20 May 2015

Dear Valued Hospira Customer,

You may be aware of an advisory recently issued by the National Cybersecurity and Communications Integration Center / Industrial Control Systems Cyber Emergency Response Team (NCCIC / ICS-CERT) titled, "ICSA-15-125-01A Hospira LifeCare PCA Infusion System Vulnerabilities" and published 12 May 2015. The advisory details the public availability of information provided by third party security vulnerability scanners. It is important to note that identified vulnerabilities require the breach of the firewall of the Hospital Information System. Cybersecurity is an industry-wide concern; therefore, it is critical that Hospital Information Systems be kept as secure as possible in order to act as the first line of defense against tampering.

In October 2014, Hospira provided Hospira MedNet™ customers with Knowledge Base articles from our Advanced Knowledge Center, "Improving Security in Hospira MedNet™ 5.5" and "Improving Security in Hospira MedNet™ 5.8", which were prepared to assist Hospira customers with deployment and use of Hospira products. These articles can be obtained by logging in to Hospira's Advanced Knowledge Center portal, https://selfservice.hospira.com/HeatWebUI/hssiHSS.jsp. Hospira is providing this communication to PCA customers as a follow up to the communication provided to Hospira MedNet customers in October 2014.

Hospira is not aware of any instances of cybersecurity breaches of Hospira devices in a clinical setting. In the unlikely event that someone is able to gain unauthorized access to the device, the pump is designed to ensure only a clinician can start, stop or change an infusion through physical interaction with the pump. It is not possible to remotely operate the LifeCare PCA Infusion Pump.

As an added layer of security to protect against these vulnerabilities, Hospira recommends closing the Telnet and FTP ports, ports 23 and 20, respectively. For assistance in closing these ports and to determine the configuration of LifeCare PCA Infusion Pumps, please call the Hospira Advanced Knowledge Center at 1-800-241-4002, option 4.

Hospira remains committed to developing new products and releasing product enhancements to support the needs of our customers. Hospira is actively working to identify additional ways to optimize security and is taking a systematic and long-term approach to cybersecurity. Hospira has put further cybersecurity protections in place in our next-generation LifeCare PCA device and software (LifeCare PCA version 7.0), which is undergoing U. S. FDA review. The release date for this new version has not been determined.

Hospira is available to assist you in determining if these protections are in place upon your request. For assistance, please call the Hospira Advanced Knowledge Center at 1-800-241-4002, option 4.

Sincerely,
June 2, 2015

Re: Hospira Plum Infusion Device Cybersecurity

Dear Valued Customer,

The technological demands placed on healthcare organizations have become increasingly sophisticated as wireless and network technologies are used in medical devices to provide connectivity at the point of care. The use of advanced technology in "smart" general infusion devices, like the Plum A+, is required to meet the clinical needs of patients today. In order to stay up to date with the most current IV medication safety limits, many Plum infusion devices with Hospira MedNet™ safety software communicate wirelessly over a hospital’s network. Accordingly, cybersecurity is a growing industry wide concern for all providers of device technology and must be continually monitored at the device and system level.

Recently, the National Cybersecurity and Communications Integration Center Industrial Control Systems Cyber Emergency Response Team (NCCIC/ICS-CERT) published an advisory regarding Hospira’s LifeCare PCA device. Hospira has published instructions on how to mitigate this potential threat to the LifeCare PCA and is working directly with our customers to resolve any concerns. Likewise, Hospira has reviewed the Plum Infusion platform to proactively assess the potential for a cybersecurity breach.

Although Hospira is not aware of any instances of a cybersecurity breach of a device in a clinical setting, our assessment identified additional steps to enhance the security of the Plum A+ on the hospital network. These steps include ensuring Telnet ports 23 and 2300, and FTP ports 20 and 21, are closed on the device. Closing these ports can typically be done remotely without intrusion to an organization’s daily practice. In certain circumstances, port closure must be performed manually at the pump.

For assistance in closing these ports, please call the Hospira Advanced Knowledge Center at (800) 241-4002, option 4. Please remember the Plum device is designed to ensure only a clinician can start or change an infusion through physical interaction with the device. It is not possible to initiate or modify an infusion remotely.

Hospira remains committed to developing new products and releasing product enhancements to support the needs of our customers. As part of that commitment within the rapidly changing healthcare industry, we continue to proactively work to identify additional ways to optimize the cybersecurity of our solutions.

Sincerely,

Hospira Worldwide, Inc.