Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

---

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on October 18, 2018.

You should submit comments and suggestions regarding this draft document within 150 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions about this document, contact Suzanne Schwartz, Office of the Center Director at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Preface

Additional Copies

CDRH

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 GUD1825 to identify the guidance you are requesting.

CBER

Additional copies are available from the Center for Biologics Evaluation and Research (CBER), Office of Communication, Outreach, and Development (OCOD), 10903 New Hampshire Ave., Bldg. 71, Room 3128, Silver Spring, MD 20993-0002, or by calling 1-800-835-4709 or 240-402-8010, by email, ocod@fda.hhs.gov or from the Internet at https://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm.

Table of Contents

I. Introduction 4
II. Scope 5
III. Definitions 6
IV. General Principles & Risk Assessment 8
V. Designing a Trustworthy Device: Application of NIST Cybersecurity Framework 11
VI. Labeling Recommendations for Devices with Cybersecurity Risks 18
VII. Cybersecurity Documentation 21
VIII. Recognized Standards 24

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 current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

I. Introduction

The need for effective cybersecurity to ensure medical device functionality and safety has become more important with the increasing use of wireless, Internet- and network- connected devices, portable media (e.g. USB or CD), and the frequent electronic exchange of medical device-related health information. In addition, cybersecurity threats to the healthcare sector have become more frequent, more severe, and more clinically impactful. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the US and globally. Such cyberattacks and exploits can delay diagnoses and/or treatment and may lead to patient harm.

This guidance is intended to provide recommendations to industry regarding cybersecurity device design, labeling, and the documentation that FDA recommends be included in premarket submissions for devices with cybersecurity risk. These recommendations can facilitate an efficient premarket review process and help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats.

Although FDA issued final guidance addressing premarket expectations in 2014, the rapidly evolving landscape, and the increased understanding of the threats and their potential mitigations, necessitates an updated approach. This guidance has been developed by the FDA to assist industry by identifying issues related to cybersecurity that manufacturers should address 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"[1] and "Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software."[2] When finalized, this guidance will replace the final guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[3]

For the current edition of the FDA-recognized standard(s) referenced in this document, see the FDA Recognized Consensus Standards Database.[4]

FDA's guidance documents, including this draft 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 guidance means that something is suggested or recommended, but not required.

II. 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 decrease the risk of patient harm by reducing device exploitability which can result in intentional or unintentional compromise of device safety and essential performance.[5]

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 (collectively referred to as "software devices").[6]

- Premarket Notification (510(k)) submissions including Traditional, Special, and Abbreviated;
- De Novo requests;
- Premarket Approval Applications (PMAs);
- Product Development Protocols (PDPs); and

[1] https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM089593
[2] https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM077823
[3] https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190
[4] Available at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm
[5] ANSI/AAMI ES60601-1:2005/(R)2012 and A1:2012, C1:2009/(R)2012 and A2:2010/(R)2012 (Consolidated Text) Medical electrical equipment— Part 1: General requirements for basic safety and essential performance (IEC 60601-1:2005, 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."
[6] 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.

- Humanitarian Device Exemption (HDE) applications.

III. Definitions

The definitions listed here are for the purposes of this guidance and are intended for use in the context of assessing medical device cybersecurity.

Asset – anything that has value to an individual or an organization.[7]

Authentication – 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. [8]

Authenticity – the property of being genuine and being able to be verified and trusted; confidence that the contents of a message originates from the expected party and has not been modified during transmission or storage.[9]

Authorization – the right or a permission that is granted to access a device resource.[10]

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

Confidentiality – the property of data, information, or system structures to be 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.

Configuration – the possible conditions, parameters, and specifications with which a device or system component can be described or arranged.[11]

[7] As defined in ISO/IEC 27032 Information technology — Security techniques — Guidelines for cybersecurity.
[8] Adapted from NIST FIPS 200 Minimum Security Requirements for Federal Information and Information Systems: Authentication is defined as verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
[9] From NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations: Authenticity is defined as the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
[10] Adapted from NISTIR 7298 Glossary of Key Information Security Terms: Authorization is the access privileges granted to a user, program, or process or the act of granting those privileges.
[11] Adapted from NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems: Configuration is the possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.

