U.S. FOOD & DRUG ADMINISTRATION

Welcome to today's
FDA/CDRH Webinar

Thank you for your patience while we register all of today's participants.

If you have not connected to the audio portion of the webinar, please do so now:

Dial: 800-369-3128

International Dial:1-312-470-7334

Conference Number: PWXW5373095

Passcode:2366523

Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices

Final Guidance

Heather Agler, Ph.D.
Senior Science Health Advisor
Office of the Center Director
Center for Devices and Radiological Health

Agenda

- Overview of the Guidance
  I. Key Definitions
  II. Introduction
  III. Background and Scope
  IV. Design Considerations
  V. Pre Market Submission Content
- Q & A

Key Definitions

- ***Interoperable medical devices:*** devices that have the ability to exchange and use information through an electronic interface with another medical/nonmedical product, system, or device. Interoperable medical devices can be involved in simple unidirectional transmission of data to another device or product or in more complex interactions, such as exerting command and control over one or more medical devices. Interoperable medical devices can also be part of a complex system containing multiple medical devices.

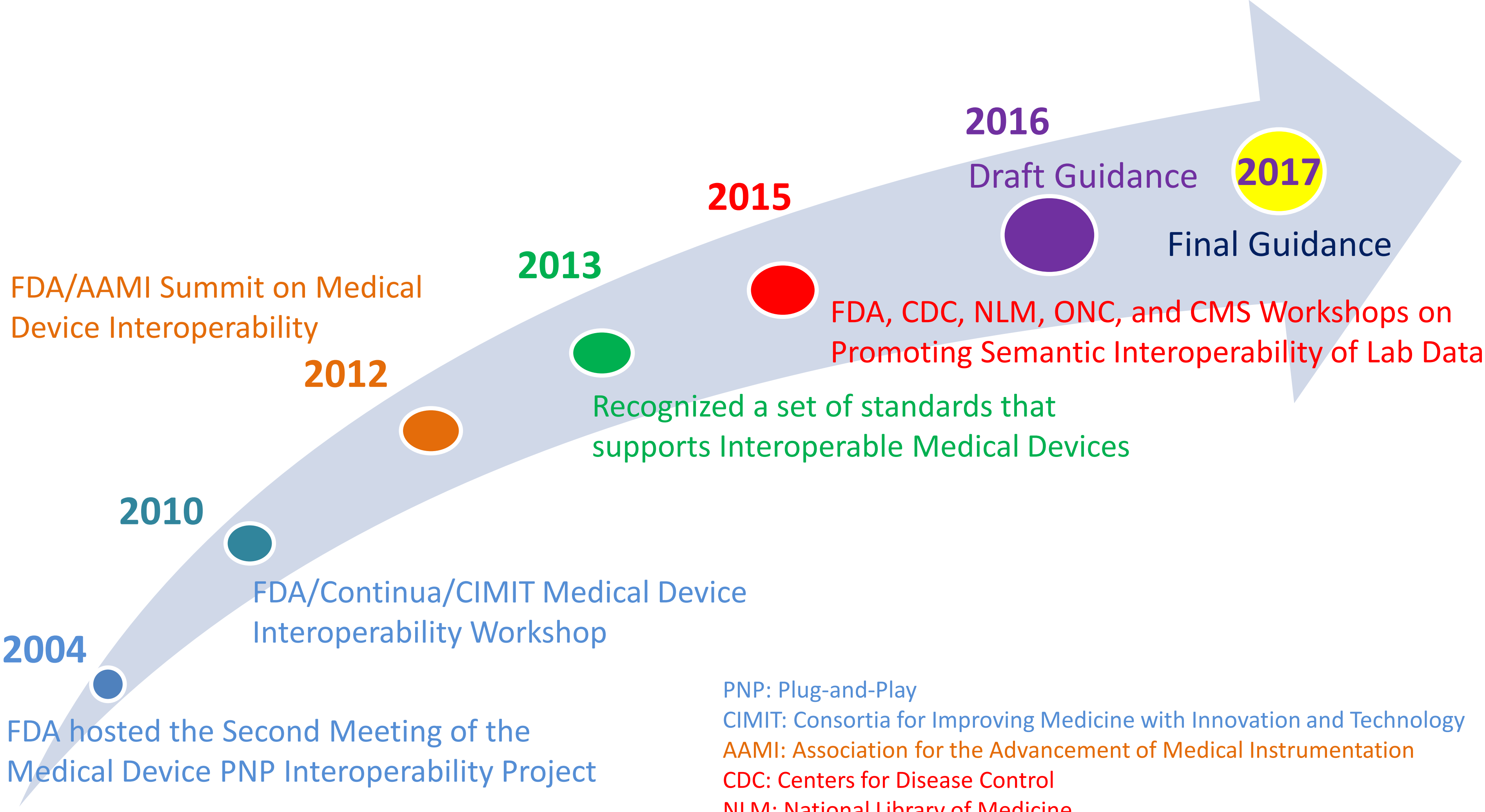
Key Definitions

- ***Electronic Interface***: the medium by which systems interact and/or communicate with each other thereby allowing the exchange of information between systems. It includes both the type of connection (e.g. USB port, wireless connection) and the information content. It is a medium by which a medical device exchanges and uses information with other equipment or other medical devices.

Purpose of the Guidance

- To promote the availability of safe and effective interoperable medical devices.
- To provide considerations to use in the development and design of interoperable medical devices.
- To clarify the contents to submit in a pre-market submission to support interoperable medical devices.
- To provide recommendations for labeling.

FDA's Involvement in Medical Device Interoperability



2004

FDA hosted the Second Meeting of the Medical Device PNP Interoperability Project

2010

FDA/Continua/CIMIT Medical Device Interoperability Workshop

2012

FDA/AAMI Summit on Medical Device Interoperability

2013

Recognized a set of standards that supports Interoperable Medical Devices

2015

FDA, CDC, NLM, ONC, and CMS Workshops on Promoting Semantic Interoperability of Lab Data

2016

Draft Guidance

2017

Final Guidance

PNP: Plug-and-Play
CIMIT: Consortia for Improving Medicine with Innovation and Technology
AAMI: Association for the Advancement of Medical Instrumentation
CDC: Centers for Disease Control
NLM: National Library of Medicine
ONC: Office of the National Coordinator
CMS: Center for Medicare and Medicaid Services

