FDA Issues Guidance on December 28, 2016 for Postmarket Management of Cybersecurity in Medical Devices

Privacy, Technology and Data Security December 28, 2016

The Food and Drug Administration (FDA) is issuing this guidance to inform industry and FDA staff of the Agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices. In addition to the specific recommendations contained in this guidance, manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device[1]. A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to health and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the overall risk to health.

This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. This guidance establishes a risk-based framework for assessing when changes to medical devices for cybersecurity vulnerabilities require reporting to the Agency and outlines circumstances in which FDA does not intend to enforce reporting requirements under 21 CFR part 806. 21 CFR part 806 requires device manufacturers or importers to report promptly to FDA certain actions concerning device corrections and removals. However, the majority of actions taken by manufacturers to address cybersecurity vulnerabilities and exploits, referred to as "cybersecurity routine updates and patches," are generally considered to be a type of device enhancement[2] for which the FDA does not require advance notification or reporting under 21 CFR part 806. For a small subset of actions taken by manufacturers to correct device cybersecurity vulnerabilities and exploits that may pose a risk to health, the FDA would require medical device manufacturers to notify the Agency.[3] Risks to health posed by the device may result in patient harm. This guidance recommends how to assess whether the risk[4] of patient harm is sufficiently controlled or uncontrolled. This assessment is based on an evaluation of the likelihood of exploit, the impact of exploitation on the device's safety and essential performance,[5] and the severity of patient harm if exploited.

http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf

[1] See FDA Guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190)

[2] See FDA Guidance titled: "distinguishing Medical Device Recalls from Medical Device Enhancements" (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationsandGuidance/GuidanceDocuments/UCM418469.pdf).

[3] See 21 CFR 806.10.

[4] ANSI/AAMI/ISO 14971: 2007®2010: *Medical Devices – Application of Risk Management to Medical Devices,* section 2.16 – definition of risk.

[5] ANSI/AAMI ES60601-1:2005/®2012 and A1:2012, C1:2009/®2012 and A2:2010/®2012 (Consolidated Text) *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance* (IEC 60601-

1:12005, MOD), section 3.27 defines “Essential Performance” as performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk.

For additional information contact Mike Cassidy.