Cybersecurity Practices

The Department of Health and Human Services (HHS) recommends ten cybersecurity practices that organizations working in healthcare should implement to secure protected health information (PHI)

Cybersecurity Practices

Why cybersecurity is important for healthcare

The healthcare industry has experienced several high profile breaches as of late, making it the most targeted industry for ransomware attacks. The healthcare industry holds a wealth of information on its' patients, making healthcare information ten times more valuable on the darkweb than financial information.

The Health Insurance Portability and Accountability Act (HIPAA) requires organizations working in healthcare to implement safeguards to secure PHI. Compliancy Group is committed to cybersecurity; as such this eBook will examine the ten cybersecurity practices recommended by the HHS.

Compliancy Group

We simplify Compliance so you can confidently focus on your business.

Email Protection Systems

What are email protection systems?

The HIPAA Security Rule requires organizations working in healthcare to use secure communications to transmit protected health information (PHI). PHI is any individually identifiable health information categorized by the Department of Health and Human Services (HHS) into 18 HIPAA identifiers.

Depending on how email is being used, the rules differ. When sending an email internally, using an organization's internal network, it is not necessary to use encryption. However, when sending external emails, which pass through a third-party server, encryption is recommend.

Encryption is the most effective way to secure PHI as it scrambles data, making it unreadable without a decryption key. While the HHS does not explicitly mandated encryption, they require organizations to assess their need for encryption. If the organization determines that encryption is not warranted, they must document why they decided not to encrypt, and what comparable protection is in place.

How to Implement Email Protection

- **Encryption** ensures that unauthorized users cannot read emails and attachments. Many professional email providers offer encryption.
- **Secure Passwords** should be implemented along with NIST standards, using mixed characters.
- **Multi-factor Authentication (MFA)** utilizes a password in combination with another authentication method such as biometrics or a one-time PIN.
- **Disable Automatic Downloads** of images. Images are often used to spread malware with a hidden link.
- **Virtual Private Network (VPN)** is an additional level of encryption that increases secure email transmission.

Endpoint Protection Systems

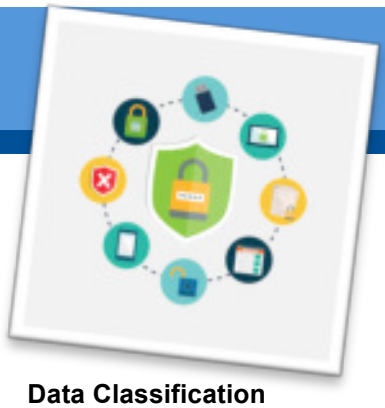
What are endpoint protection systems?

A device that connects to an organization's internal network such as a smartphone, laptop, tablet, or server in a data center, is referred to as an endpoint. Endpoint protection is the process of securing all of the endpoints connected to a business network.

Endpoint protection is often confused with anti-virus. However, anti-virus is meant to secure a device while endpoint protection secures an entire network. Endpoint security software, installed on an organization's network servers, eliminates the need to install security software on individual devices.

When choosing endpoint protection software, application control and endpoint encryption are essential features to look for. Application control blocks employees' ability to download applications, preventing them from downloading malicious content that could give network access to unauthorized individuals. Endpoint encryption hides sensitive data, also preventing unauthorized access.

How to Implement Endpoint Protection



- **Data Loss Prevention** detects and monitors PHI ensuring that unauthorized users do not access it.
- **Disk, Endpoint, and Email Encryption** makes data illegible preventing data corruption or theft.
- **Network Access Controls** prevents devices without permission from connecting to a network.
- **Endpoint Detection and Response** monitors and responds to security threats.
- **Insider Threat Protection** reduces the risk of insider breaches by monitoring employee access to PHI.
- **Applications Whitelisting or Control** determines what applications are safe to use.
- **Data Classification** categorizes data for ease of access.
- **Privileged User Control** limits access to certain features.

Access Management

What is access management?

The HIPAA Privacy Rule mandates that organizations working in healthcare limit access of PHI to the "minimum necessary." This means that individuals should only access the PHI that they need to perform their job function. For example, a nurse does not need access to a patient's billing information. Access management allows organizations to delegate different levels of access according to job roles.