Benefits of Interoperable Medical Devices

Interoperable medical devices have the potential to:

- foster new innovative healthcare solutions at lower cost.
- foster information-sharing between devices and systems and across manufacturers.

Use of Interoperable Medical Devices

- Information from medical devices can be used to:
  - display or store information
  - interpret or analyze information
  - automatically act on or control another product

- Systems that include interoperable medical devices may be composed of existing devices, products, or technologies acting together to achieve a function different from the individual medical device

Considerations for Medical Device Manufacturers

- Designing systems with interoperability as an objective
- Conducting appropriate verification, validation and risk management activities
- Specifying the relevant functional, performance, and interface characteristics in a user available manner such as labeling

Guidance Scope

- Provides manufacturers with:
  - design considerations when developing interoperable medical devices
  - recommendations regarding information to include in pre-market submissions
  - device labeling
- This document focuses on the information content exchanged over connections (e.g., USB, wireless connection). It does not focus on aspects of physical compatibility.
- This document is not intended to provide guidance on whether or not a specific product or modification to a product requires a pre-market submission. We intend for this document to complement other FDA guidance documents.

Guidance Scope

- The pre-market discussion within this guidance applies to the following premarket submissions for interoperable medical devices
  - Premarket Notification (510(k)) including Traditional Special, and Abbreviated 510(k) submissions
  - De novo requests
  - Premarket Approval Applications (PMAs)
  - Product Development Protocols (PDPs)
  - Humanitarian Device Exemption (HDE) submissions
  - Biologics License Applications (BLAs)

Design Considerations for Developing Interoperable Devices

The following considerations should be appropriately tailored to the selected interface technology, and the intended use and use environments for the medical device.

- The Purpose of the Electronic Interface
- The Anticipated Users
- Risk Management
- Verification and Validation
- Labeling Considerations
- Use of Consensus Standards

Purpose of the Electronic Interface

- Device manufacturers should consider the purpose for each of the electronic interfaces.
- Manufacturers should consider the level of interoperability needed to achieve the purpose of the interface, as well as the information necessary to describe the interface.
- Design considerations may be different for different kinds of electronic interfaces.