Cryptographically strong - cryptographic algorithms, protocols and implementations that authoritative sources in cryptography would consider sufficiently secure.

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.

Cybersecurity Bill of Materials (CBOM) – a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities.

Denial of Service – actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.[12]

Encryption –the cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used.[13]

End of support – a point beyond which the product manufacturer ceases to provide support, which may include cybersecurity support, for a product or service.

Integrity – the property of data, information and software to be accurate and complete and have not been improperly modified.

Jitter – as it relates to queuing, the difference in latency of packets.[14]

Life-cycle – all phases in the life of a medical device, from initial conception to final decommissioning and disposal.[15]

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

Patchability/Updatability – the ease with which a device and related systems can be updated and patched in a timely manner.

[12] From NIST SP 800-24 PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does.
[13] From NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security. Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.
[14] From NIST SP 800-127 Guide to Securing WiMAX Wireless Communications.
[15] ANSI/AAMI/ISO 14971 Medical Devices – Application of Risk Management to Medical Devices

Patient harm – is defined as physical injury or damage to the health of patients, including death.[16] Cybersecurity exploits (e.g. loss of authenticity, availability, integrity, or confidentiality) of a device may pose a risk to health and may result in patient harm.

Privileged User – a user who is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.[17]

Quality of Service – the measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service Level Agreement between an end-user and a service provider, so as to satisfy specific customer application requirements.[18]

Risk – the combination of the probability of occurrence of harm and the severity of that harm.[19]

Risk Analysis – the systematic use of available information to identify hazards and to estimate the risk.[19]

Trustworthy Device –a medical device containing hardware, software, and/or programmable logic that: (1) is reasonably secure from cybersecurity intrusion and misuse; (2) provides a reasonable level of availability, reliability, and correct operation; (3) is reasonably suited to performing its intended functions; and (4) adheres to generally accepted security procedures.[20]

IV. General Principles & Risk Assessment

In order to demonstrate a reasonable assurance of safety and effectiveness for software devices, documentation related to the requirements of the Quality System Regulation (QSR) (21 CFR Part 820) is often a necessary part of the premarket submission. See also "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" (available at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf). As part of QSR design controls, a manufacturer must "establish and maintain procedures for validating the devices design," which "shall include software validation and risk analysis, where appropriate." 21 CFR 820.30(g).

As part of the software validation and risk analysis required by 21 CFR 820.30(g), software device manufacturers may need to establish a cybersecurity vulnerability and management approach, where appropriate. FDA recommends that this approach include a set of cybersecurity

[16] ANSI/AAMI/ISO 14971 Medical devices—Application of risk management to medical devices defines *"harm"* as the physical injury or damage to the health of people, or damage to property or the environment.
[17] From NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
[18] From CNSSI 4009 Committee on National Security Systems (CNSS) Glossary.
[19] ANSI/AAMI/ISO 14971 Medical Devices – Application of Risk Management to Medical Devices
[20] Adapted from NIST SP 800-32 Introduction to Public Key Technology and the Federal PKI Infrastructure which defines trustworthy system as Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

design controls to ensure medical device cybersecurity and maintain medical device safety and effectiveness. Such design controls may make it more likely that FDA will find your device meets its applicable statutory standard for premarket review.[21]

FDA recognizes that medical device security is a shared responsibility among stakeholders, including health care facilities, patients, health care providers, and manufacturers of medical devices. Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) authenticity, 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.

The recommendations in this guidance are intended to aid manufacturers to:

1) employ a risk-based approach to the design and development of medical devices with appropriate cybersecurity protections;
2) take a holistic approach to device cybersecurity by assessing risks and mitigations throughout the product's lifecycle;
3) ensure maintenance and continuity of critical device safety and essential performance[22]; and
4) promote the development of trustworthy devices to help ensure the continued safety and effectiveness of the devices.

