U.S. Food and Drug Administration
Protecting and Promoting *Your* Health

Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication

Date Issued: May 13, 2015

Audience: Health care facilities using the Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems

Devices: Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems

Purpose:

The FDA is alerting users of the Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems to security vulnerabilities with these pumps.

Summary of Problem and Scope:

The Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems are computerized infusion pumps designed for the continuous delivery of anesthetic or therapeutic drugs. These systems can be programmed remotely through a health care facility's Ethernet or wireless network.

The FDA and Hospira have become aware of security vulnerabilities in Hospira's LifeCare PCA3 and PCA5 Infusion Pump Systems. An independent researcher has released information about these vulnerabilities, including software codes, which, if exploited, could allow an unauthorized user to interfere with the pump's functioning. An unauthorized user with malicious intent could access the pump remotely and modify the dosage it delivers, which could lead to over- or under-infusion of critical therapies.

The FDA is not aware of any patient adverse events or unauthorized device access related to these vulnerabilities.

Health care facilities can reduce the risk of unauthorized access by implementing the recommendations below.

Recommendations for Health Care Facilities:

- Follow the recommendations from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland in the May 13, 2015 Advisory **Hospira LifeCare PCA Infusion System Vulnerabilities (Update A) (https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01A)**. These recommendations include the following:
    - Close Port 20/FTP and Port 23/TELNET and any other unused ports on your LifeCare PCA3 and PCA5 Infusion Pump Systems.
    - Isolate the LifeCare PCA Infusion Pump System from your Internet and untrusted systems. If you must connect to a host network, ensure that the host network is isolated from the Internet.
    - Use interrogation techniques, such as an MD5 checksum of key files, to identify if there have been any unauthorized changes to your LifeCare PCA Infusion Pump System.
    - Maintain layered physical and logical security practices for environments operating medical devices.
    - Use good design practices that include network segmentation. Use properly configured firewalls to selectively control and monitor traffic passed among the systems within your organization.
- Perform a risk assessment by examining the specific clinical use of the Hospira LifeCare PCA Infusion Pump System in your organization's environment to identify any potential impacts of the identified vulnerabilities. Use this risk assessment to help determine whether to maintain wireless connectivity between the Hospira LifeCare PCA Infusion Pump System and an isolated portion of your network,

establish hard-wired connection between the system and your network, or to remove the system from the network.

CAUTION: Disconnecting the device will require drug libraries to be updated manually and data that is normally transmitted to MedNet from the device will not be available. Manual updates on each pump can be labor intensive and prone to entry error. If you adjust the drug-delivery settings on your Hopira LifeCare PCA Infusion Pump System manually, the FDA recommends that you verify the settings prior to starting an infusion.

- Look for and follow risk mitigation strategies outlined in an upcoming letter from Hospira to its customers. Customers can access the instructions and other risk mitigation measures via Hospira's **Advanced Knowledge Center (http://www.hospira.com/en/support_center/support_infusion_pumps_and_software/support_akc/)**.
- Follow the good cybersecurity hygiene practices outlined in the FDA Safety Communication **Cybersecurity for Medical Devices and Hospital Networks (/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm)**, posted in June 2013, including:
  - Restricting unauthorized access to the network and networked medical devices.
  - Making certain 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 cybersecurity problem related to a medical device. If you are unable to determine the manufacturer or cannot contact the manufacturer, the FDA and DHS ICS-CERT may be able to assist in vulnerability reporting and resolution.
  - Developing and evaluating strategies to maintain critical functionality during adverse conditions.

FDA Activities:

The FDA is actively investigating the situation based on current information and close engagement with Hospira and the Department of Homeland Security. As new information becomes available about patient risks and any additional steps users should take to secure these devices, the FDA will communicate publicly.

Reporting Problems to the FDA:

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. Please review the ICS-CERT Advisory listed in the "Other Resources" section below. If you are experiencing problems with your device as described in that advisory, we encourage you to 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.

Other Resources:

NCCIC/ICS-CERT Advisory (https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01A)

Contact Information:

For additional information or questions about the Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems, contact Hospira at 800-241-4002.

If you have questions about this communication, please contact the Division of Industry and Consumer Education (DICE) at DICE@FDA.HHS.GOV, 800-638-2041 or 301-796-7100.

More in Safety Communications (/MedicalDevices/Safety/AlertsandNotices/default.htm)

Information About Heparin (/MedicalDevices/Safety/AlertsandNotices/ucm135345.htm)