TASKNETWORKING

WHITE PAPER

What You Need To Know About HIPAA Security

The U.S. Congress enacted the **HIPAA Security Rule** in 1996 establishing national standards to protect individuals' electronic personal health information (ePHI). The Security Rule applies to all covered entities (health care providers and organizations) and their business associates that work with and transmit ePHI.

Compliance with the HIPAA Security Rule is mandatory for all health care organizations and their business associates, including:

- **Healthcare Providers**
- **Hospitals and Medical Centers**
- **Public Health Authorities**
- **Health Plans**
- **Healthcare Clearinghouses**
- **Self-Insured Employers**
- **Life Insurers**
- **Information System Vendors**
- **Various Service Organizations**
- **Universities**

Policies and Procedures

To ensure compliance with HIPAA regulations, covered entities and their business associates must:

- Document policies and procedures detailing how ePHI will be protected
- Provide these documents to their entire staff
- Require staff be trained to ensure they understand their individual roles and responsibilities in the enforcement of HIPAA policies and procedures

Train Your Employees

The HIPAA Security Rule specifies that it's mandatory for all covered entities and their business associates to implement a HIPAA security awareness/training program for their employees. This is to ensure ePHI is protected through administrative safeguards. Reoccurring security reminders for employees should also be implemented.

Four specific components must be addressed in HIPAA security awareness and training:

- Protection from Malicious Software
- Log-in Monitoring
- Security Reminders
- Password Management

Compliance

The Security Rule requires all HIPAA covered entities and their business associates ensure that ePHI remains confidential and secure at all times, with implementation of appropriate technical, physical and administrative safeguards. IT department staff must understand and continually monitor compliance with the HIPAA Security Rule. It's their role to ensure ePHI is protected from both internal and external IT threats, such as compromised passwords and email attacks.

A HIPAA Business Associate Agreement (BAA)

In the past, business associates of covered entities were directly responsible for compliance with HIPAA Privacy and Security Rules. However this has changed with the new HIPAA Omnibus Final Rule. A HIPAA BAA — a contract between a HIPAA business associate and a HIPAA covered entity — is now required, and must be signed by business associates verifying that they agree to protect ePHI and comply with all HIPAA Security Rules.

Is Encryption a Requirement Under The HIPAA Security Rule?

Encryption isn't required under the HIPAA Security Rule. However, if a risk assessment determines that encryption is an appropriate safeguard, then encryption or an acceptable alternative safeguard must be implemented.

The Top Three Benefits of Encryption:

1. If an encrypted device (desktops, USB drives, and laptops) containing ePHI is stolen, the breach doesn't need to be reported by the business associate or covered entity.
2. The liability of storing ePHI on laptops, desktops or portable devices is reduced with encryption.
3. The cost of encryption is much less than the cost of a potential fine.

What Is The HITECH Act?

The HITECH Act increases the legal liability for non-compliance with the HIPAA Security Rule. It requires business associates, who obtain ePHI under their business associate agreement, to use or disclose ePHI within the terms of the HITECH Act.

Under HITECH, business associates are subject to the same civil and criminal penalties for HIPAA Security Rule violations as are covered entities; so existing business associate agreements must integrate these new security requirements.

To keep ePHI confidential at all times its imperative that:

- Only authorized individuals be allowed to access to ePHI
- User privileges are assigned
- Users should only have access to ePHI for the purpose of fulfilling their roles and responsibilities

According to the HIPAA Privacy and Security Rules, employers will be held accountable for their employees' actions regarding the use or misuse of ePHI.

HIPAA Security Risk Assessment

According to the HIPAA Security Rule and the HIPAA Omnibus Final Rule, it's essential that covered entities and their business associates conduct an accurate assessment of any risks and vulnerabilities regarding the confidentiality of ePHI. This risk management process should include:

- An evaluation of all system threats and vulnerabilities
- A review of all security policies and procedures for HITECH/HIPAA compliance
- Implementation of security safeguards to protect ePHI
- An analysis of how ePHI can be stored and protected at all times

Ensure Compliance with a Security Incident Response Plan (SIRP)

To ensure compliance with the HIPAA Omnibus Final Rule and the HIPAA Security Rule, a Security Incident Response Plan (SIRP) must be implemented. The SIRP outline the steps to take in the event of an incident or security breach. All covered entities are required to maintain documentation of their risk assessment in order to prove that no breaches have occurred.

The director of the Office of Civil Rights (OCR) at the Department of Health and Human Services (HHS) reports that organizations with an SIRP in place will experience less severe or no monetary penalties in the event of a security breach. However, refusal to act or correct issues related to a breach will result in increased monetary penalties.

It's important to keep your SIRP updated as well, and ensure that all employees recognize and report potential data breaches immediately.

Your SIRP Should:

- **Define and Document the Incident**
  Report any and all information regarding the incident, including what happened, who was involved, when it happened and when it was discovered. Document all aspects of the incident, especially who was affected.
- **Stop the Incident**
  Take necessary steps to stop the incident, such as disabling access to a lost smartphone or preventing further access to ePHI.
- **Perform an Immediate Risk Assessment**
  A risk assessment should be performed to determine whether ePHI has been disclosed, if so what was disclosed, and who must be notified.
- **Notify all Affected Individuals/Agencies**
  Breaches that affect over 500 individuals require a significantly increased number of notifications, with notifications sent to individual patients, Health and Human Services (HHS), and possibly the local media.
- **Prevent the Occurrence of Further Incidents**
  Increase your security in an attempt to reduce the risk of further incidences. The purpose of The Security Incident Response Plan is to ensure that the incident isn't repeated in the future.

The process to comply with HIPAA will be long and continuous, but each security measure that's addressed and implemented will bring you one step closer to being HIPAA compliant.

We offer medical practices and any organization impacted by HIPAA a free HIPAA risk assessment. Contact us to learn more at (303) 835-2572.

Task Networking
P.O. Box 1396
Brighton, CO 80601
www.tasknetworking.com
(303) 835-2572