EMBARGOED UNTIL THURSDAY, JUNE 13, 2013 AT 9 AM EST

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

---

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.
Document issued on: [use release date of FR Notice]

You should submit comments and suggestions regarding this draft document within **[insert]** days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Submit electronic comments to http://www.regulations.gov. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this document, contact Abiy Desta (CDRH) at 301-796-0293 or by email at abiy.desta@fda.hhs.gov, or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 301-827-1800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

Preface

Additional Copies

Additional copies are available from the Internet. You may also send an e-mail request to dsmica@fda.hhs.gov to receive an electronic copy of the guidance or send a fax request to 301-847-8149 to receive a hard copy. Please use the document number 1825 to identify the guidance you are requesting.

Additional copies of this guidance document are also available from the Center for Biologics Evaluation and Research (CBER) by written request, Office of Communication, Outreach and Development (HFM-40), 1401 Rockville Pike, Suite 200N, Rockville, MD 20852-1448, by telephone, 1-800-835-4709 or 301-827-1800, by email, ocod@fda.hhs.gov, or from the Internet at http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/default.htm.

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

---

Draft Guidance for Industry and Food and Drug Administration Staff

This draft guidance, when finalized, will represent the Food and Drug Administration's (FDA's) current thinking on this topic. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. You can use an alternative approach if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach, contact the FDA staff responsible for implementing this guidance. If you cannot identify the appropriate FDA staff, call the appropriate number listed on the title page of this guidance.

1. Introduction

This guidance has been developed by the FDA to assist industry by identifying issues related to cybersecurity that manufacturers should consider in preparing premarket submissions for medical devices. The need for effective cybersecurity to assure medical device functionality has become more important with the increasing use of wireless, Internet- and network-connected devices, and the frequent electronic exchange of medical device-related health information. The recommendations contained in this guidance document are intended to supplement FDA's "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm) and "Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software" (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm).

FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

2. Scope

This guidance provides recommendations to consider and document in FDA medical device premarket submissions to provide effective cybersecurity management and to reduce the risk that device functionality is intentionally or unintentionally compromised. For the purposes of this document, cybersecurity is defined as the process of preventing unauthorized modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.

This guidance document applies to the following premarket submissions for devices that contain software (including firmware) or programmable logic[1]:

- Premarket Notification (510(k)) including Traditional, Special, and Abbreviated 510(k) submissions
- *De novo* petitions
- Premarket Approval Applications (PMA)
- Product Development Protocols (PDP)
- Humanitarian Device Exemption (HDE) submissions.

3. General Principles

Manufacturers should develop a set of security controls to assure medical device cybersecurity to maintain information **confidentiality, integrity,** and **availability**.

Confidentiality means that data, information, or system structures are accessible only to authorized persons and entities and are processed at authorized times and in the authorized manner, thereby helping ensure data and system security. Confidentiality provides the assurance that no unauthorized users (i.e., only trusted users) have access to the data, information, or system structures.

Integrity means that data and information are accurate and complete and have not been improperly modified.

Availability means that data, information, and information systems are accessible and usable on a timely basis in the expected manner (i.e., the assurance that the information will be available when needed).

[1] Manufacturers may also consider applying the cybersecurity principles described in this guidance as appropriate to Investigational Device Exemption submissions and to devices exempt from premarket review.

Failure to maintain cybersecurity can result in compromised device functionality, loss of data availability or integrity, or exposure of other connected devices or networks to security threats. These, in turn, have the potential to result in patient illness, injury, or death.

Manufacturers should consider cybersecurity during the design phase of the medical device, as this can result in more robust and efficient mitigation of cybersecurity risks. Manufacturers should define and document the following components of their cybersecurity risk analysis and management plan as part of the risk analysis required by 21 CFR 820.30(g)[2]:

- Identification of assets, threats, and vulnerabilities;
- Impact assessment of the threats and vulnerabilities on device functionality;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Residual risk assessment and risk acceptance criteria.

4. Security Capabilities

The extent to which security controls are needed will depend on the medical device, its environment of use, the type and probability of the risks to which it is exposed, and the probable risks to patients from a security breach. Medical devices capable of connecting to another medical device, to the Internet or other network, or to portable media (e.g. USB or CD) are more vulnerable to cybersecurity threats than devices that are not connected.

Manufacturers should also carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment of use (e.g., home use vs. health care facility use) to ensure that the security capabilities are appropriate for the intended users. For example, security controls should not hinder access to the device during an emergency situation. Similarly, manufacturers should consider how security features may interfere with the ability of healthcare providers to administer the necessary care.

The Agency recommends that medical device manufacturers provide justification in the premarket submission for the security features chosen and consider appropriate security control methods for their medical devices including, but not limited to, the following:

Limit Access to Trusted Users Only

- Limit access to devices through the authentication[3] of users (e.g., user ID and password, smartcard, biometric);
- Use automatic timed user session log-offs appropriate for the use environment;

[2] Manufacturers may elect to provide an alternative method or approach, with appropriate justification.
[3] Authentication is the act of verifying the identity of a user, process, or device as a prerequisite to allowing access to the device, its data, information, or systems.

- Employ a layered authorization[4] model by differentiating privileges based on the user role (e.g., caregiver, administrator);
- Use multi-factor authentication to permit privileged device access (e.g., to administrators, service technicians, maintenance personnel);
- Strengthen password protection by avoiding "hardcoded" passwords (i.e., passwords which are the same for each device, difficult to change, and vulnerable to public disclosure) and limit public access to passwords used for privileged device access;
- Where appropriate, provide physical locks on devices and their communication ports to minimize tampering;
- Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.

Ensure Trusted Content

- Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification;
- Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer;
- Ensure secure data transfer to and from the device, and when appropriate, use accepted methods for encryption[5].

Use Fail Safe and Recovery Features

- Implement fail-safe device features that protect the device's critical functionality, even when the device's security has been compromised;
- Implement features that allow for security compromises to be recognized, logged, and acted upon;
- Provide methods for retention and recovery of device configuration by an authenticated system administrator.

5. Cybersecurity Documentation

The type of documentation that we recommend you submit in your premarket submission is summarized in this section. These recommendations are predicated on your effective implementation and management of the quality system in accordance with the Quality System Regulation, including Design Controls.[6]

[4] Authorization is the right or a permission that is granted to access a device resource.
[5] Encryption is the cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used.
[6] 21 CFR Part 820 – Quality Systems Regulations: 21 CFR 820.30 Subpart C – Design Controls of the Quality System Regulation.

206
207 In the premarket submission, manufacturers should provide the following information related
208 to the cybersecurity of their medical device:
209
210 1. Hazard analysis, mitigations, and design considerations pertaining to intentional and
211 unintentional cybersecurity risks associated with your device, including:
212 • A specific list of all cybersecurity risks that were considered in the design of
213 your device;
214 • A specific list and justification for all cybersecurity controls that were
215 established for your device.
216
217 2. A traceability matrix that links your actual cybersecurity controls to the cybersecurity
218 risks that were considered;
219
220 3. To assure continued safe and effective device use, the systematic plan for providing
221 validated updates and patches to operating systems or medical device software, as
222 needed, to provide up-to-date protection and to address the product life-cycle;
223
224 4. Appropriate documentation to demonstrate that the device will be provided to
225 purchasers and users free of malware; and
226
227 5. Device instructions for use and product specifications related to recommended anti-
228 virus software and/or firewall use appropriate for the environment of use, even when it
229 is anticipated that users may use their own virus protection software.
230
231

232