INFO SHEET

5 Top Cybersecurity Threats and 10 Mitigating Practices to Help Combat Them

Healthcare organizations are high-priority targets for cyber-attacks, making the frequency of data breaches within the healthcare sector a cause for concern. In the first half of 2023, there were around 295 reported breaches, as per data from the HHS Office for Civil Rights (OCR) breach portal.

To address these challenges, the 405(d) Task Group has developed the "Health Industry Cybersecurity Practice (HICP): Managing Threat and Protecting Patients." This document provides relevant information about security threats affecting the healthcare sector and aims to further strengthen it against cyber threats.

5 TOP CYBERSECURITY THREATS AND IMPACTS

1. **Social Engineering:** Manipulates individuals to reveal sensitive information, leading to data breaches.
2. **Ransomware Attack:** Locks information assets for ransom, disrupting healthcare operations and risking data loss and identity theft.
3. **Loss or Theft of Equipment or Data:** Results in breaches of sensitive information and potential patient identity theft.
4. **Insider Data Loss:** Accidental or malicious removal of data can lead to breaches and compromise patient privacy.
5. **Attacks on Medical Devices:** Endanger patient safety, treatment, and well-being.

HICP'S 10 MITIGATING PRACTICES

Practice		Why is it relevant?
1	**Email Protection Systems**	Strengthen email security through configuration, education, and phishing simulations to help prevent credential theft and malware attacks.
2	**Endpoint Protection Systems**	Implement basic security controls for endpoints, including patching, firewalls, and multi-factor authentication to combat ransomware and device-related threats.
3	**Access Management**	Control user access through role-based access, regular reviews, and immediate de-provisioning to address various cyber threats.
4	**Data Protection and Loss Prevention**	Establish data classification policies, handling procedures, and workforce training to safeguard against data breaches and losses.
5	**Asset Management**	Maintain an up-to-date inventory of IT assets and securely decommission devices to mitigate social engineering and data loss risks.
6	**Network Management**	Segment networks, enforce physical security, and employ intrusion prevention systems to protect against ransomware and device attacks.
7	**Vulnerability Management**	Regularly scan for vulnerabilities, perform web application scans, and prioritize remediation to address cyber threats effectively.
8	**Incident Response**	Develop a comprehensive incident response plan, participate in information-sharing organizations, and automate incident documentation and remediation.
9	**Network Connected Medical Devices**	Ensure secure medical device practices are documented and updated to mitigate attacks on patient safety.
10	**Cybersecurity Oversight and Governance**	Establish cybersecurity governance, policies, and procedures. Also, conduct risk analysis and cybersecurity training to address various threats comprehensively.

Healthcare organizations have a responsibility to do everything they can to safeguard patient-protected health information (PHI) and meet necessary compliance.

Learn how Steri-Safe® HIPAA Compliance Solutions can help you comply with HIPAA Privacy and Security Rule obligations.

Stericycle®
We protect what matters.