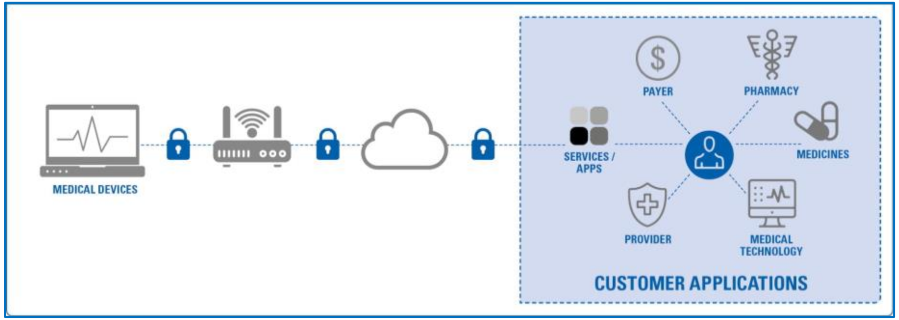
Interoperability vs Cybersecurity: Understanding How They Interrelate and Managing Risk



Jodi G. Daniel, Partner, Crowell & Moring LLP
Aftin Ross, Senior Special Advisor for Emerging Initiatives, CDRH, FDA
Charlene Cho, Senior Counsel, Medical Devices, Johnson & Johnson

Premise for Interoperability

Patients and the health care providers caring for them are often presented with an incomplete picture of their health and care as pieces of their information are stored in various, unconnected systems and do not accompany the patient to every care setting . . . When a patient receives care from a new provider, a record of their health information should be readily available to that care provider, regardless of where or by whom care was previously provided. ***85 Fed. Reg. 25510, 25511.***

Headlines from the Press

THE WALL STREET JOURNAL.

English Edition ▾ | Print Edition | Video | Podcasts | Latest Headlines

CIO JOURNAL | Content by Deloitte.

Content from our Sponsor. The Wall Street Journal news department was not involved in the creation of this content.

Shifting to a Culture of Interoperability in Health Care

BIG DATA | DATA MANAGEMENT | HEALTH CARE

Interoperability Promises a Superhighway of Data

REGULATORY | HEALTH CARE PROVIDERS | HEALTH REFORM | TECHNOLOGY | LIFE SCIENCES

Strategies to Improve Interoperability in Health Care

Federal Actions Relevant to Interoperability

- 1996: Health Insurance Portability and Accountability Act (HIPAA)
- 2009: Health Information Technology for Economic and Clinical Health (HITECH) Act
- 2016: 21st Century Cures Act
- 2017: Executive Order 13813 – Promoting Health Care Choice and Competition (revoked by President Biden in Jan 2021)
- 2018: MyHealthEData Initiative
- 2020: CMS Interoperability and Patient Access Final Rule
- 2020: ONC Cures Act Final Rule on Interoperability, Information Blocking, and Health IT Certification

HHS Offices Involved in Interoperability

Office	Significance
Centers for Medicare and Medicaid Services (CMS)	Develops policies to promote interoperability; Oversees programs that leverage Fast Healthcare Interoperability Resources (FHIR) - based Application Programming Interfaces (APIs) for Medicare beneficiaries (e.g., “BlueButton”); Works with Standards Development Organizations (SDOs) to provide open-source implementation guides.
Office of the National Coordinator for Health IT (ONC)	Coordinates nationwide efforts to support the electronic use and exchange of health information; Sets federal strategy for health IT, Establishes regulatory standards for and certification of health IT; Develops information blocking policies and receives information blocking complaints.
Office of the Inspector General (OIG)	Investigates Health IT developers and health information networks & exchanges that may have engaged in information blocking; Imposes Civil Monetary Penalties (CMPs) of up to $1M per violation; Refers healthcare providers who have engaged in information blocking to appropriate authorities for sanctions.
Office of Civil Rights (OCR)	Enforces HIPAA Privacy Rule; HIPAA Security Rule, HIPAA Breach Notification Rule AND the confidentiality provisions of the Patient Safety Rule.

Select Definitions Related to ONC's & CMS' Final Rule

Electronic Health Information (EHI)

Effective October 6, 2022, *all* electronic protected health information (ePHI) as defined in 45 CFR 160.103 and to the extent that it would be included in a designated record set (DRS) as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity, excluding psychotherapy notes and information collected in anticipation of litigation or administrative action.

Information Blocking

A practice by a health IT developer of certified health IT, health information network, health information exchange, or health care provider that is likely to interfere with access, exchange, or use of electronic health information (EHI), except as permitted by law or specified by HHS as a reasonable and necessary activity.

Interoperability (with respect to Health IT)

Health information technology that (A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; (B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and (C) does not constitute information blocking.

