Health Care Risk Insights

Brought to you by: Medical Society of Virginia Insurance Agency

MSV℠ INSURANCE AGENCY

Cyber Security for Medical Devices and Hospital Networks

Many medical devices contain configurable embedded computer systems that can be vulnerable to cyber-security breaches. In addition, as medical devices are increasingly interconnected via the Internet, hospital networks, other medical devices or smartphones, there is an increased risk of cyber-security breaches, which could affect how a medical device operates.

The Food and Drug Administration (FDA) has recently become aware of cyber-security vulnerabilities and incidents that could directly impact medical devices or hospital network operations, such as the following:

- Network-connected/configured medical devices infected or disabled by malware
- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems and implanted patient devices
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical and maintenance personnel)
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices)
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals and poor coding/SQL injection.

The FDA has been working closely with other federal agencies and manufacturers to identify, communicate and mitigate vulnerabilities and incidents as they are identified.

FDA Recommendations/Actions

The FDA Has a number of recommendations to mitigate the risks that technology may pose to health care organizations.

For all device manufacturers:

Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cyber security, and are responsible for putting appropriate mitigations in place to address patient safety and ensure proper device performance.

The FDA expects medical device manufacturers to take appropriate steps to limit the opportunities for unauthorized access to medical devices. Specifically, it is recommended that manufacturers review their cyber-security practices and policies to ensure that appropriate safeguards are in place to prevent unauthorized access or modification to their medical devices or compromise the security of the hospital network that may be connected to the device. The extent to which security controls are needed will depend on the medical device, its environment of use, the type and probability of the risks to which it is exposed, and the probable risks to patients from a security breach.

In evaluating your device, consider doing the following:

- Take steps to limit unauthorized device access to trusted users only, particularly for those devices that are life-sustaining or could be directly connected to hospital networks.
- Appropriate security controls may include user authentication, such as user ID and password, smartcard, or biometrics; strengthening password protection by avoiding hard-coded passwords and limiting public access to passwords used for technical device access; physical locks; card readers; and guards.
- Protect individual components from exploitation and develop strategies for active security protection appropriate for the device's use environment. Such strategies should include timely deployment of routine, validated security patches and methods to restrict software or firmware updates to authenticated code. The FDA typically does not need to review or approve medical device software changes made solely to strengthen cyber security.
- Use design approaches that maintain a device's critical functionality, even when security has been compromised, known as "fail-safe modes."
- Provide methods for retention and recovery after an incident where security has been compromised.
- Cyber-security incidents are increasingly likely and manufacturers should consider incident response plans that address the possibility of degraded operation and efficient restoration and recovery.

For health care facilities:

The FDA recommends that you take steps to evaluate your network security and protect your hospital system. In evaluating network security, hospitals and health care facilities should consider doing the following:

- Restricting unauthorized access to the network and networked medical devices
- Making certain that appropriate antivirus software and firewalls are up to date
- Monitoring network activity for unauthorized use
- Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services
- Contacting the specific device manufacturer if you think you may have a cyber-security problem related to a medical device
    - If you are unable to determine the manufacturer or cannot contact the manufacturer, the FDA may be able to assist in vulnerability reporting and resolution.
- Developing and evaluating strategies to maintain critical functionality during adverse conditions

Reporting Problems to the FDA

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. If you suspect that a cyber-security event has impacted the performance of a medical device or has impacted a hospital network system, file a voluntary report through MedWatch, the FDA Safety Information and Adverse Event Reporting program.

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Device manufacturers must comply with the Medical Device Reporting (MDR) regulations.

Contact the cyber security professionals at Medical Society of Virginia Insurance Agency today to discuss how to keep your health care facility safe and secure from cyber threats.

This Risk Insights is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.