INFO SHEET

Five Strategies To Help Enhance HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules have been in place for over 20 years, yet some healthcare organizations still struggle with compliance. A thorough review of your current approach to HIPAA privacy and security compliance is crucial to safeguard patients' protected health information (PHI) and mitigate organizational risk and liability.

Here are five strategies to help enhance your HIPAA compliance program:

1. **Provide comprehensive and accessible staff training:**

HIPAA compliance problems often stem from a lack of staff awareness of privacy rules or negligence when handling PHI, including electronic protected health information (ePHI). Covered entities must provide training to new hires within a reasonable amount of time, before they have access to PHI. Furthermore, annual or periodic training is extremely important to keep employees informed and reinforce the importance of protecting PHI. Training must cover the regulations and best practices for maintaining information, confidentiality, and cybersecurity. In addition, covered entities must go over their site-specific privacy and security policies along with procedures for affected employees. Online training modules can be beneficial to help staff easily understand HIPAA requirements and best practices. Not only can staff access the tools at their convenience, but the system can document training completion to demonstrate compliance.

2. **Keep policies and procedures up-to-date:**

Regular reviews of your HIPAA compliance program—ideally annually—are imperative. Cover areas like assessing information privacy and security risks, protective measures for sensitive health information, and breach response strategies across verbal, electronic, and paper-based communications.

3. **Address cybersecurity threats strategically:**

Robust security and encryption software is crucial. Staff education on recognizing and mitigating threats—particularly phishing emails, ransomware, and malware—should evolve rapidly in response to new cyber threats. Healthcare facilities should implement the 405(d) cybersecurity practices or another recognized security program.

4. **Define medical record request procedures:**

Establishing clear procedures for handling patient requests and third-party access is essential. Educate staff on handling medical record requests. Prioritize easy patient access to medical information. Adhering to HIPAA guidelines while allowing patient information accessibility is critical.

5. **Be prepared for investigations:**

The Office for Civil Rights (OCR) investigates HIPAA violations triggered by patient complaints, reported breaches, or agency concerns. Preparedness involves having current HIPAA policies, security and privacy risk analyses, well-documented staff training, and effective security controls and mitigation solutions to minimize breach occurrences.

At Stericycle, we offer a comprehensive program that includes assessment assistance, training, and more, serving as a valuable resource when you are creating, modifying, and sustaining your HIPAA compliance program. For further information, visit Stericycle.com/HIPAA.

Stericycle®
We protect what matters.