The best way to accomplish access management is through multi-factor authentication (MFA). MFA requires a password in combination with another security factor to access data such as a onetime PIN code, biometric scan, or physical location.

Additionally, the HHS requires users to have easy access to PHI. Authentication systems such as a single sign-on system (SSO) allows for this. SSO provides employees with one set of login credentials to access various applications, while maintaining the advanced security of MFA.

How to Implement Access Management

- **Provide Users** with unique login credentials.
- **Restrict Employees** from sharing their login information with others.
- **Track Employee** access to protected health information.
- **Restrict Access** to data based on employee's job functions.
- **Review Access** to data when an employee changes job roles within an organization.
- **Enforce** the use of secure passwords and MFA.
- **Monitor Logon and Logoff Activity** to establish normal behavior patterns for each employee. This allows organizations to quickly detect insider breaches.

Data Protection and Loss Prevention

What is data protection and loss prevention?

Data loss prevention (DLP) software is an essential component to safeguarding PHI. When DLP is implemented, it ensures that sensitive data is not misused or lost. This is done through the categorization of data, determining which data is confidential or critical to business operations. Data categorization can be accomplished through a predefined HIPAA policy pack.

Categorization enables DLP to detect data access violations and provide remediation alerts. Additionally, DLP software encrypts PHI to prevent unauthorized access or accidental sharing. DLP is a powerful tool as it monitors and controls endpoint activities, filters out harmful data, and monitors data in the cloud.

DLP software also facilitates the development of incident response plans as it identifies weaknesses in an organization's data security practices. In the event of a breach, DLP enables organizations to quickly recover data, reducing downtime. DLP also provides documentation that proves an organization's "good faith effort" in the event of a HIPAA audit.

How to Implement Data Loss Prevention

- **Safeguards PHI** by identifying, classifying, and tagging sensitive information. This enables PHI access to be monitored to ensure that it is not accessed excessively by individual users or by unauthorized individuals.
- **Data Visibility** is accomplished by allowing organizations to track data on networks, the cloud, and endpoints. DLP software allows organizations to track how data is used, who uses it, and how much time they spend accessing data.
- **IP Protection** is enabled as DLP software identifies intellectual property and trade secrets to protect the data from exfiltration.

Asset Management

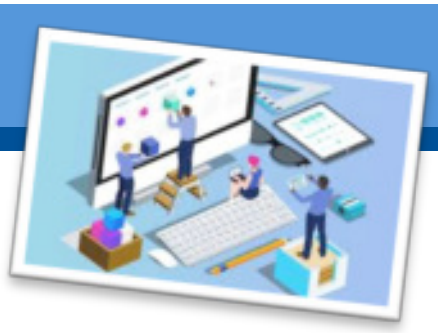
What is asset management?

Asset management is a means to track and maintain devices that access or store protected health information. The HIPAA Security Rule requires organizations to “maintain a record of the movements of hardware and electronic media and any person responsible therefore.”

Asset management takes an inventory of an organization’s devices that access PHI, who uses the device, and what security measures are in place on the device to protect PHI. The HIPAA Security Rule also requires organizations to identify where PHI is maintained, stored, received, or transmitted, which is addressed by asset management.

Organizations subject to a HIPAA audit will be prompted by the Office for Civil Rights (OCR) to provide documentation on “management as to how the location and movement of media and hardware containing ePHI is tracked, and obtain and review policies and procedures and evaluate the content relative to the specified criteria regarding tracking the location of ePHI media and hardware.”

How to Implement Asset Management



- **Asset Inventory List** should include all of the devices that access PHI. It should be updated whenever there is a new device or employee added to the organization.
- **What Information Should be Included** the device name, employee(s) name(s) that access the device, device age, what operating system the device uses, and what security measures are in place securing the device.
- **Outdated Operating Systems** put patient data at risk, as they are no longer supported with security patches. Devices must be updated and replaced to secure PHI.

Network Management

What is network management?

