HIMSS

Cybersecurity in Healthcare: A Critical Concern

Cybersecurity in the healthcare and public health sector is of paramount importance. Healthcare organizations face unique challenges, due to the high value of their data, the widespread use of connected devices, and the complex data exchanges required for patient care, care coordination, administrative functions, and other critical operations.

Key Challenges in Healthcare Cybersecurity:

Sensitive Data: Healthcare organizations are entrusted with a wide range of sensitive data, including protected health information (PHI), personally identifiable information (PII), and proprietary information, all of which must be safeguarded.

Ransomware Attacks: Ransomware is a type of malware (malicious software) that prevents victims from accessing their computer files, data, systems, devices, or networks and demands that victims pay the ransom so that access is restored. However, paying the ransom does not guarantee that access will be restored or data recovered.

Legacy Systems/Devices: Unsupported systems/devices may not be regularly updated or patched and will typically require compensating controls.

Connected Devices: Healthcare organizations use a wide variety of connected devices, such as HVAC systems, lighting systems, security cameras, smart elevators, and medical devices. Any of these, if compromised, can affect patient safety and/or disrupt healthcare operations.

Insider Threats: Individuals with trusted physical or technical access to an organization's assets can, either intentionally or unintentionally, cause data breaches, system disruptions, or otherwise cause harm to the organization, its assets, or its data.

Key Strategies for Improving Healthcare Cybersecurity Posture:

Data Encryption: Encrypting sensitive patient data both in transit and at rest is essential for safeguarding against unauthorized access. Effective encryption reduces the likelihood of compromise. Robust key management practices, including regular key rotation, secure storage, and access control, are critical to ensure that encryption keys themselves are not vulnerable to attack.

Multi-Factor Authentication (MFA): Implementing phishing-resistant MFA can significantly reduce the risk of unauthorized access to systems, software, and devices.

Regular Updates: Regularly updating systems, software, and devices with the latest updates and patches to mitigate vulnerabilities and ensure optimal performance.

Workforce Training: Regular cybersecurity training helps staff identify phishing attempts, follow best practices, and understand the importance of protecting patient information as well as sensitive and proprietary information.

Incident Response: Healthcare organizations must have comprehensive incident response plans to quickly contain, eradicate, and respond to security incidents. Rapid response is essential for minimizing harm and protecting patient safety.

Business Continuity: Business continuity is a comprehensive strategy developed by the organization to ensure that critical functions such as clinical care, administrative operations, and other essential services can continue during disruptive events, like natural disasters, cyberattacks, or equipment failures. It involves contingency planning to maintain operations and minimize downtime.

Disaster Recovery: Disaster recovery is a component of business continuity that specifically focuses on the recovery and restoration of IT systems, data, and applications following a disruptive event. It ensures that healthcare systems can quickly resume normal operations after manmade or natural disasters.

Compliance: In the United States, healthcare organizations must comply with HIPAA, which establishes national standards for safeguarding protected health information, along with other federal, state, and contractual obligations. Globally, various jurisdictions have established their own data protection mandates governing the protection of personal data, including individually identifiable health information.