The QSR requires that manufacturers of devices automated with computer software establish and maintain procedures to ensure that the design requirements relating to the device are appropriate and address the intended use of the device, including the needs of the user and patient. 21 CFR 820.30(c). FDA recommends that manufacturers consider the following elements as they address cybersecurity during the design and development of their medical device:

- 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[23] of a threat and of a vulnerability being exploited;
- determination of risk levels and suitable mitigation strategies; and
- assessment of residual risk and risk acceptance criteria.

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. Manufacturers should employ a risk-based approach when determining the design features and the level of cybersecurity resilience

[21] For more information about how FDA evaluates substantial equivalence in 510(k) submissions, see the FDA guidance document "The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)]

[22] Postmarket Management of Cybersecurity in Medical Devices https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[23] Likelihood assessments should leverage an analysis of exploitability not probability.

appropriate for a device. A Cybersecurity Bill of Materials (CBOM) can be a critical element in identifying assets, threats, and liabilities. Leveraging a CBOM may also support compliance with purchasing controls (21 CFR 820.50), by facilitating the establishment of requirements regarding cybersecurity for all purchased or otherwise received products. The extent to which security controls are needed will depend on the device's intended use, the presence and functionality of its electronic data interfaces, its intended environment of use, the type of cybersecurity vulnerabilities present, the exploitability of the vulnerability, either intentionally or unintentionally, and the probable risk of patient harm due to a cybersecurity breach.

For the purposes of this guidance, and to help clarify FDA's premarket cybersecurity recommendations, we are defining two "tiers" of devices according to their cybersecurity risk:

Tier 1 "Higher Cybersecurity Risk"

A device is a Tier 1 device if the following criteria are met:

1) The device is capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, or to a network, or to the Internet; AND

2) A cybersecurity incident affecting the device could directly result in patient harm to multiple patients.

Examples of Tier 1 devices, include but are not limited to, implantable cardioverter defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps, and the supporting connected systems that interact with these devices such as home monitors and those with command and control functionality such as programmers.

Tier 2 "Standard Cybersecurity Risk"

A medical device for which the criteria for a Tier 1 device are not met.

For this cybersecurity guidance only, FDA introduces the tiers of higher and standard cybersecurity risk to aid medical device manufacturers in the design of secure devices and aid in providing supporting documentation to FDA. We recognize that this cybersecurity risk tiering may not track to FDA's existing statutory device classifications. For example, based on the manufacturer's assessment and device design, a class II device such as an infusion pump, may meet the criteria for Tier 1 higher cybersecurity risk while a class III device, such as a coronary atherectomy device with no connectivity may meet the criteria for Tier 2 standard cybersecurity risk. The principles and approaches described in this guidance are broadly applicable to all medical devices and are intended to be consistent with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure

Cybersecurity to manage cybersecurity-related risks by focusing on core functions of identify, protect, detect, respond, and recover.[24]

V. Designing a Trustworthy Device: Application of NIST Cybersecurity Framework

As mentioned in Section IV, for software devices, documentation related to design controls, and specifically design validation and software validation and risk analysis in 21 CFR 820.30(g), is often necessary to provide a reasonable assurance of safety and effectiveness in a premarket submission. For devices with cybersecurity risks, we recommend that manufacturers design devices that are trustworthy because trustworthy devices may be more likely to meet their applicable statutory standard for premarket review and because trustworthy devices are more likely to remain safe and effective throughout their life-cycle. Trustworthy devices: (1) are reasonably secure from cybersecurity intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures. In addition, documentation demonstrating the trustworthiness of a device will help FDA more quickly and efficiently assess the device's safety and effectiveness with respect to cybersecurity.