Purpose of the Electronic Interface

Elements that should be considered include, but are not limited to the following:

- types of devices that it is meant to connect to
- type of data exchange taking place
- the use of standards
- the need for time synchronization
- method of data transmission
- necessary timeliness and reliability of information
- method of data transmission
- limitations or contraindications
- clinical context
- anticipated use of the interface
- the functional and performance requirements of the device

The Anticipated Users

- Manufacturers should determine the anticipated user(s) for each of the electronic interfaces.

- Determining the anticipated users will help in appropriately applying risk management strategies for activities such as developing appropriate instructions for use and setting limitations for use of the device, including contraindications, warnings and precautions.

The Anticipated Users

Manufacturers should consider the different users when designing the device and developing the instructions.

- Users, operators, and clinicians need to know the clinical uses and potential risks relevant to the use environment and the clinical task at hand.
- Equipment maintenance personnel and hospital clinical engineers need to know what actions to take to verify correct configuration and operation. They need to assure that the system is performing as specified.
- IT professionals need to understand the performance needs and security requirements of the devices connected to the networks they maintain and operate.
- System integrators may need to know the capabilities of the components so that they can perform adequate risk management and validation.
- Patients may need specific instructions on how to use their device in a home environment.

The Anticipated Users

- In addition to expected users, manufacturers should also consider malicious users or attackers in the design of the device.

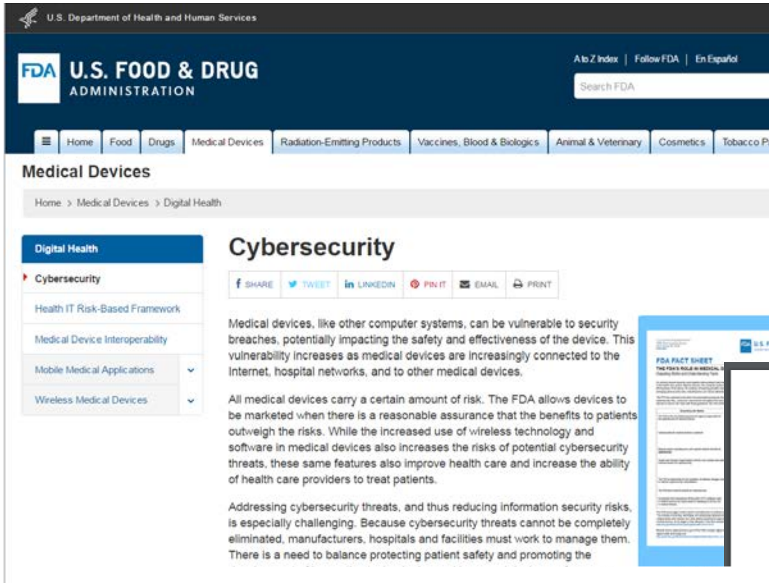
- These considerations may influence whether the manufacturer places certain limitations on the users of the device or limitations on how the device may be used.

- Developing different instructions for different users may help to mitigate the risks.

Risk Management

- Consider both intended and unintended access through the interface.
- Balance how to allow intended access while implementing security features to restrict unintended access to the medical devices.
- Consider reasonably foreseeable uses and misuses of the electronic interface.
- Develop an ongoing process for identifying hazards, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls over the lifecycle of the device.

Cybersecurity



U.S. Department of Health and Human Services

FDA U.S. FOOD & DRUG ADMINISTRATION

A to Z Index | Follow FDA | En Español

Search FDA

≡ | Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

Medical Devices

Home › Medical Devices › Digital Health

Digital Health
- Cybersecurity
- Health IT Risk-Based Framework
- Medical Device Interoperability
- Mobile Medical Applications
- Wireless Medical Devices

