PUBLICATION

FDA's Cybersecurity Alert Puts Medical Device Users on Notice

August 14, 2015

On July 31, 2015, the United States Food and Drug Administration (FDA) issued a cybersecurity alert to health care facilities currently using certain infusion pumps manufactured by Hospira, Inc. The alert warns health care facilities about security vulnerabilities in Hospira's Symbiq Infusion System (Version 3.13 and prior) that could allow unauthorized access to the device and interfere with the device's proper functioning. The Hospira device communicates with a health care facility's network and information systems to control dosage delivery. According to the alert, an unauthorized user could potentially access the Hospira device remotely and alter the dosage it delivers, which could lead to over- or under-infusion of critical patient treatments. The FDA strongly encourages health care facilities to transition to alternative infusion systems and discontinue use of this particular Hospira infusion pump.

Although the FDA and Hospira are currently not aware of any patient adverse events or unauthorized device access related to the vulnerabilities in the Hospira Symbiq Infusion Pump in a health care facility, Hospira is working with customers to transition to alternative systems. Hospira no longer manufactures and distributes the Symbiq Infusion System, but the devices are still available for purchase from third-party medical supply companies. The FDA advises health care facilities to avoid purchasing the devices from such third parties.

Other Hospira infusion pump systems, including the LifeCare PCA3 and PCA5 Infusion Pump Systems, reportedly contain similar vulnerabilities. The FDA did not address these other Hospira devices in its most recent cybersecurity alert and has not recommended their use be discontinued; however, the FDA did warn of similar security vulnerabilities in these devices in an alert issued on May 13, 2015. Thus, health care facilities using the devices mentioned in the May alert should also seriously consider transitioning to other infusion pump systems and should exercise caution when selecting replacement devices.

An independent researcher identified and released information about the vulnerabilities in the Hospira device, which was later confirmed by Hospira and the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team. The Hospira device can be accessed remotely through a health care facility's network by using either a wired or wireless network connection. Therefore, physical access to a health care facility is not necessary to exploit these vulnerabilities.

This is the first time the FDA has recommended discontinuing use of a specific medical device based on cybersecurity concerns. The fact that the FDA issued a device-specific cybersecurity alert indicates both the seriousness of the vulnerabilities in the Hospira devices and the FDA's seriousness in addressing cybersecurity issues. The security vulnerabilities in the Hospira devices could be life threatening if exploited by a person with malicious intent. Because of the serious threat to patient safety presented by these security vulnerabilities and the FDA's willingness to issue device-specific warnings, medical device manufacturers should also heed the FDA's warning.

Health care facilities and providers should also take the FDA's warning seriously because a medical device cyberattack that results in harm to a patient would almost certainly cause reputational harm and have adverse legal and financial consequences. Thus, health care facilities and providers should seriously consider medical device issues in their HIPAA compliance programs. Information security officers should take action to ensure

they have physical, technical and administrative safeguards in place to protect against these types of threats. Examples of recommended actions to take to protect against such threats include, but are not limited to:

- Obtaining a thorough understanding of the medical devices that connect to the computer systems and anticipating potential threats and vulnerabilities
- Creating policies, procedures and contingency plans for preventing or minimizing damage from cyberattacks and maintaining critical functionality
- Creating policies and procedures for securely integrating medical devices into a health care facility's electronic infrastructure, as well as securely removing such devices
- Employing good design practices that include network segmentation, properly configured firewalls and monitoring traffic among systems and devices within your organization for unauthorized use
- Conducting regular risk assessments of your organization's networks and information systems, including medical devices
- Disabling wireless connectivity for as many devices as possible
- Restricting unauthorized access to your organization's networks and network-connected medical devices
- Keeping software, firmware and operating systems up-to-date on all systems and devices
- Closing all unnecessary ports and disabling all unnecessary services
- Contacting the device manufacturer if you think you have a cybersecurity problem with a medical device
- Conducting employee cybersecurity training

If you have a Hospira infusion system containing the above-mentioned security vulnerabilities, consider taking the following actions to reduce the risk of unauthorized access while transitioning to an alternative infusion system:

- Disconnect the device from the network
  - **CAUTION: Disconnecting the device from the network will impact operations and will require drug libraries to be updated manually, which can be labor intensive and prone to entry error.**
- Ensure that all unnecessary ports are closed, including port 20 (FTP) and port 23 (telnet)
- Monitor all network traffic attempting to reach the device via port 20 (FTP), port 23 (telnet) and port 8443
- Contact Hospira's technical support to change the default password used to access port 8443 or close port 8443

On a separate, but related note, information security officers are faced with a seemingly conflicting position recently issued by the Federal Communications Commission (FCC). The FCC voted to allow unlicensed devices to operate on the same frequency as wireless medical monitoring devices. Examples of such unlicensed devices include garage door openers, cordless phones and Bluetooth devices. If operated in relatively close proximity to wireless medical monitoring devices, such unlicensed devices could potentially cause interference with wireless monitoring and prevent doctors and nurses from receiving vital information. This creates an interesting conundrum for information security officers when analyzing when to authorize medical-related wireless activity in a hospital or provider office.

For more information about how this FDA cybersecurity alert may affect your business, or related matters, contact the author of this alert, Bill O'Connor, or any members of the Firm's Privacy and Information Security Team.