This section describes the specific design features and cybersecurity design controls that the Agency believes should be included in the design of a trustworthy device. We recommend premarket submissions for Tier 1 devices with higher cybersecurity risk to include documentation demonstrating how the device design and risk assessment incorporate the cybersecurity design controls described below. For Tier 2 devices with standard cybersecurity risk, we recommend that manufacturers include documentation in their premarket submissions that either 1) demonstrates they have incorporated each of the specific design features and cybersecurity design controls described in this section, or 2) provide a risk-based rationale for why specific cybersecurity design controls, described in this section, are not appropriate. Risk-based rationales should leverage an analysis of exploitablity to describe likelihood instead of probability.

Submitted documentation may include the demonstration of comparable and/or additional cybersecurity design controls that may not be described in this document. Furthermore, as cybersecurity design controls are established early on during the development phase, we recommend industry utilize the FDA presubmission process to discuss design considerations for meeting adequacy of cybersecurity risk management throughout the device life-cycle.[25]

[24] National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, available at: https://www.nist.gov/cyberframework

[25]For more information, see FDA's guidance entitled "Request for Feedback on Medical Device Submissions: The Pre-Submission Program and Meetings with Food and Drug Administrative Staff" (https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm311176.pdf)

A. Identify and Protect Device Assets and Functionality

Manufacturers should design trustworthy devices and provide documentation to demonstrate the trustworthiness of their devices in premarket review. In particular, devices and systems should be designed to protect assets and functionality in order to reduce the risk of multi-patient harm due to the loss of authenticity, availability, integrity, and confidentiality. Specifically, protection mechanisms should prevent all unauthorized use (through all interfaces); ensure code, data, and execution integrity (subversion of system functionality/safety/security features); and as appropriate, protect confidentiality of data (insofar as its release could be leveraged to effect multi-patient harm. As a part of premarket submissions, manufacturers should submit documentation demonstrating how these design expectations are met.

1. Prevent Unauthorized Use

In order to reduce the risk of multi-patient harm due to the loss of authenticity, availability, integrity, and confidentiality, we have provided design recommendations with respect to authentication, authorization, and encryption in the section below. Authentication is used to prevent unauthorized access to device functions and to prevent unauthorized software execution. It provides the assurance that a communication and/or command is unmodified and originates from an authorized source, which, in conjunction with other controls that prevent replays, makes it more difficult for external adversaries to issue potentially harmful commands to a safety-critical system. Usually, authorization is only effective as a security control in conjunction with correctly implemented authentication. Except in circumstances when system design features intrinsically provide equivalent or stronger assurance, all devices should properly authenticate potentially harmful commands and/or data.

As a defensive measure, authorization enforces privileges associated with authentication credentials and/or roles to reject all disallowed behavior. That means that an adversary using a credential with lower privileges should not be able to access device resources or functionality that require higher privileges (i.e., the default device design should prevent this from occurring). Devices should have appropriate protections in place that prevent sensitive information from being read by unauthorized parties either in storage or in transmission. Encryption should be used as appropriate, since it protects sensitive information from unauthorized disclosure. The following outline provides recommended design implementations of authentication, authorization, and encryption:

(a) Limit Access to Trusted Users & Devices Only

(i) Limit access to devices through the authentication of users (e.g., user ID and password, smartcard, biometric).

(ii) Use automatic timed methods to terminate sessions within the system where appropriate for the use environment.

(iii) Employ a layered authorization model by differentiating privileges based on the user role (e.g., caregiver, patient, health care provider, system administrator) or device functions.

(iv) Use appropriate authentication (e.g., multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel).

(v) Strengthen password protection. Do not use credentials that are hardcoded, default, easily-guessed, easily compromised (i.e., passwords which are the same for each device; unchangeable; can persist as default; difficult to change; and vulnerable to public disclosure). Limit public access to passwords used for privileged device access.

(vi) Consider physical locks on devices and their communication ports to minimize tampering.

(b) **Authenticate and Check Authorization of Safety-Critical Commands**

(i) Use authentication to prevent unauthorized access to device functions and to prevent unauthorized (arbitrary) software execution.

(ii) Require user authentication before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.

