FACT SHEET

Your Cheat Sheet for Protecting Healthcare Data

Ensuring the security of sensitive healthcare data is critical for healthcare organizations. Here is what you and your team need to know to help safeguard protected health information (PHI) and maintain regulatory compliance with HIPAA and HITECH:

Your Security Best Practices Checklist

- **Check Compliance Regulations:** Regularly check for updates to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) to stay compliant.
- **Implement a Healthcare Information Security Strategy:** Develop a comprehensive plan covering risk identification, vulnerability assessments, protection measures, threat responses, and recovery strategies to safeguard protected health information (PHI) and electronic protected health information (ePHI).
- **Conduct Regular Employee Training:** Conduct ongoing training sessions to enhance employee awareness of privacy and security issues, utilizing solutions like Stericycle's Steri-Safe® HIPAA Training & Compliance.
- **Use Early Detection Tools:** Deploy intrusion detection and prevention systems to identify and prevent unauthorized access or attacks on PHI.
- **Update Business Continuity Plans:** Maintain up-to-date disaster recovery plans to efficiently respond to and recover from data breaches.
- **Enforce Mobile Device Security Policies:** Implement policies and security features such as encryption, Multi-factor Authentication (MFA), and endpoint security software to protect data on mobile devices.
- **Verify Vendor Compliance:** Ensure that all business associates have conducted appropriate healthcare IT risk analysis and are also safeguarding your healthcare facility's PHI.
- **Use Professional Document Destruction Services:** Partner with a trusted shredding company that offers services for paper and hard drive destruction to securely dispose of sensitive documents and help maintain HIPAA compliance.

Top 5 Risky Healthcare Documents:

1. **Patient Chart and Treatment Details:** Discarded and obsolete patient charts containing treatment details must be safely destroyed to prevent ethical violations and legal risks. It's not just good practice – it's the law.
2. **Drug and Rx Information:** Proper storage and destruction of medication, dosage, and prescription information are crucial to prevent prescription fraud.
3. **Registration and Payment Documents:** Personally Identifiable Information (PII) in registration and payment documents—such as IDs, credit cards, billing information, addresses, and phone numbers—must be securely stored or shredded to mitigate the risk of identity theft.
4. **Insurance Documents:** Safeguarding insurance documents is essential to protect patient identity and maintain the hospital's reputation.
5. **Diagnosis Records:** Patient diagnosis documents should only be shared with authorized personnel to avoid regulatory risks and ensure patient confidentiality.

By following these guidelines, healthcare organizations can effectively help safeguard patient information, mitigate risks, and uphold regulatory compliance standards.

We protect what matters.℠

Shred-it®
A Stericycle® Solution