Network management refers to the process of securing and maintaining an organization's internal network. As part of the HIPAA Security Rule, organizations working in healthcare must implement administrative, physical, and technical safeguards to secure PHI.

Network management allows organizations to implement administrative safeguards in the form of user authentication and audit controls. Physical safeguards that are addressed by network management include physical site security and storage site security. Lastly, network management addresses technical safeguards with data encryption and data backup and recovery.

Network security is one of the most effective ways to prevent healthcare breaches. Hackers that gain access to an organization's internal network can spread malware throughout an organization's entire systems, infecting any device that connects to the network. As such, failure to implement effective network management can be detrimental to a business.

How to Implement Network Management

- **Authentication** provides users with unique login credentials for network access. Utilizing MFA to authenticate users ensure that unauthorized users do not have access.
- **Audit Controls** monitors user access on a network and alerts administrators to suspicious activity.
- **Physical Site Security** prevents device tampering. Installing cameras, alarm systems, and keypad locks that give each user a unique code can be utilized.
- **Network Security Management** allows administrators to manage firewalls to prevent unauthorized access.
- **Encryption** encodes data to prevent unauthorized access.
- **Data Backup and Recovery** HIPAA requires exact copies of PHI to be backed up. A disaster recovery plan also ensures that data is not lost in an emergency.

Vulnerability Management

What is vulnerability management?

Vulnerability management identifies possible risks in an organization's network security. Once risks are identified remediation plans are developed to address security gaps. Vulnerability management consists of checking for, identifying, verifying, mitigating, and patching vulnerabilities.

The purpose of vulnerability management is to address security gaps before they result in a breach. As such, the Office for Civil Rights (OCR) recommends that organizations working in healthcare implement a patch management program:

- Evaluate patches to determine if they apply to your software/systems
- Test patches on an isolated system to discover if there are any unforeseen or unwanted side effects
- Approve patches for deployment once they have been evaluated and tested
- Schedule patches to be installed on live or production systems once approved
- Test and audit systems to ensure that the software patches were applied correctly

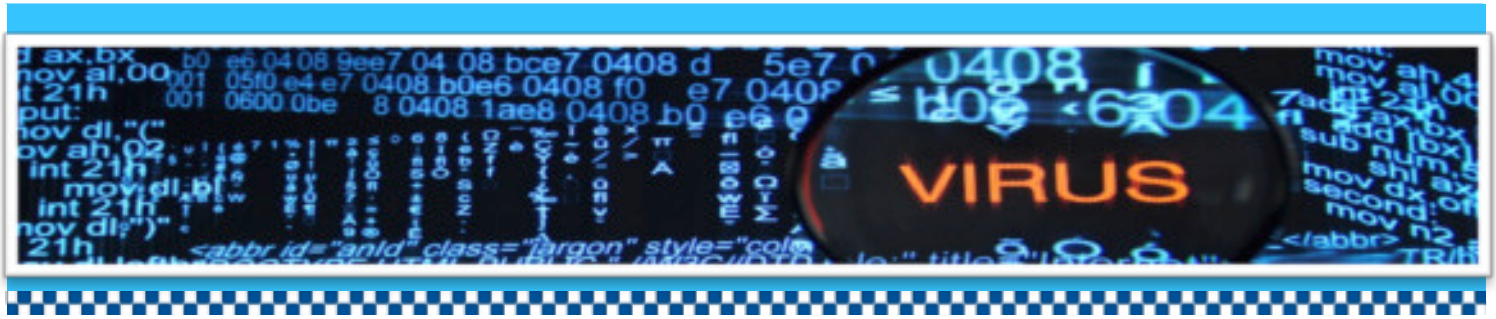
How to Implement Vulnerability Management

Checking for Vulnerabilities

- **Network Scanning** identifies active devices on a network to determine device "health."
- **Firewall Logging** is a log showing all devices active on a network, including devices that were denied access.
- **Penetration Testing** determines where security is lacking through ethical hacking.

