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Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.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: June 14, 2013

You should submit comments and suggestions regarding this draft document within **90** days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance.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

38

Preface

40

Additional Copies

42

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.

47

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/de
fault.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Draft Guidance for Industry and Food and Drug Administration Staff

This draft guidance, when finalized, will represent the Food and Drug Administration's (FDA's) current thinking on this topic.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).

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

93 # 2. Scope

94
95 This guidance provides recommendations to consider and document in FDA medical
96 device premarket submissions to provide effective cybersecurity management and to
97 reduce the risk that device functionality is intentionally or unintentionally compromised.
98 For the purposes of this document, cybersecurity is defined as the process of preventing
99 unauthorized modification, misuse or denial of use, or the unauthorized use of
100 information that is stored, accessed, or transferred from a medical device to an external
101 recipient.

102
103 This guidance document applies to the following premarket submissions for devices that
104 contain software (including firmware) or programmable logic[1]:
105 - Premarket Notification (510(k)) including Traditional, Special, and Abbreviated
106 510(k) submissions
107 - *De novo* petitions
108 - Premarket Approval Applications (PMA)
109 - Product Development Protocols (PDP)
110 - Humanitarian Device Exemption (HDE) submissions.

111 # 3. General Principles

112
113 Manufacturers should develop a set of security controls to assure medical device
114 cybersecurity to maintain information **confidentiality, integrity,** and **availability**.

115
116 **Confidentiality** means that data, information, or system structures are accessible only to
117 authorized persons and entities and are processed at authorized times and in the authorized
118 manner, thereby helping ensure data and system security. Confidentiality provides the
119 assurance that no unauthorized users (i.e., only trusted users) have access to the data,
120 information, or system structures.

121
122 **Integrity** means that data and information are accurate and complete and have not been
123 improperly modified.

124
125 **Availability** means that data, information, and information systems are accessible and usable
126 on a timely basis in the expected manner (i.e., the assurance that the information will be
127 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.

128
129 Failure to maintain cybersecurity can result in compromised device functionality, loss of data
130 availability or integrity, or exposure of other connected devices or networks to security
131 threats. These, in turn, have the potential to result in patient illness, injury, or death.
132
133 Manufacturers should consider cybersecurity during the design phase of the medical device,
134 as this can result in more robust and efficient mitigation of cybersecurity risks.
135 Manufacturers should define and document the following components of their cybersecurity
136 risk analysis and management plan as part of the risk analysis required by 21 CFR
137 820.30(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.

138
139
140
141
142

4. Security Capabilities

143

144
145 The extent to which security controls are needed will depend on the medical device, its
146 environment of use, the type and probability of the risks to which it is exposed, and the
147 probable risks to patients from a security breach. Medical devices capable of connecting to
148 another medical device, to the Internet or other network, or to portable media (e.g. USB or
149 CD) are more vulnerable to cybersecurity threats than devices that are not connected.
150
151 Manufacturers should also carefully consider the balance between cybersecurity safeguards
152 and the usability of the device in its intended environment of use (e.g., home use vs. health
153 care facility use) to ensure that the security capabilities are appropriate for the intended users.
154 For example, security controls should not hinder access to the device during an emergency
155 situation. Similarly, manufacturers should consider how security features may interfere with
156 the ability of healthcare providers to administer the necessary care.
157
158 The Agency recommends that medical device manufacturers provide justification in the
159 premarket submission for the security features chosen and consider appropriate security
160 control methods for their medical devices including, but not limited to, the following:
161
162 **Limit Access to Trusted Users Only**
163

164 - Limit access to devices through the authentication[3] of users (e.g., user ID
165   and password, smartcard, biometric);
166 - Use automatic timed user session log-offs appropriate for the use
167   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.

168   • Employ a layered authorization[4] model by differentiating privileges based
169   on the user role (e.g., caregiver, administrator);
170   • Use multi-factor authentication to permit privileged device access (e.g., to
171   administrators, service technicians, maintenance personnel);
172   • Strengthen password protection by avoiding "hardcoded" passwords (i.e.,
173   passwords which are the same for each device, difficult to change, and
174   vulnerable to public disclosure) and limit public access to passwords used
175   for privileged device access;
176   • Where appropriate, provide physical locks on devices and their
177   communication ports to minimize tampering;
178   • Require user authentication or other appropriate controls before permitting
179   software or firmware updates, including those affecting the operating
180   system, applications, and anti-malware.
181

182 **Ensure Trusted Content**
183

184   • Restrict software or firmware updates to authenticated code. One
185   authentication method manufacturers may consider is code signature
186   verification;
187   • Use systematic procedures for authorized users to download version-
188   identifiable software and firmware from the manufacturer;
189   • Ensure secure data transfer to and from the device, and when appropriate,
190   use accepted methods for encryption[5].
191

192 **Use Fail Safe and Recovery Features**
193

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

5. Cybersecurity Documentation

200
201
202 The type of documentation that we recommend you submit in your premarket submission is
203 summarized in this section. These recommendations are predicated on your effective
204 implementation and management of the quality system in accordance with the Quality System
205 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.

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. To assure continued safe and effective device use, the systematic plan for providing validated updates and patches to operating systems or medical device software, as needed, to provide up-to-date protection and to address the product life-cycle;

4. Appropriate documentation to demonstrate that the device will be provided to purchasers and users free of malware; and

5. Device instructions for use and product specifications related to recommended anti-virus software and/or firewall use appropriate for the environment of use, even when it is anticipated that users may use their own virus protection software.