(iii) Use cryptographically strong authentication resident on the device to authenticate personnel, messages, commands and as applicable, all other communication pathways.

(iv) Authenticate all external connections. For example, if a device connects to an offsite server, then it and the server

should mutually authenticate, even if the connection is initiated over one or more existing trusted channels.

(v) Authenticate firmware and software. Verify authentication tags (e.g., signatures, message authentication codes (MACs)) of software/firmware content, version numbers, and other metadata. The version numbers intended to be installed should themselves be signed/have MACs. Devices should be electronically identifiable (e.g., model number, serial number) to authorized users.

(vi) Perform authorization checks based on authentication credentials or other irrefutable evidence. For example, a medical device programmer should have elevated privileges that are granted based on cryptographic authentication or a signal of intent that cannot physically be produced by another device, e.g., a home monitor, with a software-based attack.

(vii) Devices should be designed to "deny by default," i.e., that which is not expressly permitted by a device is denied by default. For example, the device should generally reject all unauthorized connections (e.g., incoming TCP, USB, Bluetooth, serial connections).

(viii) The principle of least privilege should be applied to allow only the level of access necessary to perform a function.

2. Ensure Trusted Content by Maintaining Code, Data, and Execution Integrity

(a) Code Integrity

(i) Only allow installation of cryptographically verified firmware/software updates. Use cryptographically signed updates to help prevent unauthorized reduction in the level of protection (downgrade or rollback attacks) by ensuring

that the new update is more recent than the currently installed version.

(ii) Where feasible, ensure that the integrity of software is validated prior to execution, e.g., 'whitelisting' based on digital signatures.

(b) Data Integrity

(i) Verify the integrity of all incoming data (ensuring it is not modified in transit or at rest, and it is well-formed/compliant with the expected protocol/specification).

(ii) Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption and authentication of the end points with which data is being transferred.

(iii) Protect the integrity of data necessary to ensure the safety and essential performance of the device.

(iv) Use current NIST recommended standards for cryptography (e.g., FIPS 140-2, NIST[26] Suite B[27]), or equivalent-strength cryptographic protection for communications channels.

(v) Use unique per device cryptographically secure communication keys to prevent leveraging the knowledge of one key to access a multitude of devices.

(c) Execution Integrity

Where feasible, use industry-accepted best practices to maintain/verify integrity of code while it is being executed on the device.

3. Maintain Confidentiality of Data

Manufacturers should ensure the confidentiality of any/all data whose disclosure could lead to patient harm (e.g., through use of credentials, encryption). Loss of confidentiality of credentials could be used by a threat to effect multi-patient harm. Lack of encryption to protect sensitive information "at rest" and "in transit" can expose this information to misuse that can lead to patient harm.

[26] NIST FIPS 140-2 Cryptographic Module Validation Program available at: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards

[27] NIST FIPS 140-2 Suite B available at: https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2851.pdf

Other harms, such as loss of confidential protected health information (PHI), are not considered "patient harms" for the purposes of this guidance. Although protecting the confidentiality of PHI is beyond the scope of this document, it should be noted that manufacturers and/or other entities, depending on the facts and circumstances, may be obligated to protect the confidentiality, integrity and availability of PHI throughout the product lifecycle, in accordance with applicable federal and state laws, including the Health Information Portability and Accountability Act (HIPAA).[28]

B. Detect, Respond, Recover: Design Expectations

Proper device design can significantly reduce cybersecurity risk for the device while it is marketed and deployed in its use environment. Therefore, appropriate design should anticipate the need to detect and respond to dynamic cybersecurity risks, including the need for deployment of cybersecurity routine updates and patches as well as emergency workarounds. The following items articulate recommendations for the design of a trustworthy device as it pertains to the NIST core functions of detect, respond, and recover.

1. Design the Device to Detect Cybersecurity Events in a Timely Fashion

(a) Implement design features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use.

(b) Devices should be designed to permit routine security and antivirus scanning such that the safety and essential performance of the device is not impacted.

