Cyber Security and Medical Devices

May 22, 2017

Hospitals around the world have faced challenges as a result of the recent ransomware attack. The software that operates medical devices is one area of particular challenge. With the myriad devices that run on operating systems such as patient beds, blood pressure pumps, laboratory equipment and radiology equipment, the ability of hospitals to protect these devices from malicious attackers depends on the cooperation of the device manufacturers. IHA received reports from members that some device manufacturers will not or cannot update software to correct the security gap for older operating systems.

The Department of Health and Human Service (HHS) recently encouraged hospitals that have encountered manufacturers unresponsive to requests for upgrades to send specific vendor responses to CIP@HHS.gov.

- Use “Medical Device Manufacturer Refusal to Upgrade” as the subject line.
- Include in your email the name of the manufacturer, date of the request and details about the type of device.

While the Food and Drug Administration (FDA) cannot require manufacturers to upgrade their operating systems, the devices would not be de-certified if the manufacturer did so.

Medical Device Software Changes Differ from Other Operating Systems in a Number of Ways

- The lifecycle of an operating system and the support available is typically much shorter than the lifecycle of medical devices that rely upon those operating systems, especially large capital equipment. The vulnerability called “WannaCry” was patched by Microsoft in March for operating systems Microsoft continues to support. Older, but still functional, devices that are running on older operating systems may lack protection.
- The number of medical devices throughout the hospital as well as the acquisition point makes it difficult for hospitals to track. Medical devices are sometimes acquired as part of a clinical trial, some are acquired through a purchasing or supply chain process that does not include an inventory system monitored by or available to the information technology department, and some are acquired from individual departments.
- Updating, patching and replacing the thousands of devices used is costly, requires human capital and may require that devices are removed from use.
- Even with the financial resources to replace older devices, the replacement process takes time, from selection to purchase to implementation and integration.
- Medical devices are often interfaced with other software, such as the electronic medical record. Updating the operating system of a medical device may result in a necessary change to the interface.

What Can You Do If a Manufacturer Will Not or Cannot Protect Your Devices?

- Check manufacturer websites for information about their proposed solutions.
- Bring your information technology clinical applications team, supply chain leadership and lawyers together to evaluate opportunities to find solutions and negotiate fixes or replacement devices.
- Regularly follow information found online. The Department of Homeland Security issues alerts, such as listing product vendors who reported that they support products that use Microsoft Windows and have proactively issued customer notifications with recommendations for users. In addition, the FDA addresses steps medical device manufacturers and healthcare facilities to reduce the risk of cyberattacks. While the FDA and HHS are interested in hearing from hospitals about their cyberattacks, you should seek counsel on the pros and cons of sharing this information.
- Reach out to your group purchasing organization and ask it to advocate on behalf of you and its other participants.