Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

---

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

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

Public Comment

You may submit electronic comments and suggestions at any time for Agency consideration to http://www.regulations.gov. Submit written comments to the Division of Dockets Management, Food and Drug Administration, 5630 Fishers Lane, rm. 1061, (HFA-305), Rockville, MD, 20852. Identify all comments with the docket number FDA-2013-D-0616-0001[. Comments may not be acted upon by the Agency until the document is next revised or updated.

Additional Copies

Additional copies are available from the Internet. You may also send an e-mail request to CDRH-Guidance@fda.hhs.gov to receive a copy of the guidance. 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 10903 New Hampshire Avenue, Bldg. 71, Rm. 3128, Silver Spring, MD 20993-0002, by telephone, 1-800-835-4709 or 240-402-7800, 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

---

Guidance for Industry and Food and Drug Administration Staff

This guidance represents 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

The need for effective cybersecurity to assure medical device functionality and safety 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. This guidance has been developed by the FDA to assist industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices. 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 information to include in FDA medical device premarket submissions for effective cybersecurity management. Effective cybersecurity management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity.

This guidance document is applicable to the following premarket submissions for devices that contain software (including firmware) or programmable logic as well as software that is a medical device:[1]

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

3. Definitions

Asset[2] - is anything that has value to an individual or an organization.

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.

Authorization - is the right or a permission that is granted to access a device resource.

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

Confidentiality – data, information, or system structures are accessible only to authorized persons and entities and are processed at authorized times and in the authorized manner,

[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.
[2] As defined in ISO/ICE 27032:2012(E) Information technology — Security techniques — Guidelines for cybersecurity.

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.

Cybersecurity - is the process of preventing unauthorized access, 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.

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.

Harm[3] - is defined as physical injury or damage to the health of people, or damage to property or the environment.

Integrity – in this document means that data, information and software are accurate and complete and have not been improperly modified.

Life-cycle[2] – all phases in the life of a medical device, from initial conception to final decommissioning and disposal.

Malware - is software designed with malicious intent to disrupt normal function, gather sensitive information, and/or access other connected systems.

Privileged User[3] - is a user who is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Risk[2] – is the combination of the probability of occurrence of harm and the severity of that harm.

Risk Analysis[2] – is the systematic use of available information to identify hazards and to estimate the risk.

4. General Principles

Manufacturers should develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety.

FDA recognizes that medical device security is a shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices. Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or networks to security threats. This in turn may have the potential to result in patient illness, injury, or death.

[3] As defined in ANSI/AAMI/ISO 14971:2007 Medical devices – Application of risk management to medical devices.

Manufacturers should address cybersecurity during the design and development of the medical device, as this can result in more robust and efficient mitigation of patient risks. Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g).[4] The approach should appropriately address the following elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

5. Cybersecurity Functions

The Agency recommends that medical device manufacturers consider the following cybersecurity framework core functions to guide their cybersecurity activities: Identify, Protect, Detect, Respond, and Recover.[5]

Identify and Protect

Medical devices capable of connecting (wirelessly or hard-wired) to another 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. The extent to which security controls are needed will depend on the device's intended use, the presence and intent of its electronic data interfaces, its intended environment of use, the type of cybersecurity vulnerabilities present, the likelihood the vulnerability will be exploited (either intentionally or unintentionally), and the probable risk of patient harm due to a cybersecurity breach.

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 controls are appropriate for the intended users. For example, security controls should not unreasonably hinder access to a device intended to be used during an emergency situation.

The Agency recommends that medical device manufacturers provide justification in the premarket submission for the security functions chosen for their medical devices.

[4] 21 CFR Part 820 – Quality Systems Regulations: 21 CFR 820.30 Subpart C – Design Controls of the Quality System Regulation.

[5] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Examples of security functions to consider for protection of medical devices should include, but should not be limited to, the following:

Limit Access to Trusted Users Only

- Limit access to devices through the authentication of users (e.g. user ID and password, smartcard, biometric);
- Use automatic timed methods to terminate sessions within the system where appropriate for the use environment;
- Where appropriate, employ a layered authorization model by differentiating privileges based on the user role (e.g. caregiver, system administrator) or device role;
- Use appropriate authentication (e.g. multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel);
- Strengthen password protection by avoiding "hardcoded" password or common words (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 capability of secure data transfer to and from the device, and when appropriate, use methods for encryption.

Detect, Respond, Recover

- Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use;
- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event;
- Implement device features that protect critical functionality, even when the device's cybersecurity has been compromised;
- Provide methods for retention and recovery of device configuration by an authenticated privileged user.

Manufacturers may elect to provide an alternative method or approach, with appropriate justification.

6. Cybersecurity Documentation

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

In the premarket submission, manufacturers should provide the following information related to the cybersecurity of their medical device:

1. Hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device, including:
   - A specific list of all cybersecurity risks that were considered in the design of your device;
   - A specific list and justification for all cybersecurity controls that were established for your device.

2. A traceability matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered;

3. A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness. The FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity.

4. A summary describing controls that are in place to assure that the medical device software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer; and

5. Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g. anti-virus software, use of firewall).

7. Recognized Standards

The following is a list of FDA recognized consensus standards dealing with Information Technology (IT) and medical device security.

1. CLSI, AUTO11-A - IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard.
2. IEC, TR 80001-2-2 Edition 1.0 2012-07 - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.
3. AAMI/ANSI/IEC, TIR 80001-2-2:2012, - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.
4. IEC, /TS 62443-1-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.
5. IEC, 62443-2-1 Edition 1.0 2010-11 - Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
6. IEC, /TR 62443-3-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems.

For an updated list of FDA recognized consensus standards the Agency recommends that you refer to the FDA Recognized Consensus Standards Database (http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm), and type "security" in the title search for the current list of IT and medical device security consensus standards that are recognized by the Agency. For information on recognized consensus standards, see the guidance document "Frequently Asked Questions on Recognition of Consensus Standards" (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm074973.htm).