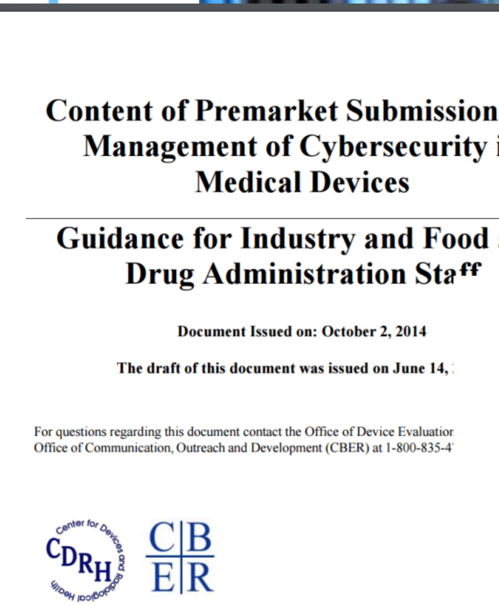
Cybersecurity

SHARE | TWEET | LINKEDIN | PIN IT | EMAIL | PRINT

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices.

All medical devices carry a certain amount of risk. The FDA allows devices to be marketed when there is a reasonable assurance that the benefits to patients outweigh the risks. While the increased use of wireless technology and software in medical devices also increases the risks of potential cybersecurity threats, these same features also improve health care and increase the ability of health care providers to treat patients.

Addressing cybersecurity threats, and thus reducing information security risks, is especially challenging. Because cybersecurity threats cannot be completely eliminated, manufacturers, hospitals and facilities must work to manage them. There is a need to balance protecting patient safety and promoting the



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Sta

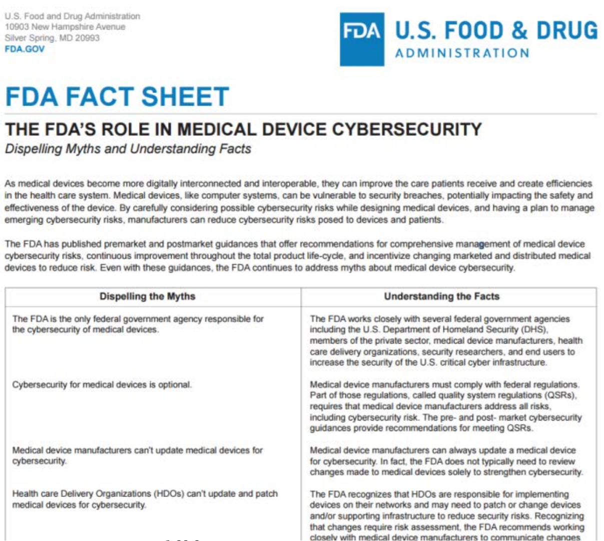
Document Issued on: October 2, 2014

The draft of this document was issued on June 14,

For questions regarding this document contact the Office of Device Evaluatior Office of Communication, Outreach and Development (CBER) at 1-800-835-4

Center for Devices and Radiological Health CDRH

CBER



U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
FDA.GOV

FDA U.S. FOOD & DRUG ADMINISTRATION

FDA FACT SHEET

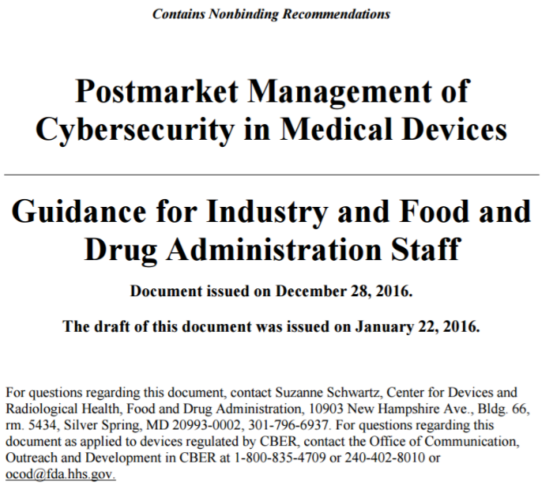
THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY

Dispelling Myths and Understanding Facts

As medical devices become more digitally interconnected and interoperable, they can improve the care patients receive and create efficiencies in the health care system. Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage emerging cybersecurity risks, manufacturers can reduce cybersecurity risks posed to devices and patients.

The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product life-cycle, and incentivize changing marketed and distributed medical devices to reduce risk. Even with these guidances, the FDA continues to address myths about medical device cybersecurity.

Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.
Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.	The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

Risk Management

Focus on the potential hazards, safety concerns, and security issues introduced when including an electronic interface. For example, as part of the evaluation and design process, manufacturers should consider the following:

- whether implementation and use of the interface degrades the basic safety or risk controls of the device;
- whether implementation and use of the interface/interfaces degrades the essential performance of the device as defined in IEC 60601-1;
- whether appropriate security features are included in the design; and
- whether the device has the ability to handle data that is corrupted or outside the appropriate parameters.

Risk Management

An interoperable system should maintain basic safety and essential performance during normal and fault conditions. A manufacturer should design an interoperable medical device that can appropriately mitigate risks associated with possible error scenarios such as:

- failures or malfunctions caused by direct or indirect connection of intended devices;
- failures or malfunctions caused by invalid commands;
- failures or malfunctions caused by receiving and processing erroneous data or commands; and
- failures or malfunctions caused by not adhering to the non-functional requirements of the communication specification. By non-functional requirements, FDA refers to the examples listed in ASTM 2761-09(2013)(e.g., bandwidth, latency, time synchronization).

Verification and Validation

- The verification and validation considerations depend on:
  - The level of risks associated with the device
  - The purpose of the interface
  - The anticipated use of the device in the target system
  - The intended use of the device
- Testing should demonstrate that the interactions on the electronic interface perform as intended and complies with the intended specifications.

Verification and Validation

- For devices meant to be used with a limited number of specific devices, appropriate testing to demonstrate safe operation with those specific devices.
- For devices meant to work with many devices, it may be appropriate to test the device against the interface specification and with representative devices for verification.
- For devices meant to be a part of a larger interoperable system, the manufacturer should conduct testing to reasonably assure that the medical device will continue to safely and effectively fulfill its intended use when it is assembled, installed, and maintained according to its instructions.

Verification and Validation

Appropriate testing may include:

- Testing to assure that the device continues to operate safely when data is received in a manner outside of the bounds of the parameters specified;
- Establish and specify fail safe states for critical functions (e.g., delivering energy, real-time monitoring);
- Verifying only authorized users (individuals, devices and systems) are allowed to exchange information with the interoperable medical device;
- Validating the user interface(s). Determining that the user(s) are capable of correctly using the interface(s);
- Assuring that reasonably foreseeable interactions only cause correct operation of other networked systems and nothing else; and
- Testing that simulates real-world use of the device.

Labeling

- Labeling should contain the functional, interface, and performance requirements of the electronic interfaces that may be used to connect medical devices with other electronic equipment.
- Labeling may include materials within the packaging of the device, the instructions for use, or device-specific information posted on the manufacturer's web site.
- There may be different directions for different users.
- Further recommendations can be found in the "Content for Pre-Market Submissions" section of this guidance.

Use of Consensus Standards

- FDA encourages the use of consensus standards to support medical device interoperability.
- Standards that support interoperability are for manufacturers and other stakeholders such as healthcare delivery organizations, system integrators, system designers, and information technology professionals who work in health care settings.
- FDA recognition of design standards that support interoperability are meant to encourage manufacturers, health care organizations, and others to implement interoperability in a standardized way. Alternatively, manufacturers may choose to use their own design preferences.
- FDA welcomes recommendations of published consensus standards for consideration of recognition http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Standards/ucm123739.htm
- Please refer to the FDA Recognized Consensus Standards Database for a current listing of recognized standards http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm

Content of Pre-market Submissions

- This section provides guidance for those interoperable medical devices that require a premarket submission.
- For a medical device intended to exchange and use information with or from another product, technology, or system, FDA recommends sponsors provide basic information similar to what would normally be provided to support other functions or features on a medical device.
- Please note:
  - There may be FDA guidances or special controls applicable to the device.
  - Some device specific standards may contain interface specification recommendations.

Device Description

- As part of the normal device description, a sponsor should discuss each externally-facing electronic interface.

- If the interface is only meant to be used by the manufacturer, this should be clearly stated.

- If the interface is meant to be used with only specific devices, those devices should be clearly specified.

- Please note that the level of detail may depend upon the intended interoperable scenario(s) in which the manufacturer expects the interoperable medical device to be used.