(c) Ensure the design enables forensic evidence capture. The design should include mechanisms to create and store log files for security events. Documentation should include how and where the log file is located, stored, recycled, archived, and how it could be consumed by automated analysis software (e.g. Intrusion Detection System, IDS). Examples of security events include but are not limited to configuration changes, network anomalies, login

[28] The HHS Office for Civil Rights enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information that covered entities or their business associates create, receive, maintain, or transmit; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. See Health Information Privacy at: http://www.hhs.gov/ocr/privacy/index.html.

attempts, and anomalous traffic (e.g., sending requests to unknown entities).

(d) The device design should limit the potential impact of vulnerabilities by specifying a secure configuration. Secure configurations may include endpoint protections such as anti-malware, firewall/firewall rules, whitelisting, defining security event parameters, logging parameters, physical security detection.

(e) The device design should enable software configuration management and permit tracking and control of software changes to be electronically obtainable (i.e., machine readable) by authorized users.

(f) The product life-cycle, including its design, should facilitate a variant analysis of a vulnerability across device models and product lines.

(g) The device design should provide a CBOM in a machine readable, electronic format to be consumed automatically.[29]

2. Design the Device to Respond to and contain the impact of a potential cybersecurity incident

[29] Recommendation 2.2 from the Health Care Industry and Cybersecurity Task Force (HCIC TF) Report on Improving Cybersecurity in the Health Care Industry available here: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

(a) The device should be designed to notify users upon detection of a potential cybersecurity breach.

(b) The device should be designed to anticipate the need for software patches and updates to address future cybersecurity vulnerabilities.

(c) The device should be designed to facilitate the rapid verification, validation, and testing of patches and updates.

(d) The design architecture should facilitate the rapid deployment of patches and updates.

3. Design the Device to Recover capabilities or services that were impaired due to a cybersecurity incident

(a) Implement device features that protect critical functionality and data, even when the device's cybersecurity has been compromised.

(b) The design should provide methods for retention and recovery of device configuration by an authenticated privileged user.

(c) The design should specify the level of autonomous functionality (resilience) any component of the system possesses when its communication capabilities with the rest of the system are disrupted including disruption of significant duration.

(d) Devices should be designed to be resilient to possible cybersecurity incident scenarios such as network outages, Denial of Service attacks, excessive bandwidth usage by other products, disrupted quality of service (QoS), and excessive jitter (i.e., a variation in the delay of received packets).

VI. Labeling Recommendations for Devices with Cybersecurity Risks

This section gives background on some device labeling requirements and regulations and explains the role labeling may have in safety and effectiveness for devices with cybersecurity risks. It then contains labeling recommendations for communicating relevant security information to end-users that may help manufacturers comply with applicable requirements and help ensure a device remains safe and effective throughout its life-cycle.

FDA regulates device labeling in several ways. For example, section 502(f) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) requires that labeling include adequate directions for use. Under section 502(a)(1) of the FD&C Act, a medical device is deemed misbranded if its labeling is false or misleading in any particular. Under section 201(n), labeling may be misleading if it

fails to reveal facts material with respect to consequences which may result from use of the article under the conditions of use prescribed in the labeling or under such conditions of use as are customary or usual. *See also* 21 CFR 1.21.

FDA device regulations contain further requirements related to labeling. For example, 21 CFR 801.5 requires that labeling include adequate directions for use, including statements of all conditions, purposes, or uses for which the device is intended (e.g., hazards, warnings, precautions, contraindications). For prescription devices, 21 CFR 801.109(c) requires that labeling include any relevant hazards, contraindications, side effects, and precautions under which practitioners licensed by law to administer the device can use the device safely and for the purpose for which it is intended.