- **Identifying Vulnerabilities** assesses the results to determine how hackers can exploit gaps.
- **Verifying Vulnerabilities** determines if gaps can be reasonably exploited.
- **Mitigating Vulnerabilities** addresses gaps with patches or by restricting or disabling network access.

- **Patching Vulnerabilities** fixes security gaps through software or hardware updates provided by the vendor. OCR states, "In situations where patches are not available or testing or other concerns weigh against patching as a mitigation solution, entities should implement reasonable compensating controls to reduce the risk of identified vulnerabilities to a reasonable and appropriate level."



Incident Response

What is incident response?

HIPAA defines a security incident as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” When an organization working in healthcare experiences a data breach it must be reported to the Department of Health and Human Services’ (HHS) Office for Civil Rights (OCR). Depending on the size of the breach, reporting requirements differ.

- *Meaningful Breach:* affects more than 500 individuals and must be reported within 60 days of discovery. A meaningful breach must be reported to the OCR, affected individuals, and the media.

- *Minor Breach:* affects less than 500 individuals and must be reported by the end of the calendar year. A minor breach must be reported to the OCR and affected individuals.

Organizations that experience a breach must develop corrective action plans to address gaps in security that allowed the breach to occur. Organizations that have an incident response plan are able to detect and respond to breaches quickly, limiting the scope of the breach and the need for corrective action.

How to Implement Incident Response

What an Incident Response Plan Does:

- Detects and incident
- Contains an incident
- Corrects the situation
- Recovers lost data

What Should be Included:

- What to do when an incident is suspected
- Who is responsible for evaluating the situation to determine if it is actionable
- How to quickly limit the damage
- How to find the source of the incident and how to address it
- How to recover from the incident
- Who ensures changes are made to prevent future incidents

Medical Device Security

What is medical device security?

Medical devices are increasingly connecting to healthcare networks. When developing cybersecurity policies, medical device security is often overlooked. Since many medical devices are operating on outdated operating systems, they can pose a huge risk to an organization's security.

However, medical device security is not up to the healthcare organization. Manufacturers must be aware of areas in which medical devices may be vulnerable. The Food and Drug Administration (FDA) requires medical device manufacturers to submit a "Cybersecurity Bill of Materials" during premarket reviews. This identifies security vulnerabilities in the software and hardware of devices.

For older medical devices, there may be patches available to update operating systems. Healthcare organizations should contact device manufacturers to inquire about updates for older devices.

How to Implement Medical Device Security

Access Controls

Access to medical devices should be granted to only those that need access. Users should have unique login credentials, enabling organizations to attribute actions to specific individuals. This ensures that in the event of an insider breach, the individual responsible can be easily identified.

Asset Management

Create a list of all of the medical devices used within your organization, including what operating system it uses and what protections are in place. This ensures that medical devices are running on current systems, limiting the risk of a healthcare breach.

Patch Management

Healthcare organizations with medical devices using outdated operating systems are at risk. To implement patches, it is recommended that they contact device manufacturers for updates.

Cybersecurity Policies

What are cybersecurity policies?

Cybersecurity policies are written policies dictating an organization's security controls and procedures. Cybersecurity policies must be aligned with HIPAA standards, including what administrative, technical, and administrative safeguards are in place protecting PHI.

Developing cybersecurity policies, allows an organizations to have a complete picture of their overall cybersecurity. It is essential to implement cybersecurity policies to limit the risk of a healthcare breach. When creating cybersecurity policies, they should address the cybersecurity practices recommended by the HHS.

There should be policies surrounding email protection, endpoint protection, access management, data protection and loss prevention, asset management, network management, vulnerability management, incident response, and medical device security.

How to Implement Cybersecurity Policies

Asses Current Practices before creating a cybersecurity plan, it is important to analyze current security procedures. Effective security measures can remain unchanged while ineffective methods must be updated to ensure the protection of PHI.

Create Policies and Procedures that incorporate HIPAA Security, Privacy, and Breach Notification Rules. Additionally, organizations should include the above-mentioned HHS cybersecurity practices. Policies and procedures must be written and communicated to employees.

Train Employees once a cybersecurity plan is created, employees must be trained to ensure that they are aware of organization's best practices.