Device Description

The description of the electronic interface may include some or all of the following elements based upon the claims of data exchange and use made for the medical device:

- the purpose of the interface and the role the device plays within an interoperable system.
- if the interface is meant to transmit, receive, or exchange information;
- standards used;
- requirements for timeliness and the integrity of the information (e.g. sample rate, transmission rate);
- communication format, rate, and transmission method;
- limitations (what the user should not do), contraindications, precautions, and warnings;
- functional and performance requirements; and
- the Application Programming Interface (API) if the device is software that can be used by other software, medical device, or system.

Risk Analysis

- Manufacturers' risk analysis should consider the risks associated with interoperability, reasonably foreseeable misuse, and reasonably foreseeable combinations of events that could result in a hazardous situation.
- As discussed in ISO 14971, risk control measures may not be necessary for risks that are broadly acceptable.
- There may be additional hazardous situations that arise when more than one medical device is connected within a system.
- The manufacturer should specify which mitigations are implemented and which are necessary for safe use but may require implementation by other parties, such as the party responsible for set-up or installation.

Risk Analysis

FDA recommends including an analysis of the interface or interfaces on the devices, the intended connections, and any effects that the connection may have on the device performance. Your submitted analysis should include the normal elements in a risk analysis and address:

- the risk control measures for reducing unacceptable risks to acceptable levels;
- fault tolerant behavior, boundary conditions, and fail safe behavior;
- any risks potentially arising from security vulnerabilities that may be involved with the presence of an electronic interface; and
- risks arising from normal use as well as reasonably foreseeable misuse.

Verification and Validation

- A sponsor should include results of verification and validation testing for the electronic interfaces. The nature and extent of the validation depends upon the risks associated with the device, the purpose of the interface, the anticipated use of the device in the interoperable system, and the intended use of the device.
- For devices only meant to be used with a limited number of specific devices, documentation demonstrating appropriate testing with those specific devices may be appropriate.
- For devices meant to connect with a class of devices or to be used by any device or computer system, documentation demonstrating appropriate testing with a representative of that class of devices or within the context of the system may be more appropriate.

Verification and Validation

Documentation which demonstrates the following performance testing should be included in the submission:

- verification that the device interface meets its design specifications;
- validation that the device interface performs as intended;
- determination and verification of the information that should be provided to a user to connect to the interface and to allow the user to ensure that the connection has been made correctly; and
- verification that the device will perform safely and within specification when used under normal conditions and abnormal conditions that are reasonably likely to occur.

Content of Pre-market Submissions: Verification and Validation

The degree of documentation can vary based upon the risks. If the purpose of the interface along with the intended scenarios for use of the interface do not add significant risk to the operation of the medical device, then test summaries may be sufficient.

Examples:

- If an infusion pump is intended to receive patient data from several devices (e.g., a pulse oximeter, ventilator, and blood pressure monitor) and use this data to change infusion pump settings, complete test reports should be provided to the FDA in the planned submission.

- If a non-invasive blood pressure monitor has an interface intended to allow historical data to be downloaded to a computer, then a summary of the testing performed on the interface may be sufficient.

Content of Pre-market Submissions: Labeling

- Information regarding the electronic interface on the device should be included in the labeling, so that the device can be used safely and effectively for its intended uses.

- Information should enable users to connect to the device in the specified manner, and should give proper instruction on how to use the connection to the device in the ways for which it was designed.

- This should include any limitations of the connection to discourage any misuse of the device.

- Precautions, warnings, and contraindications should be included in device labeling as well.

- Validation of labeling regarding the use of the electronic interface should consider human factors as appropriate.

Labeling

Scenario 1: The device is meant to interact with only a few specific devices. The labeling should explicitly state that the medical device is meant to connect with the specific devices listed (including the version) and that it should not be used with other medical devices or nonmedical device technologies.

Scenario 2: The interface is only meant to be used by the manufacturer’s technicians for software updates or diagnostics. It should be explicitly stated in the labeling that the use of the electronic interface is reserved for representatives of the manufacturers.

Scenario 3: The device is not meant to be interoperable. The labeling should state that the electronic interfaces found on the device are not meant for connecting to other medical devices or non-medical device technologies.

Labeling

Scenario 4: If the electronic interface is meant to interact with other medical devices, the guidance lists a series of items to consider placing in your labeling.