For devices with cybersecurity risks, informing end-users of relevant security information may be an effective way to comply with labeling requirements. FDA also believes that informing end-users of security information through labeling may be an important part of QSR design controls to help mitigate cybersecurity risks and help ensure the continued safety and effectiveness of the device. Therefore, when drafting labeling for inclusion in a premarket submission, a manufacturer should consider all applicable labeling requirements and how informing users through labeling may be an effective way to manage cybersecurity risks. Specifically, we recommend the following be included in labeling to communicate to end-users relevant security information:[30]

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

2. A description of the device features that protect critical functionality, even when the device's cybersecurity has been compromised.

3. A description of backup and restore features and procedures to regain configurations.

4. Specific guidance to users regarding supporting infrastructure requirements so that the device can operate as intended.

5. A description of how the device is or can be hardened using secure configuration. Secure configurations may include end point protections such as anti-malware, firewall/firewall rules, whitelisting, security event parameters, logging parameters, physical security detection.

6. A list of network ports and other interfaces that are expected to receive and/or send data, and a description of port functionality and whether the

[30] See IEC TR 80001-2-2 and IEC TR 80001-2-8 and IEC TR 80001-2-9 for further information

ports are incoming or outgoing (note that unused ports should be disabled).

7. A description of systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer.

8. A description of how the design enables the device to announce when anomalous conditions are detected (i.e., security events). Security event types could be configuration changes, network anomalies, login attempts, anomalous traffic (e.g., send requests to unknown entities).

9. A description of how forensic evidence is captured, including but not limited to any log files kept for a security event. Log files descriptions should include how and where the log file is located, stored, recycled, archived, and how it could be consumed by automated analysis software (e.g., Intrusion Detection System, IDS).

10. A description of the methods for retention and recovery of device configuration by an authenticated privileged user.

11. Sufficiently detailed system diagrams for end-users.

12. A CBOM including but not limited to a list of commercial, open source, and off-the-shelf software and hardware components to enable device users (including patients, providers, and healthcare delivery organizations (HDOs)) to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the device (and the connected system), and to deploy countermeasures to maintain the device's essential performance.

13. Where appropriate, technical instructions to permit secure network (connected) deployment and servicing, and instructions for users on how to respond upon detection of a cybersecurity vulnerability or incident.

14. Information, if known, concerning device cybersecurity end of support. At the end of support, a manufacturer may no longer be able to reasonably provide security patches or software updates. If the device remains in service following the end of support, the cybersecurity risks for end-users can be expected to increase over time.

These recommendations aim to communicate to end-users relevant security information, thereby helping ensure a device remains safe and effective through its life-cycle.

VII. Cybersecurity Documentation

This section lists recommended documentation manufacturers should submit in their premarket submission in addition to any submitted software documentation[31]. Specifically, FDA recommends that manufacturers include documentation of the design features from section V above, as well as risk management documentation, and labeling to demonstrate a risk-based approach that incorporates design features and a level of cybersecurity resilience appropriate for the device.

A. Design Documentation

The design documentation should demonstrate that the device is trustworthy.

1. For Tier 1 devices, documentation that addresses each recommendation in Section V.

2. For Tier 2 devices, documentation that addresses each recommendation in Section V or include a risk-based rationale for why a cybersecurity design control was not necessary. Risk-based rationales should leverage an analysis of exploitablity to describe likelihood instead of probability.

3. System Diagrams sufficiently detailed to permit an understanding of how the specific device design elements (from section V) are incorporated into a system-level and holistic picture. Analysis of the entire system is necessary to understand the manufacturer's threat model and the device within the larger ecosystem.

System diagrams should include:

[31] Content of Premarket Submissions for Software Contained in Medical Devices https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM089593.

(a) Network, architecture, flow, and state diagrams.

(b) The interfaces, components, assets, communication pathways, protocols, and network ports.

(c) Authentication mechanisms and controls for each communicating asset or component of the system including web sites, servers, interoperable systems, cloud stores, etc.

(d) Users' roles and level of responsibility if they interact with these assets or communication channels.

(e) Use of cryptographic methods should include descriptions of the method used and the type and level of cryptographic key usage and their style of use throughout your system (one-time use, key length, the standard employed, symmetric or otherwise, etc.). Descriptions should also include details of cryptographic protection for firmware and software updates.

