Workers' Comp

Specialty Solutions Spotlight: Cybersecurity Risks With Internet Connected Medical Devices

January 15, 2024
3 MIN READ
Author profile image

Ebonee Hunter-Goldsby

Senior Manager, Customer Service

Are internet-connected medical devices a cybersecurity risk?

The advent of the Internet of Medical Things (IoMT) has facilitated the transmission of data from medical devices and enabled physicians to remotely customize treatment settings. However, like other computer systems, medical devices are susceptible to security breaches, which have the potential to compromise the device's safety and effectiveness.

The health care sector is a prime target for cyberattacks, with hospitals accounting for 30% of major data breaches. Frequently, medical devices stay in operation despite outdated serviceability, potentially exposing vulnerabilities that attackers can exploit.

A security company report identified nurse call systems, infusion pumps and medication dispensing technologies as the most high-risk medical devices with internet connectivity. This conclusion was drawn based on an analysis of common vulnerabilities and exposures (CVEs). The assessment conducted by the security company revealed that 39% of nurse call systems and 27% of infusion pumps have unpatched critical CVEs.

Unfortunately, numerous medical devices are exposed to cybersecurity risks because of outdated software, insufficient encryption and weak password security. These vulnerabilities can be exploited by cybercriminals to compromise patient data, enabling them to engage in activities such as identity theft, fraud and other malicious acts.

After years of concerns regarding the vulnerability of an increasing number of internet-connected medical devices used in hospitals and health care facilities to hacking and ransomware attacks, the Food and Drug Administration (FDA) has implemented new recommendations. The document offers guidance on ensuring medical devices align with cybersecurity standards to reduce potential risks.

According to the updated guidance, all prospective manufacturer applicants for new medical devices are now required to present a comprehensive strategy outlining how they intend to monitor, detect and resolve cybersecurity concerns. Additionally, they must establish a systematic approach that ensures a reasonable level of protection for the device under consideration. Manufacturers will be responsible for regularly releasing updates and patches, both as part of predetermined schedule and during critical circumstances. Furthermore, they are obligated to furnish the FDA with a software bill of materials, encompassing any open-source or other software utilized in their devices.

Maintaining the health of medical devices and safeguarding personal information is not solely the responsibility of device manufacturers and health care providers. Patients and caregivers also have a vital role to play in this regard. The FDA provides the following tips to consider:

- Adopt good password practices.
- Maintain physical control over the device.
- Only establish connections between other devices/software if both device manufacturer and health care provider approve.
- Regularly update the device to ensure optimal protection.
- Consult the device manufacturer or health care provider to acquire specific best practices.

As the utilization of wireless, internet-connected devices, portable media and the regular electronic sharing of medical device information continues to rise, the significance of proficient cybersecurity will continue to grow, emphasizing the necessity to safeguard device functionality and safety.

This information is meant to serve as a general overview, and any specific questions should be fully reviewed with a health care professional or specialty service provider.

To make a referral for specialty solution services, call us today at 877.203.9899 or send an email to referrals@apricusinc.com.

Resources:

https://www.healthcaredive.com/news/medical-device-cybersecurity-risk/648306/

https://www.cnn.com/2023/03/29/tech/fda-medical-devices-secured-cyberattacks/index.html

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#:~:text=Medical%20devices%2C%20like%20other%20computer,cybersecurity%20risks%20is
.

https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

©2022 Enlyte Group, LLC.

mitchell | genex | coventry