- Consider whether certain information is needed for someone to properly connect to your device through the electronic interface and use the information as described.
- Consider what information is appropriate based on the risk associated the device, the purpose of the interface, the anticipated use of the device in the interoperable system, and the intended use of the device.
- Consider the use of standards for the electronic interfaces.

Labeling

FDA recommends the following information be included in the device labeling as appropriate, based on the purpose of the medical device interface:

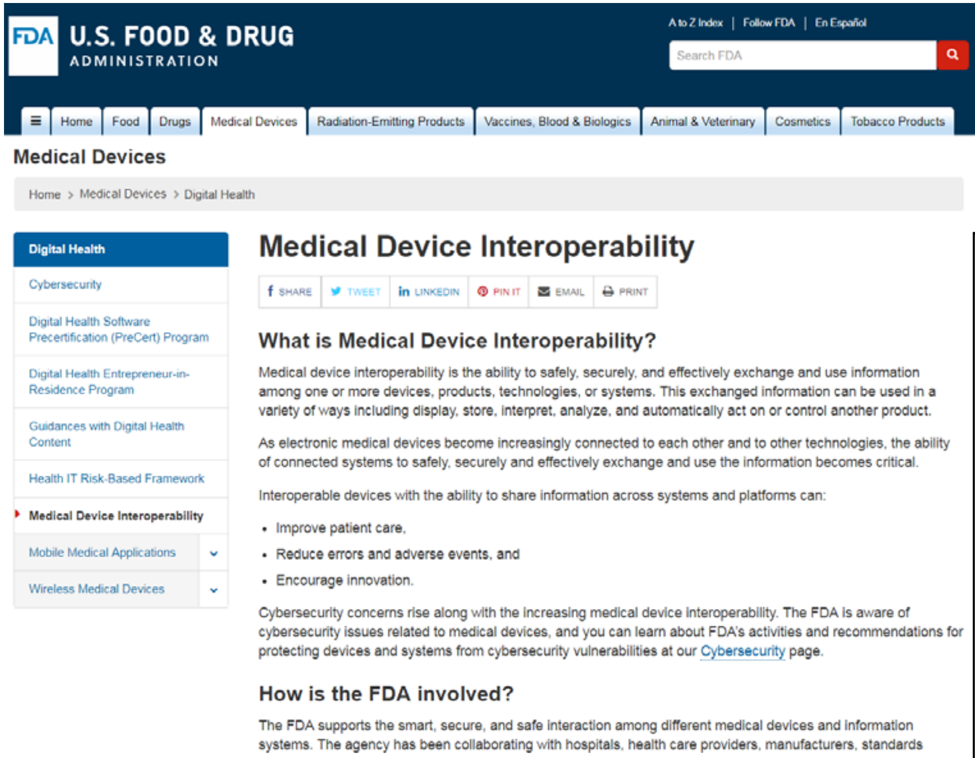
- the purpose of the interface including any devices, device types, interface standard/specification, or software with which it is meant to connect;
- the anticipated user(s);
- whether the connection is meant to control the operations of another device;
- specifications for each interface (e.g., physiological waveforms, probe type, accuracy, frequency of response, update rate, data rate, bandwidth), as well as the necessary performance and functional requirements from the device related to the sending or receiving of data/control;
- list of the data attributes being exchanged;
- summary of the testing performed on the interfaces to verify interoperability claims and any activities suggested for the user to verify safe operation. In the case where testing was performed to an interface specification and verified with a representative device, the manufacturer should specify the representative device used;

Labeling

FDA recommends the following information be included in the device labeling as appropriate, based on the purpose of the medical device interface (continued):

- relevant standards used and certifications received;
- any method used for time synchronization;
- a description of any fault tolerance behavior, boundary condition testing, or fail safe for critical functions (e.g., delivering energy) that will allow the user to understand how to use the interface correctly;
- any known limitations (what the user should not do), contraindications, precautions and warnings;
- recommended connections;
- recommended settings, or configurations for the electronic interface; and
- instructions for specific users such as IT personnel on how to connect or install and disconnect or uninstall the device.

