White Paper

Secure Messaging Helps Protect Your Organization from Incurring HIPAA Violations

What's Inside

amtelco

amtelco.com
info@amtelco.com
800.356.9148
4800 Curtin Drive
McFarland, WI 53558

The Department of Health and Human Services' Office for Civil Rights (OCR) conducts occasional audits of covered entities and their business associates to ensure compliance with HIPAA regulations. These entities include health plans, healthcare clearinghouses, and healthcare providers.

Business associates are classified as any business that handles electronic protected health information (ePHI) for a covered entity. ePHI is anything transmitted electronically that can be used to specifically identify a patient: name, date of birth, admission/discharge date, date of death, medical record number, telephone number, address, city, state, postal code, email address, and so forth.

What Are the Financial Impacts of a HIPAA Fine?

OCR audits result in millions of dollars in penalties and incurred costs, which can be devastating to covered entities and their business associates. Actual penalties can vary significantly based on the severity of the

violation, the organization's size and resources, and the level of cooperation with the investigation. However, HIPAA violations can have significant financial impacts on organizations. There are two types of violations, civil and criminal, and each has graded tiers to determine penalties:

Tier 1 (Lack of Knowledge):
Minimum: $137 per violation
Maximum: $68,928 per violation
Annual Cap: $2,134,831

Tier 2 (Reasonable Cause, Not Willful Neglect):
Minimum: $1,424 per violation
Maximum: $71,162 per violation
Annual Cap: $2,134,831

Tier 3 (Willful Neglect, Corrected Within 30 Days):
Minimum: $14,232 per violation
Maximum: $71,162 per violation
Annual Cap: $2,134,831

Tier 4 (Willful Neglect, Not Corrected Within 30 Days):
Minimum: $68,928 per violation
Maximum: No official upper limit

If a HIPAA-covered entity of a business associate violates a HIPAA Rule(s), the violation could be considered criminal. The Department of Justice (DOJ) prosecutes criminal HIPAA violations against people who have purposefully violated HIPAA Rules, resulting in hefty fines and prison sentences.

How Do Data Breaches Happen?

Almost half of all significant breaches occur due to lost or stolen mobile devices. Data breaches in hospitals can happen through various means, including:

Cyberattacks

- Ransomware: Malicious software that encrypts patient data and demands a ransom for its release.

- Phishing: Emails or messages designed to trick employees into clicking on malicious links or downloading attachments, allowing hackers to gain access to systems.
- Hacking: Exploiting vulnerabilities in hospital networks or software to gain unauthorized access to sensitive data.
- Malware: Malicious software like viruses, worms, and Trojans that can infect systems and steal data.

Insider Threats

- Malicious Employees: Employees with access to patient data may intentionally misuse or steal information.
- Accidental Disclosure: Employees may inadvertently share patient information with unauthorized individuals or through unsecured channels.

Third-Party Vendors

- Breaches at Vendor Organizations: If a hospital shares patient data with third-party vendors (e.g., for billing), a breach at the vendor can expose patient information.

Human Error

- Improper Disposal: Improperly disposing of paper records or electronic devices can lead to data exposure.
- Lack of Training: Insufficient training for employees in data security best practices can increase the risk of breaches.

These are just some of the ways data breaches can occur in hospitals. Healthcare organizations must implement robust security measures to protect patient data and minimize the risk of breaches. Ensuring your ePHI is always protected, even on all mobile devices, using encryption and other technical safeguards can help eliminate the potential for a reportable breach of that data.

If an encrypted information breach occurs, it will not be subject to the breach notification rule as the encrypted data is considered to be unusable, unreadable, or indecipherable.

How Can I Protect My Organization?

It's more important than ever to ensure that your organization uses or provides secure, encrypted tools when communicating about patients. Under the HITECH Act of 2009 requirements, which supplemented the HIPAA security guidelines, ePHI handled by both covered entities and their business associates must be transmitted, stored, and accessed securely and protected from reasonable threats and unauthorized access.

Several devices and software solutions, including encryption software for files and databases, data loss prevention solutions (DLP), and virtual private networks (VPNs), can help healthcare organizations enhance data security and comply with HIPAA regulations.

Upgrading from pagers to a secure messaging app can also protect your staff, patients, and organization. In most cases, secure messaging apps offer significantly better HIPAA compliance than traditional pagers. Many apps are specifically designed with HIPAA compliance in mind, offering features like data segmentation, role-based access control, and secure file sharing. Secure messaging apps typically employ end-to-end encryption to protect data both in transit and at rest. However, pagers offer minimal or no encryption, leaving messages highly vulnerable to interception.

Secure messaging apps allow for better control over access and data retention, minimizing the risk of unauthorized access or data breaches, but there is limited control over who can access messages and how long they are stored on pagers. Apps also offer detailed audit trails, making tracking message history and identifying potential security incidents easier.

A modest investment in a secure communication method can be a huge insurance policy to avoid civil and criminal penalties.

7 Tips for Data Protection

You must perform a risk analysis to determine if your ePHI data could be at risk. Here's an example framework and key tips for a data protection strategy:

1). Conduct a Risk Assessment: Identify assets and determine all sensitive data types (e.g., PHI, PII, research data). Evaluate potential threats (cyberattacks, insider threats, physical breaches), and identify weaknesses in systems, devices, and processes.

2). Implement Strong Access Controls: Grant employees only the necessary access to perform their jobs and follow role-based access control (RBAC) to define access permissions based on employee roles. Use multi-factor authentication (MFA) that requires multiple forms of

authentication (e.g., passwords, biometrics, one-time codes), and enforce strong password policies with regular password changes.

3). Data Encryption: Encrypt data at rest when stored on servers, laptops, and mobile devices, as well as data in transit that is transmitted over networks (e.g., VPNs, HTTPS).

4). Employee Training and Awareness: Conduct regular training and phishing simulations to instill best practices, phishing awareness, and the importance of HIPAA compliance. Develop and enforce clear data security policies and procedures.

5). Incident Response Plan: Create a comprehensive incident response plan to address data breaches effectively and test it. Have a clear process for notifying patients, regulators (like the HHS Office for Civil Rights), and law enforcement in case of a breach.

6). Technology Solutions: Implement firewalls to protect the network perimeter from unauthorized access. Monitor network traffic for malicious activity by using intrusion detection and prevention systems (IDPS), and employ data loss prevention (DLP) solutions: Prevent sensitive data from leaving the organization through unauthorized channels.

7). Audits and Monitoring: Conduct periodic audits to assess the effectiveness of security controls and continuously monitor system logs for suspicious activity. Run regular risk assessments of applicable third-party vendors.

Stay current on the latest cybersecurity threats and best practices and keep informed about changes to HIPAA regulations and other relevant laws. An easy way to do this is to establish Google Alerts to monitor the web for new content.

Whatever strategy you choose, remember to tailor it to your organization's specific needs and resources. Involve all departments and employees in the data protection effort. Ask your vendors for their input, and make data security a continuous and evolving process.

Please contact us with questions.

800.356.9148

info@amtelco.com

amtelco.com

4800 Curtin Drive
McFarland, WI 53558

amtelco