his mission. She was a long-time nurse who was detail-oriented and dedicated to ensuring excellent care for each patient.

Ten years ago, Dr. Smith hired his daughter, Sandra, to be the office manager. Over the years, she has transitioned some of their files to an electronic format.

Next

Despite its long-standing reputation in the community, the clinic has struggled to keep up with modern information security standards and requirements. Garrett Shaw, a family friend and the clinic's attorney, has recommended that the clinic review its data security posture. The review has two goals:

- Evaluate and improve the clinic's current data security practices.
- Determine changes needed to comply with the information security requirements outlined in HIPAA.

Next

In this case there decide hire a Cyber Security expert to build there polices with HIPAA company and rebuild there's infrastructure of office with security measures.

Here we have information, you'll the following documentation to help you assess Cedarville

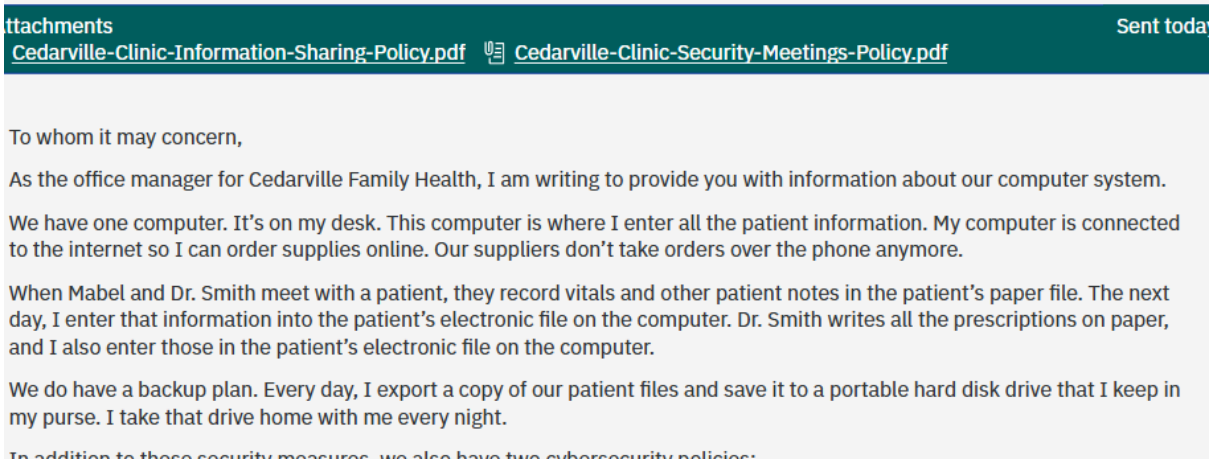
Family Health's risk:

- An email from the office manager
- The clinic's information sharing policy
- The clinic's security meetings and training sessions policy
- A summary of the Security Rule of the Health Insurance Portability and

  Accountability Act (HIPAA)

Email from office manager

In the following email, Sandra describes the clinic's existing cybersecurity infrastructure.


ttachments Sent toda

Cedarville-Clinic-Information-Sharing-Policy.pdf Cedarville-Clinic-Security-Meetings-Policy.pdf

To whom it may concern,

As the office manager for Cedarville Family Health, I am writing to provide you with information about our computer system.

We have one computer. It's on my desk. This computer is where I enter all the patient information. My computer is connected to the internet so I can order supplies online. Our suppliers don't take orders over the phone anymore.

When Mabel and Dr. Smith meet with a patient, they record vitals and other patient notes in the patient's paper file. The next day, I enter that information into the patient's electronic file on the computer. Dr. Smith writes all the prescriptions on paper, and I also enter those in the patient's electronic file on the computer.

We do have a backup plan. Every day, I export a copy of our patient files and save it to a portable hard disk drive that I keep in my purse. I take that drive home with me every night.

In addition to these security measures, we also have two cybersecurity policies:

Summary:

The officer write's about there infrastructure, information sharing policy and security meeting policy.

After go through this email, officer said that they only one computer in clinic and, In night she

Uploads all data of patients into hard disk. Then takes with her to home. Computer is using internal

Network. It there back up plan.

Information Sharing policy it means sharing information of patients or customer. For this they are used this policy.

Security Meeting policy it means meeting about, necessary of meeting and requirements of meeting. For this they are used this policy.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Security Rule establishes requirements for protecting private health information (PHI) that covered entities must follow. The US Department of Health and Human Services (HHS) provides the following definition for **covered entities:**

"Health plans, health care clearinghouses, and … any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates".

– Summary of the HIPAA Security Rule. *US Department of Health and Human Services,* October 19, 2022.

Area's we focusing:

I. **Compliance with the Security Rule of HIPAA**
II. **Governance and oversight**
III. **Risk management**
IV. **Other compliance areas**
V. **Risk assessment**
VI. **Data backup plan**
VII. **Encryption strategy**

I.Compliance with the Security Rule of HIPAA:

We have some rules in HIPAA, where every health care provider want follows:

1.Maintain reasonable and appropriate administrative, technical, and physical controls for protecting e-PHI.

Not compliant

Analysis:

Cedarville Family Health lacks the comprehensive security measures needed to protect e-PHI adequately. Current practices, such as staff taking non-encrypted portable hard disk drives offsite, don't meet the requirements of HIPAA for reasonable and appropriate safeguards.

2. Ensure the confidentiality, integrity, and availability of all e-PHI that covered entities create, receive, maintain or transmit.

