Cyberattacks and Data Breaches: Are Medical Devices at Risk?

By Yvonne Flaherty

Technological advances in medical devices can improve the functionality of the devices and provide health care providers with increased tools to combat serious health concerns in patients. Many medical devices now have the ability to electronically track vital statistics, monitor diagnostics and transmit patient specific data. According to the FDA, as medical devices become more interconnected, they can improve the care patients receive and create efficiencies in the health care system. However, some medical devices can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device – and comprising the personal data of the individual patient. Indeed, heart rate monitors, X-ray communication systems and insulin pumps have proven vulnerable to cyberattacks. With the increased use of wireless devices and the exchange of health information electronically, there needs to be a focus on cybersecurity to ensure the effectiveness of these medical devices. "There is no such thing as a threat-proof medical device," said Suzanne Schwartz, M.D., MBA, director of emergency preparedness/operations and medical countermeasures at the FDA's Center for Devices and Radiological Health. "It is important for medical device manufacturers to remain vigilant about cybersecurity and to appropriately protect patients from those risks."

Yvonne Flaherty is a partner at Lockridge Grindal Nauen P.L.L.P. and leads the firm's drug and device department. She focuses her practice on the representation of injured parties in complex litigation against pharmaceutical and medical device manufacturers, as well as class actions involving product defect claims.

In response to increased concerns regarding cyberattacks, the Food and Drug Administration opened a cybersecurity lab and issued recommendations to manufacturers for managing cybersecurity risks. These recommendations, issued in October 2014, include steps which manufacturers should take in the design phase to reduce the risk that device functionality is compromised as well as steps that manufacturers should take to maintain the integrity of both the device and the data connected to the device. The final guidance was issued in a report, titled, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." In this report, the FDA recommends that manufacturers submit documentation to the FDA about the risks identified and controls in place to mitigate those risks. The guidance also recommends that manufacturers take an additional step and submit their plans for providing patches and updates to operating systems and medical software.

Unfortunately, despite the FDA guidance, which is currently voluntary for device manufacturers, patients are still at risk. White House cybersecurity coordinator Michael Daniel said medical device manufacturers need to more effectively incorporate cybersecurity into the development of their products. "I think it goes back to some of the root design of just making cybersecurity one of the design features included in any [medical] device or product, the same way we have incorporated electrical security into all of our appliances," Daniel said at an FDA workshop.

Earlier this year, FDA issued additional recommendations to manufacturers regarding cybersecurity for networked medical devices. The guidance is drafted in a question and answer format. Key points and include:

- The device manufacturer bears the responsibility for the continued safe and effective performance of the medical device, including the performance of OTS (off the shelf) software that is part of the device.
- The need to be vigilant and responsive to cybersecurity vulnerabilities is part of the device manufacturer's obligation under 21 CFR 820.100 to systematically analyze sources of information and implement actions needed to correct and prevent problems.

> "It is important for medical device manufacturers to remain vigilant about cybersecurity and to appropriately protect patients from those risks."

- Under 21 CFR 820.30(g), design validation requires that devices conform to defined user needs and intended uses, including an obligation on the device manufacturer to perform software validation and risk analysis. Software changes to address cybersecurity vulnerabilities are design changes and must be validated before approval and issuance. 21 CFR 820.30(i).
- FDA premarket review is generally not required prior to implementation of a software patch to address a cybersecurity vulnerability. A PMA supplement is required for a software patch only if the patch results in a change to the approved indications for use or is deemed by the manufacturer to have an adverse effect on the safety and effectiveness of the approved medical device. 21 CFR 814.39. Otherwise, the device manufacturer should report the decision to apply a software patch to FDA in their annual reports. 21 CFR 814.39(b), 814.84.
- Device manufacturers should validate all software design changes, including computer software changes to address cybersecurity vulnerabilities, according to an established protocol before approval and issuance. 21 CFR 820.30(i).
- Device manufacturers should develop a single cybersecurity maintenance plan to address compliance with the QS regulation and the issues discussed in the guidance document.
- Device manufacturers should report cybersecurity patches if software patch affects the safety or effectiveness of the medical device.

In addition to the guidelines referenced above, FDA has implemented an industrial control systems cyber emergency response team and has issued an official safety communication regarding cybersecurity for medical devices and hospital networks. This communication sets forth additional steps that should be taken in the event of a data breach. For health care providers, these steps include updates to their anti-malware software and firewalls, restricted access to networked devices, and communication and report protocols to alert medical device manufacturers about potential cybersecurity issues.

Medical device security is an evolving and complex issue for the health care sector and patients. Patients rely on these devices for their life-saving technologies and removal of the device can present significant health risks to the individual. However, through careful consideration of the cybersecurity risks during the design phase and implementation of protocols to manage these issues, manufacturers can reduce the vulnerability in their medical devices and increase safety for patients.