U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
FDA.GOV

U.S. FOOD & DRUG ADMINISTRATION

FDA FACT SHEET

THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY

Dispelling Myths and Understanding Facts

As medical devices become more digitally interconnected and interoperable, they can improve the care patients receive and create efficiencies in the health care system. Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage emerging cybersecurity risks, manufacturers can reduce cybersecurity risks posed to devices and patients.

The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product life-cycle, and incentivize changing marketed and distributed medical devices to reduce risk. Even with these guidances, the FDA continues to address myths about medical device cybersecurity.

Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.
Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.	The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.
The FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities.	The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.
Companies that manufacture off-the-shelf (OTS) software used in medical devices are responsible for validating its secure use in medical devices.	The medical device manufacturer chooses to use OTS software, thus bearing responsibility for the security as well as the safe and effective performance of the medical device.

The FDA encourages medical device manufacturers to address cybersecurity risks to keep patients safe and better protect the public health. This includes monitoring, identifying, and addressing cybersecurity vulnerabilities in medical devices once they are on the market. Working collaboratively with industry and other federal government agencies, the FDA continues its efforts to ensure the safety and effectiveness of medical devices, at all stages in their lifecycle, in the face of potential cyber threats. Learn more about medical device cybersecurity on www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.

Medical device cybersecurity is part of the FDA's broader digital health technology platform. To learn more about the FDA's efforts to advance digital health technology visit http://www.fda.gov/MedicalDevices/DigitalHealth/default.htm, or email digitalhealth@fda.hhs.gov.