4. A summary describing the design features that permit validated software updates and patches as needed throughout the life cycle of the medical device to continue to ensure its safety and effectiveness.[32]

B. Risk Management Documentation

Risk assessments tie design to threat models, clinical hazards, mitigations, and testing. It is important to establish a secure design architecture such that risk can be adequately managed. The suggested documentation leverages the concept of a Security Risk management report as described in the technical information report, AAMI TIR57 Principles for medical device security—Risk management,[33] although other forms of documentation that contain the same or similar information are acceptable. A security risk management report is a comprehensive approach that considers both security and safety risk analysis in a meaningful way. It provides a summary of the evaluation, assessment, and mitigation activities that assure a device is reasonably secure. The following recommendations relate to what is expected in the risk management report of a trustworthy device.

1. A system level threat model that includes a consideration of system level risks, including but not limited to risks related to the supply chain (e.g., to ensure the device remains free of malware), design, production, and deployment (i.e., into a connected/networked environment).

[32] For more information on FDA's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed devices, see Postmarket Management of Cybersecurity in Medical Devices https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[33] AAMI TIR57: Principles for medical device security—Risk management

2. A specific list of all cybersecurity risks that were considered in the design of your device. We recommend providing descriptions of risk that leverage an analysis of exploitablity to describe likelihood instead of probability. If numerical probabilities are provided, we recommend providing additional information that explains how the probability was calculated.

3. A specific list and justification for all cybersecurity controls that were established for your device. This should include all risk mitigations and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device, including:

   (a) A list of verifiable function/subsystem requirements related to access control, encryption/decryption, firewalls, intrusion detection/prevention, antivirus packages, etc.

   (b) A list of verifiable of security requirements impacting other functionality, data, and interface requirements.

4. A description of the testing that was done to ensure the adequacy of cybersecurity risk controls (e.g., security effectiveness in enforcing the specified security policy, performance for required traffic conditions, stability and reliability as appropriate). Test reports should include:

   (a) testing of device performance

   (b) evidence of security effectiveness of third-party OTS software in the system.

   (c) static and dynamic code analysis including testing for credentials that are "hardcoded", default, easily-guessed, and easily compromised.

   (d) vulnerability scanning

   (e) robustness testing

   (f) boundary analysis

   (g) penetration testing

   (h) Third Party test reports

5. A traceability matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered in your security risk and hazard analysis.

6. A CBOM cross referenced with the National Vulnerability Database (NVD) or similar known vulnerability database. Provide criteria for addressing known vulnerabilities and a rationale for not addressing remaining known vulnerabilities, consistent with the FDA's final guidance, Postmarket Management of Cybersecurity in Medical Devices.[34]

FDA believes that providing cybersecurity documentation like those recommended above will help FDA find that your device meets its applicable statutory standard for premarket review.

VIII. Recognized Standards

Please refer to FDA's website for a current list of FDA recognized consensus standards addressing Information Technology (IT) and medical device security to date.

For an updated list of FDA recognized consensus standards the Agency recommends that you refer to the FDA Recognized Consensus Standards Database,[35] 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 recognition of consensus standards, see the guidance document "CDRH Standard Operating Procedures for the Identification and Evaluation of Candidate Consensus Standards for Recognition."[36]

For information on the use of standards in premarket submissions, see the guidance document "Appropriate Use of Voluntary Consensus Standards in Premarket Submissions for Medical Devices."[37]

[34] This activity would support compliance with purchasing controls (21 CFR 820.50) by ensuring that all purchased or otherwise received product and services conform to specified requirements regarding cybersecurity. Similarly, this activity would support compliance with design controls and design validation (21 CFR 820.30(g)) to help assure that devices conform to defined user needs and intended uses, including that the software and hardware in the device are free of unacceptable cybersecurity vulnerabilities.

[35] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm

[36] https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077322

[37] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077295.pdf