Codify
BY AAPC

Health Information Compliance Alert

Security Rule: Find Out What The FDA Has In Store For Medical Device Security

Employ these 5 strategies now to add your own layer of protection.

Medical devices like dialysis machines, patient monitors, medication dispensers, and ventilators are extremely common in the healthcare industry. But these devices often rely on their connection to provider networks, which are always vulnerable to hackers and other unauthorized access.

Good news: Now the **U.S. Food and Drug Administration** (FDA) is giving medical device security the much-needed attention that it deserves.

What Dangers Do Medical Devices Pose?

Problems: The rising risks, threats, and inherent vulnerabilities of medical devices have been documented, warned attorneys **Kirk Davis** and **Jason Betke** of **Akerman LLP** in a recent analysis. And the FDA, which is responsible for guidance on medical devices, has acknowledged that certain devices are susceptible to breaches. In fact, the FDA has pinpointed cybersecurity vulnerabilities in medical devices that could allow unauthorized users to not only access patient data, but also control the device.

"The FDA's oversight comes at a critical time, as hospitals are increasing the amount of network-connected medical devices used in the delivery of care," Davis and Betke wrote. "With the ongoing changes in healthcare technology, many providers remain unaware that medical devices pose a unique and serious cybersecurity risk to patient safety and data privacy."

Because of the risks of unauthorized individuals accessing the provider networks and wireless connections for remote access to medical devices, the FDA issued a draft guidance on Jan. 15 that outlines its post-market recommendations for medical device manufacturers to proactively monitor, identify, and address cybersecurity vulnerabilities.

Significance: "The FDA's initiatives further its continuing efforts to ensure the security and effectiveness of medical devices at all stages in their lifecycle," noted attorney **Steven Richard** in a Jan. 19 **Nixon Peabody LLP** blog posting. "The guidance is the FDA's latest initiative to improve cybersecurity information-sharing and risk-based standards since the White House's issuance of Executive Order 13636 in 2013 and Presidential Policy Directive 21 to mobilize the public and private sectors to engage in the collective strengthening of critical cybersecurity infrastructure."

Guidance Addresses Devices' Entire Lifecycle

The FDA's draft guidance recommends that device manufacturers implement a structured and systematic comprehensive cybersecurity risk-management program, and respond in a timely manner to identified vulnerabilities. The recommended program should include the following critical components:

- Applies the 2014 NIST voluntary Framework for Improving Critical Infrastructure Cybersecurity;
- Monitors cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;

- Understands, assesses, and detects the presence and impact of a vulnerability;
- Establishes and communicates processes for vulnerability intake and handling;
- Clearly defines essential clinical performance to develop mitigations that protect, respond, and recover from the cybersecurity risk;
- Adopts a coordinated vulnerability disclosure policy and practice; and
- Deploys mitigations that address cybersecurity risk early and prior to exploitation.

In most cases, the FDA will consider manufacturers' efforts to address cybersecurity vulnerabilities and exploits as "cybersecurity routine updates or patches," for which the FDA won't require advance notification, additional premarket review, or reporting under its regulations. But for certain vulnerabilities that could compromise a device's essential clinical performance and present "a reasonable probability of serious adverse health consequences or death," the FDA would require manufacturers to notify the agency.

Under the draft guidance, if a manufacturer addresses a vulnerability quickly and in a way that sufficiently reduces the risk of harm to patients, the FDA won't enforce urgent reporting. But manufacturers must also meet certain other conditions, including:

- There are no serious adverse events or deaths associated with the vulnerability;
- The manufacturer notifies users and implements changes that reduce the risk to an acceptable level within 30 days of learning of the vulnerability; and
- The manufacturer is a participating member of an Information Sharing Analysis Organization (ISAO) and reports the vulnerability, its assessment and remediation to the ISAO.

Implement 5 Cybersecurity Strategies

In addition to the new FDA draft guidance, the **HHS Office of Inspector General** (OIG) has also launched an initiative in its 2016 Work Plan to examine whether the FDA's current oversight of networked medical devices adequately protects patient health and data, according to Davis and Betke. "The oversight by the FDA and OIG in the healthcare industry underscore the potential life-threatening perils that could arise from cybersecurity breaches involving medical devices."

So what should healthcare providers and health plans do? Healthcare organizations should apply enterprise-wide protections to mitigate breaches and enhance the safety of medical devices, Davis and Betke advised. Among other strategies, you should:

1. Understand your organization's cybersecurity risks by reviewing medical devices, operating systems, and authorized users;
2. Implement/update your medical device management policies;
3. Establish security risk assessments for medical devices;
4. Evaluate your network security (e.g., restrict access, monitor activity, maintain and update antivirus software); and
5. Encrypt data.

Bottom line: "As more devices reside on provider networks, it is only a matter of time before the vulnerabilities found within such devices are tested," Davis and Betke cautioned. "Providers should not require a breach as a prerequisite for implementing medical device safety measures, but instead should work vigilantly within their organizations, and with medical device manufacturers, to maintain the cybersecurity of their instrumentation."

Link: The draft guidance has a 90-day public comment period. To read the FDA's new draft guidance, go to www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.