Not compliant

Analysis:

Using unencrypted portable hard disk drives for data backups means that Cedarville Family Health does not adequately protect the confidentiality and integrity of e-PHI.

Also, taking these backups offsite without proper security measures compromises the availability of e-PHI.

3.Identify and protect against reasonably anticipated threats to the security or integrity of the information.

Not compliant

Analysis:

Cedarville Family Health lacks a formal risk assessment process, which is essential for identifying and mitigating potential threats to e-PHI. Without this process, the organization cannot effectively protect against data breaches, data loss, or unauthorized access.

4. Protect against reasonably anticipated, impermissible uses or disclosures.

Compliant

Analysis:

Cedarville Family Health has implemented effective measures to protect against impermissible uses Or disclosures. The clinic employs physical and electronic measures to safeguard patient data, with access to sensitive information strictly limited to authorized personnel based on their roles.

5. Ensure compliance by the covered entity's workforce.

Compliant

Analysis:

Cedarville Family Health has established comprehensive training programs and strict policy Enforcement mechanisms that effectively educate and regulate staff behaviour regarding e-PHI security. These programs include annual security and policy update meetings with mandatory attendance and rigorous record-keeping to ensure compliance.

II.Governance and oversight:

1.Security official - The organization has a designated individual explicitly responsible for overseeing cybersecurity policies and procedures.

Not compliant

Analysis:

Cedarville Family Health has not established, Any cyber security policies and procedures for cyber security experts.

.

2.Organizational policies - Comprehensive policies cover all aspects of cybersecurity, including prevention, detection, and response, which are needed to enforce security practices consistently and effectively across the organization.

Not compliant

Analysis:

Cedarville Family Health has not established, It means they didn’t have any prevention, detection and response plans.

3.Training programs - Well-implemented training programs ensure that all employees are regularly

informed on data protection best practices and the specific requirements of the organization's policies.

Compliant

Analysis:

Cedarville Family Health has established training program for all employees about real threats.

4.Data sharing policies - Effective policies regarding data sharing are in place and comply with legal standards, ensuring patient information is disclosed only to

Compliant

Analysis:

Cedarville Family Health has established the data sharing policy. It means inform the patients or customer about the data sharing policy.

IV.Risk management:

1.Risk analysis and management – the organization conducts regular risk analysis

as part of its security management process.

Not Compliant

Analysis:

Cedarville Family Health has not established, it means not conducting any regular risk analysis.

2.Regular risk assessments - The organization conducts regular and comprehensives

risk assessments to identify and mitigate vulnerabilities.

Not Compliant

Analysis:

Cedarville Family Health has not established, it means not conducting risk assessments and risk mitigation.

3.Risk communication - The organization effectively communicates risks and ongoing security measures to all relevant stakeholders.

Not Compliant

Analysis:

Cedarville Family Health has established, it means they regular conducting meetings on security frameworks and security awareness.

V.Other compliance areas:

1.Evaluation of security measures - The organization routinely evaluates the effectiveness of existing security measures to maintain an adaptive and effective security posture.

Not Compliant

Analysis:

Cedarville Family Health has not established, it means they not mixing routinely of security measures and not effecting security postures.

2.Incident response plan. The organization has a clearly defined and tested incident response plan that is regularly reviewed and updated.

Not Compliant

Analysis:

Cedarville Family Health has not established, it means they not planned incident response plan and not regularly reviewed.

3.Technical safeguards. The organization implements technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Not Compliant

Analysis:

Cedarville Family Health has not established, it means they not fix access control and Role based Access control.

4.Physical safeguards. The organization limits physical access to its facilities while ensuring that only authorized personnel can access sensitive areas.

Not Compliant

Analysis:

Cedarville Family Health has not established, it means they didn't fix access controls on physical devices. They not prepared firewall for network security.

VI.Risk assessment:

It process of identify risks and evaluate their impact and then decide what to do about them.

1.Risk Identification:

They are two risks the health care clinic is facing.

External risk: It means this risk comes for outsides on organization.

They are: Phishing emails, Ransomware attacks and internal network hacking.

Internal risk: It means this risk comes for insider of organization.

They are: unauthorized access to PHI data, Data backup hacking

2.Risk Impact:

Now think about how much the risk can make noise or consequences.

Phishing email – It can access patient data and trust of organization.

Ransomware – It can be encrypted patient data they ask for ransom money.

Unauthorized access – It can access PHI data and sensitive information of organization.

3.Risk Tolerance:

It means how much effects that risk and find solution of risk by based on risk impact.

Very high – Ransomware

High – Unauthorized access

Medium – Phishing

4.Risk Mitigation: It means decide how to respond to them. Risk response involves planning and developing ways to reduce risks.

Ransomware attack – Data backup on site.

Unauthorized access – IDS/IPS and RBAC roles based on employees roles (or) strong passwords (or) MFA

Phishing – Awareness to employees and customer about new threats regularly.

VII. Data backup plan:

In this we implement the 3-2-1 strategy. It means all preforms three back up copies. In this three two different back up storages and one it off site back up.

For this health care clinic we are storing on two different back up like USB flash drives and DVDs.

The one on hard drives.

Some key points:

- All perform full back up disk is encrypted.
- The need to maximize data protection and accessibility.

VIII.Encryption strategy:

In this we used all data must be encrypted. For health care clinic we need follows on security measures based on sensitive.

Some key points:

- All performed network encryption is used by public key encryption process (Symmetric key).
- All performs full back up encryption.
- Email encryption by using Asymmetric Encryption process.
- On site encryption always used file encryption of patient data and records.