PREMIER PERSPECTIVES

Six Things You Need to Know About Medical Devices and Cybersecurity

Concern over cybersecurity touches our lives in new ways almost daily. Today, there is growing concern over millions of people who use connected medical devices that use off-the-shelf software.

Here are six things the FDA's Center for Devices and Radiological Health wants you to know about the safety of networked medical devices:

1. Hacking of commercially-available software can give attackers unauthorized access to networks and medical devices, compromising device effectiveness and patient safety. This concern prompted the agency guidance that covers major responsibilities for makers of devices using this software.
2. What's affected? Examples include systems that obtain, archive, and communicate pictures on networks at healthcare facilities (such as computed tomography, magnetic resonance, ultrasound, and nuclear medicine), systems that monitor patient activity (such as ECG systems), and those that communicate with clinical labs.
3. FDA guidance explaining agency rules for makers of devices that use off-the-shelf software and connect to networks also may be useful to others responsible for keeping networked devices safe, such as suppliers of network software and hardware (e.g., computers, routers, and operating systems) and healthcare organizations and administrators who set up and maintain networks of connected devices.
4. While device manufacturers do not routinely need FDA approval to implement software patches, such authorization is required when a patch would change what the software does and how it works or would make the device less safe and effective.
5. Manufacturers must validate software changes under the agency's Quality Systems regulation, providing evidence that the revised software meets user needs and consistently does what it is supposed to do.
6. Most of the responsibility for assuring security lies with device makers. In the FDA's view, healthcare organizations rarely have enough technical resources and information on the design of medical devices to independently maintain device software.

How Can We Help?

Premier's regulatory group can:

- Perform a cybersecurity gap analysis and present a report outlining overall risk
- Assist in the development of mitigation steps and work with you to implement a strategy that will bring your product(s) into compliance
- Provide on-going support and insight as regulations change or if new products require additional review

AUTHOR DETAILS

Joanne Emmett has been part of the clinical research industry for 20+ years with a keen focus on operational design and delivery. Since joining Premier Research, she has been responsible for the operational delivery structures and planning for both clinical and project management. She focuses on the key needs and standards relevant to medical device and diagnostics, ensuring core process, training designations for pricing, staffing, and oversight as well as including the unique regulatory and scientific avenues required for medical device.

Nach Davé oversees Premier Research's regulatory affairs service offerings across its broad range of therapeutic focus areas, bringing to his position more than 20 years of experience in the pharmaceutical and contract research industries. Mr. Davé holds a master's degree in drug regulatory affairs from Long Island University and a bachelor's degree in pharmacy from the Philadelphia College of Pharmacy and Sciences. He is a registered pharmacist in the state of New Jersey.