Release

The U.S. Food and Drug Administration today issued a draft guidance outlining important steps medical device manufacturers should take to continually address cybersecurity risks to keep patients safe and better protect the public health. The draft guidance details the agency's recommendations for monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they have entered the market. The draft guidance is part of the FDA's ongoing efforts to ensure the safety and effectiveness of medical devices, at all stages in their lifecycle, in the face of potential cyber threats.

Cybersecurity threats to medical devices are a growing concern. The exploitation of cybersecurity vulnerabilities presents a potential risk to the safety and effectiveness of medical devices. While manufacturers can incorporate controls in the design of a product to help prevent these risks, it is essential that manufacturers also consider improvements during maintenance of devices, as the evolving nature of cyber threats means risks may arise throughout a device's entire lifecycle.

"All medical devices that use software and are connected to hospital and health care organizations' networks have vulnerabilities—some we can proactively protect against, while others require vigilant monitoring and timely remediation," said Suzanne Schwartz, M.D., M.B.A., associate director for science and strategic partnerships and acting director of emergency preparedness/operations and medical countermeasures in the FDA's Center for Devices and Radiological Health. "Today's draft guidance will build on the FDA's existing efforts to safeguard patients from cyber threats by recommending medical device manufacturers continue to monitor and address cybersecurity issues while their product is on the market."

Today's draft guidance outlines postmarket recommendations for medical device manufacturers, including the need to proactively plan for and to assess cybersecurity vulnerabilities—consistent with the FDA's Quality System Regulation. It also addresses the importance of information sharing via participation in an Information Sharing Analysis Organization (ISAO), a collaborative group in which public and private-sector members share cybersecurity information. The draft guidance recommends that manufacturers should implement a structured and systematic comprehensive cybersecurity risk management program and respond in a timely fashion to identified vulnerabilities. Critical components of such a program should include:

- Applying the 2014 NIST voluntary Framework for Improving Critical Infrastructure Cybersecurity, which includes the core principles of "Identify, Protect, Detect, Respond and Recover;"
- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

For the majority of cases, actions taken by manufacturers to address cybersecurity vulnerabilities and exploits are considered "cybersecurity routine updates or patches," for which the FDA does not require advance notification, additional premarket review or reporting under its regulations. For a small subset of cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death, the FDA would require medical device manufacturers to notify the agency.

The draft guidance indicates that in cases where the vulnerability is quickly addressed in a way that sufficiently reduces the risk of harm to patients, the FDA does not intend to enforce urgent reporting of the vulnerability to the agency if certain conditions are met. These conditions include: there are no serious adverse events or deaths associated with the vulnerability; within 30 days of learning of the vulnerability, the manufacturer notifies users and implements changes that reduce the risk to an acceptable level; and the manufacturer is a participating member of an ISAO and reports the vulnerability, its assessment and remediation to the ISAO.

“The FDA is encouraging medical device manufacturers to take a proactive approach to cybersecurity management of their medical devices,” said Schwartz. “Only when we work collaboratively and openly in a trusted environment, will we be able to best protect patient safety and stay ahead of cybersecurity threats.”

The FDA encourages public comments on the draft guidance, which will be open for 90 days. The FDA will also discuss the guidance at its upcoming public workshop, “Moving Forward: Collaborative Approaches to Medical Device Cybersecurity,” January 20-21 at the FDA’s headquarters in Silver Spring, Maryland. The workshop will engage the multi-stakeholder community in focused discussions on unresolved gaps and challenges that have hampered progress in advancing medical device cybersecurity and identify specific solutions to addressing these issues moving forward.

The FDA has been actively working to improve cybersecurity information sharing and to collaboratively develop and implement risk-based standards since 2013, when the White House issued Executive Order 13636 and Presidential Policy Directive 21 to mobilize the public and private sectors to collectively strengthen critical cybersecurity infrastructure. In October 2014, the FDA finalized its guidancecontaining recommendations for incorporating premarket management of cybersecurity during the design stage of device development. Other activities have included establishing formal partnerships with the Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team and the National Health Information Sharing and Analysis Center; providing input on the NIST voluntary cybersecurity framework; holding in-person meetings with stakeholders, including a 2014 FDA public workshop; and issuing product-specific safety communications on medical device cybersecurity vulnerabilities.

The FDA, an agency within the U.S. Department of Health and Human Services, protects the public health by assuring the safety, effectiveness, and security of human and veterinary drugs, vaccines and other biological products for human use, and medical devices. The agency also is responsible for the safety and security of our nation’s food supply, cosmetics, dietary supplements, products that give off electronic radiation, and for regulating tobacco products.