HealthManagement
Promoting Management and Leadership

Safeguarding Patient Care: The Imperative of Infusion Pump Cybersecurity

Inadequate cybersecurity within healthcare systems poses a significant threat to patient safety. This assertion, supported by the American Hospital Association, underscores the urgent need for aligning cybersecurity initiatives with patient safety protocols to protect both patient well-being and network integrity. Brian Heersink, the IT Director at San Luis Valley Health in Alamosa, Colorado, highlights a commonly overlooked vulnerability: infusion pump systems. These devices, originally designed solely for medication delivery, now serve as potential entry points for cyberattacks due to their integration into hospital networks. The risks associated with outdated software, firmware, and inadequate patching render them susceptible to exploitation by malicious actors.

The Vulnerability of Infusion Pump Systems to Cyberattacks

The evolution of infusion pumps from standalone devices to network-connected systems has inadvertently exposed them to cybersecurity threats. As these pumps became integrated into hospital networks for software updates and data transmission, their susceptibility to cyber intrusions escalated. Heersink warns of instances where hackers infiltrated hospital networks through compromised infusion pumps, using them as gateways to launch attacks on broader network infrastructure. This heightened connectivity, particularly with the requirement for live connections between electronic medical records and infusion pumps, exacerbates the vulnerability.

Advocating for Comprehensive Cybersecurity Solutions

Although some healthcare organisations have attempted to mitigate these risks by isolating infusion pumps from their networks, Heersink argues that such measures are insufficient. Instead, he advocates for investing in comprehensive cybersecurity solutions that facilitate the management of cybersecurity certificates, pump provisioning, and robust authentication and encryption protocols. Certificates play a crucial role in ensuring secure communication by allowing interaction only with known devices while also aiding in data encryption. Pump provisioning offers the benefit of targeted response to security breaches, enabling the isolation of compromised pumps without disrupting the entire fleet and jeopardising patient care.

San Luis Valley Health's Proactive Approach to Cybersecurity

San Luis Valley Health exemplifies proactive cybersecurity measures by investing in the Ivenix Infusion System. This advanced system incorporates sophisticated computer technology equipped with firewalls and intrusion prevention capabilities, enabling prompt patching and upgrades to ensure uninterrupted medication delivery. The system's seamless management of wireless settings and software updates minimises the need for extensive human intervention, alleviating the burden on multiple teams and enhancing network security. Furthermore, its ability to perform background updates of drug libraries without disrupting clinical workflows enhances patient safety.

Ensuring Uninterrupted Patient Care Through Cybersecurity Measures

Given the historical vulnerability of infusion pumps to security breaches, Heersink emphasises the importance of collaborating with vendors knowledgeable in both medication management and cybersecurity principles. By prioritising security-conscious vendors with a long-term cybersecurity vision, healthcare organisations can better safeguard infusion pumps and, by extension, protect patient care. He underscores the necessity for infusion pump security to be an integral component of any healthcare organization's cybersecurity strategy, stressing that securing these devices not only shields networks from potential threats but also ensures uninterrupted delivery of critical patient care services.

The intersection of healthcare and cybersecurity underscores the critical importance of protecting infusion pump systems to safeguard patient safety and network integrity. As these devices become increasingly integrated into hospital networks, healthcare organizations must prioritize comprehensive cybersecurity measures to mitigate risks effectively. By investing in advanced systems and collaborating with knowledgeable vendors, healthcare providers can fortify their cybersecurity posture and ensure continuous, secure delivery of lifesaving medications to patients.

Source: **Health IT News**

Image Credit: **iStock**

Published on : Tue, 30 Apr 2024