Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software"

The Center for Devices and Radiological Health, FDA, has issued a **guidance document for manufacturers on cybersecurity (/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm)** of networked medical devices that use OTS software. We know that you are very interested in this issue, so we have prepared the following questions and answers to help you understand the guidance document.

What medical devices does this guidance cover?

This guidance covers medical devices that:

- use OTS software
- can connect to networks, such as a private intranet or the public Internet, and
- need updates or patches because their OTS software is found vulnerable to viruses, worms, and other threats.

Examples are

- systems that obtain, archive, and communicate pictures on networks within healthcare facilities, such as computed tomography (CT), magnetic resonance (MR), ultrasound (US), nuclear medicine (NM), and endoscopy
- systems that monitor patient activity, such as electrocardiographic (ECG) systems
- systems that communicate with clinical laboratory analyzers, such as laboratory information systems

Who is this guidance for?

FDA has addressed the guidance to manufacturers of medical devices. This guidance explains some of FDA's rules for manufacturers of medical devices that use OTS software and connect to networks. However, information in this guidance may be useful to others who are responsible for keeping networked devices safe from threats, such as

- suppliers of non-medical device network software and hardware, such as computers, routers, switches, operating systems, database engines
- healthcare organizations and their network administrators who set up and maintain computer networks connected to medical devices

Why is FDA concerned about security of networks?

FDA is concerned about the security of networks because vulnerable OTS software can allow an attacker to get unauthorized access to a network or medical device and reduce the safety and effectiveness of devices that connect to those networks.

What does this guidance cover?

The guidance covers major responsibilities of manufacturers of medical devices containing OTS software. These responsibilities are based on **FDA's Quality System regulation (/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/QualitySystemsRegulations/default.htm)**. FDA has already explained those responsibilities to manufacturers. (See FDA's guidance on **Off-The-Shelf Software Use In Medical Devices (ssLINK/ucm073778.htm)**.) We intend this guidance to help manufacturers better understand these responsibilities.

- If manufacturers chose to use OTS software in their devices and vulnerabilities in OTS software can affect the safety and effectiveness of their networked devices, they have to act to keep their devices safe and effective.
- FDA’s Quality System regulation requires medical device manufacturers to examine sources of quality data and correct or prevent quality problems.
- Ordinarily, FDA will not need to review software patches before a device manufacturer puts them in place. FDA views most software patches as design changes that manufacturers can make without prior discussion with FDA. FDA has already advised manufacturers on when they should involve FDA. (See FDA's guidances on **General Principles of Software Validation (/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM085371.pdf)** and **Deciding When to Submit a 510(k) for a Change to an Existing Device (/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm080235.htm)** and regulations on notification and premarket approval application **supplements (http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?FR=814.39)** and **reports (http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?**

fr=814.84).)

For example, manufacturers need to seek FDA's approval or clearance before installing a software patch if

  - it would change who it’s for, what it does, or how it works (a change in the indication for use), and/or
  - it would make the device less safe and effective

- Manufacturers must validate their software changes under the Quality System regulation. This means they have to look at what the change does, have evidence that the changed software meets user needs and consistently does what it is supposed to. (See "**Software validation. . . ." under FDA's guidance on General Principles of Software Validation (ssLINK/ucm085281.htm#_toc517237938)**.)
- Although manufacturers rarely need to ask FDA for approval for their patches, as part of quality control, they should have a plan for how to make these changes and follow it.

When can healthcare organizations apply software patches to medical devices that don't come from the medical device manufacturer?

In our view, it is rare for healthcare organizations to have enough technical resources and information on the design of medical devices to independently maintain medical device software. Thus, most healthcare organizations need to rely on the advice of medical device manufacturers.

What is my role in solving this problem?

Now that you are aware of the manufacturers’ responsibilities, work with them and with your institution to devise and implement a plan for dealing with potential cybersecurity vulnerabilities in your institution.

If you have questions concerning this document, contact John F. Murray Jr. 301-796-5543, john.murray@fda.hhs.gov (mailto:john.murray@fda.hhs.gov).

More in Guidance Documents (Medical Devices and Radiation-Emitting Products) (/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/default.htm)

Cross-Center Final Guidance (/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm081752.htm)

Office of Compliance Final Guidance (/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070269.htm)

Office of the Center Director Final Guidance (/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm110228.htm)

Office of Communication and Education Final Guidance
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070271.htm)

Office of Device Evaluation Final Guidance 2010 - 2016
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm198577.htm)

Office of Device Evaluation Final Guidance 1998 - 2009
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070272.htm)

Office of Device Evaluation Final Guidance 1976 - 1997
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm080283.htm)

Office of In Vitro Diagnostics and Radiological Health Final Guidance
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070274.htm)

Office of Surveillance and Biometrics Final Guidance
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070275.htm)

Office of Science and Engineering Laboratories Final Guidance
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070277.htm)

Draft Guidance
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm407274.htm)

Radiation-Emitting Products Guidance
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm283507.htm)

Withdrawn Guidance
(/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm425025.htm)