ACUPUNCTURE Today

YOUR PRACTICE / BUSINESS

Common HIPAA Violations Every Acupuncturist Should Know

David Bibbey, Dipl. Ac., LAc | DIGITAL EXCLUSIVE

WHAT YOU NEED TO KNOW

- Encryption is a critical tool in protecting PHI data from falling into the wrong hands. To prevent this from happening, acupuncturists should follow the National Institute of Standards & Technology (NIST) recommendations.
- Hacking often results in HIPAA violations. To combat this risk, acupuncturists should keep anti-virus software up to date and regularly change passwords that hackers may find difficult to penetrate.
- Unauthorized access by employees (or anyone else) should be prevented through an authorization and verification system.
- Protecting your patients' and clinic's PHI is essential for maintaining compliance with state and federal privacy, data security and consumer protection laws.

Consequences for HIPAA violations can often be quite harsh. If someone has breached the HIPAA privacy regulations – even without any malicious intent, civil penalties are applicable: $100 per violation for unawareness, a minimum of $1,000 for reasonable cause, a minimum of $10,000 if willful neglect is present and then rectified, and finally, a minimum of $50,000 for individuals who act with willful neglect and ignore the issue.

As you can see, ignoring HIPAA requirements exposes acupuncturists to the greatest risks for data breaches, complaints and costly fines. Here are some HIPAA violation examples so you can avoid them.

Encryption

Encryption is a critical tool in protecting PHI data from falling into the wrong hands. To prevent this from happening, acupuncturists should follow the National Institute of Standards & Technology (NIST) recommendations for using encryption tools to add a layer of cybersecurity. This helps ensure that any communication containing patient information is secure and only accessible by authorized providers and business associates.

Hacking

Hacking often results in HIPAA violations. To combat this risk, acupuncturists should keep anti-virus software up to date and regularly change passwords that hackers may find difficult to penetrate. Additionally, if you have staff, employee training sessions on cyberthreats should also be conducted regularly.

Unauthorized Access

Unauthorized access by employees (or anyone else) should be prevented through an authorization and verification system. This ensures patient data remains protected from anyone who does not have permission to view it. It also helps ensure compliance with regulations such as the HIPAA privacy & security rules.

Device Loss / Theft

Loss or theft of devices is common, but data loss and breach can be avoided with encryption safeguards. All devices containing PHI data should be encrypted to prevent unauthorized access in the event they are lost or stolen. Passwords should also be changed regularly according to company policy.

Lack of Training

HIPAA also requires covered entities to provide staff training on how to comply with the law. Failing to complete and document this training often results in staff being unaware of their responsibilities under the privacy & security rules, meaning providers and staff commit violations without realizing it.

Failing to Document Policies & Procedures

HIPAA requires covered entities to have written policies and procedures in place for handling PHI. However, many covered entities fail to document or follow these procedures, which can lead to mistakes being made that could put patient information at risk.

Retaliation Against Employees

Many HIPAA complaints and audits begin with an employee or patient whistleblower. HIPAA prohibits covered entities from retaliating against employees and patients who report violations or participate in investigations. However, many clinic owners retaliate against those cooperating with auditors, which only compounds a provider’s troubles.

Final Thoughts

Protecting your patients' and clinic’s PHI is essential for maintaining compliance with state and federal privacy, data security and consumer protection laws. Taking proactive steps, such as documenting office policies and procedures to manage PHI, encrypting patient data, using a HIPPA-compliant email service and HIPAA-compliant web hosting, can all help protect patient’s sensitive information and reduce the risks posed by cyberattacks and other unauthorized data access.

Getting help to implement software and providing staff training on cybersecurity threats is the first step needed to help providers respond and defend against data thieves. Using a checklist is a helpful way to get started: https://www.netsec.news/hipaa-compliance-checklist/.

JANUARY 2024