Medical Device Interoperability


FDA U.S. FOOD & DRUG ADMINISTRATION
A to Z Index | Follow FDA | En Español
Search FDA
≡ Home Food Drugs Medical Devices Radiation-Emitting Products Vaccines, Blood & Biologics Animal & Veterinary Cosmetics Tobacco Products
Medical Devices
Home > Medical Devices > Digital Health
Digital Health
Cybersecurity
Digital Health Software Precertification (PreCert) Program
Digital Health Entrepreneur-in-Residence Program
Guidances with Digital Health Content
Health IT Risk-Based Framework
Medical Device Interoperability
Mobile Medical Applications
Wireless Medical Devices
SHARE TWEET LINKEDIN PIN IT EMAIL PRINT

Medical Device Interoperability

What is Medical Device Interoperability?

Medical device interoperability is the ability to safely, securely, and effectively exchange and use information among one or more devices, products, technologies, or systems. This exchanged information can be used in a variety of ways including display, store, interpret, analyze, and automatically act on or control another product.

As electronic medical devices become increasingly connected to each other and to other technologies, the ability of connected systems to safely, securely and effectively exchange and use the information becomes critical.

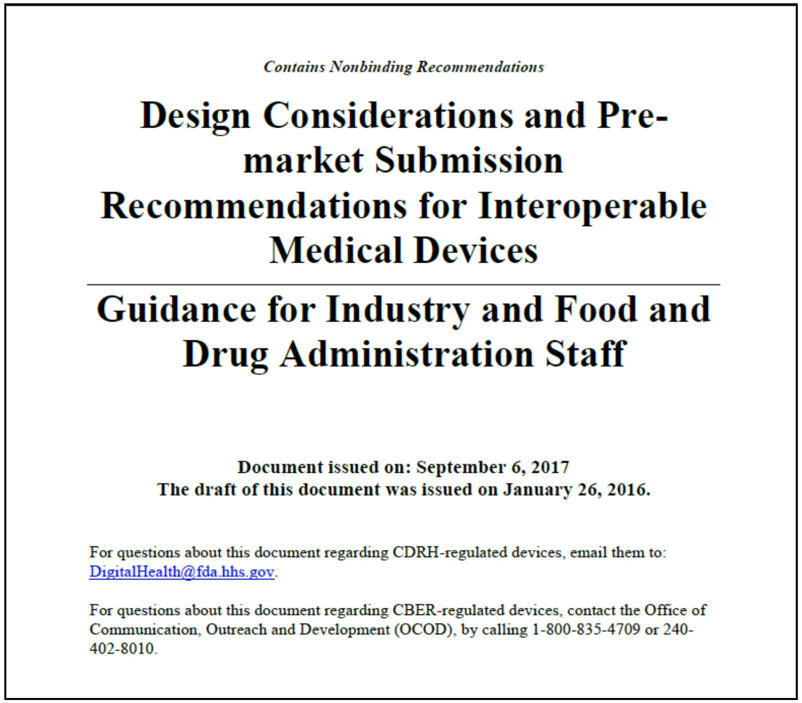
Interoperable devices with the ability to share information across systems and platforms can:

- Improve patient care,
- Reduce errors and adverse events, and
- Encourage innovation.

Cybersecurity concerns rise along with the increasing medical device interoperability. The FDA is aware of cybersecurity issues related to medical devices, and you can learn about FDA's activities and recommendations for protecting devices and systems from cybersecurity vulnerabilities at our Cybersecurity page.

How is the FDA involved?

The FDA supports the smart, secure, and safe interaction among different medical devices and information systems. The agency has been collaborating with hospitals, health care providers, manufacturers, standards



Contains Nonbinding Recommendations

Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 6, 2017
The draft of this document was issued on January 26, 2016.

For questions about this document regarding CDRH-regulated devices, email them to: DigitalHealth@fda.hhs.gov.

For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 240-402-8010.

Digital Health related questions: DigitalHealth@fda.hhs.gov

Questions?

For questions related to the guidance document, please contact the Digital Health Team: digitalhealth@fda.hhs.gov

For general questions, please contact the Division of Industry and Consumer Education: DICE@fda.hhs.gov

Slide Presentation, Transcript and Webinar Recording will be available at:
http://www.fda.gov/training/cdrhlearn
Under the Heading: Specialty Technical Topics; Subheading: IT and Software

Please complete a short survey about your FDA CDRH webinar experience. The survey can be found at www.fda.gov/CDRHWebinar
immediately following the conclusion of the live webinar.