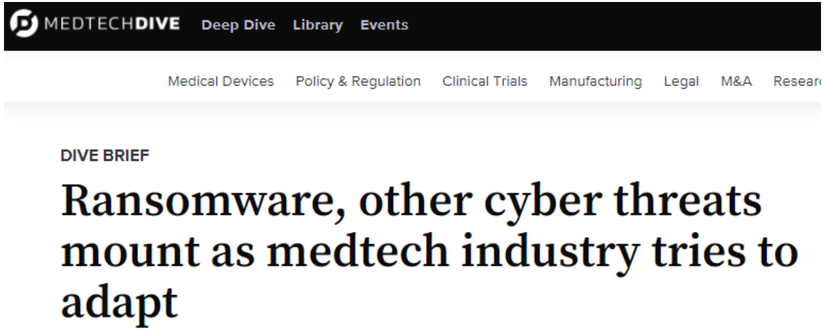
Application Programming Interface (API)

Software intermediary that allows two different applications to talk with each other. In the context of Health IT, the API must provide access to all data elements of a patient's eHRs, subject to applicable privacy laws.

Some Notable Cyber Attacks

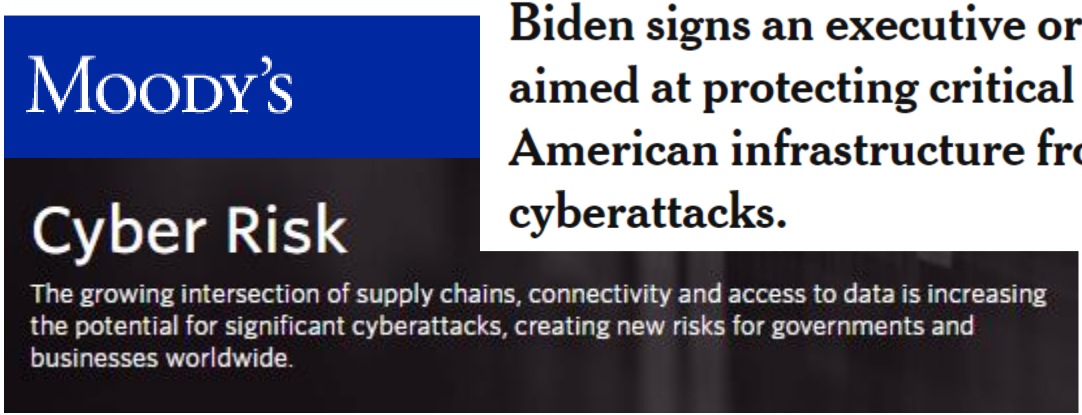
- Solar Winds (2021)
  - Microsoft, Cisco, Intel, Deloitte, CA Hospitals, Kent State University
  - Departments of Defense, Homeland Security, Energy, Treasury, etc.
  - SVR (Russia’s Foreign Intelligence Service)
  - $70M ransom demand
- Colonial Pipeline (2021)
- NetWalker (2020)
- TravelEx (2019)
- Marriott Hotels (2018)
- WannaCry (2017)
- NotPetya (2017)

Headlines from the Press



DIVE BRIEF

Ransomware, other cyber threats mount as medtech industry tries to adapt



Cyber Risk

The growing intersection of supply chains, connectivity and access to data is increasing the potential for significant cyberattacks, creating new risks for governments and businesses worldwide.

The New York Times

Biden signs an executive order aimed at protecting critical American infrastructure from cyberattacks.

Federal Actions on Cybersecurity

- 2013: Executive Order 13636 – Improving Critical Infrastructure Cybersecurity
- 2013: Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience
- 2014: Federal Information Security Modernization Act
- 2015: National Cybersecurity Information Sharing Act
- 2015: Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing
- 2016: Presidential Policy Directive 41 – United States Cyber Incident Coordination
- 2017: Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- 2021: Executive Order 14028 – Improving the Nation’s Cybersecurity

Federal Agencies Involved in Cybersecurity

Agency	Sub-Agency, Division or Office	Significance
DHS	Cybersecurity and Infrastructure Security Agency (CISA)	Assesses cyber and other risks to the nation’s critical infrastructure sectors, such as the power grid, water systems, and hospitals.
DoD	National Security Agency (NSA)	Leads the government’s efforts in signals intelligence and “information assurance” of national security IT systems.
DoJ	Federal Bureau of Investigation (FBI)	FBI’s National Cyber Investigative Joint Task Force (NCIJTF) coordinates with over 30 federal partners to share information relating to cyberthreat investigations.
HHS	Office of the Asst Sec of Preparedness & Response (ASPR) Office of the Chief Information Officer (OCIO) Office of Security and Strategic Information (OSSI) Office of Civil Rights (OCR) Office of the National Coordinator for Health IT (ONC)	ASPR: Health Care Industry Cybersecurity Task Force (HCICTF) OCIO: Develops IT Security and Privacy Policies OSSI: Serves as point of contact for insider threats OCR: Publishes quarterly cybersecurity newsletters ONC: Facilitates cyber threat info sharing across HHS
FTC	Bureau of Consumer Protection	Enforces cybersecurity requirements related to consumer privacy based on a "reasonable security" standard.
DoC	National Institute of Standards and Technology (NIST)	NIST’s Computer Security Division develops cybersecurity and privacy standards, best practices, and technology to protect federal government and private sector networks.

Select Definitions from FDA Guidance Documents

Cybersecurity
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.

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).

Threat
Any circumstance or event with the potential to adversely impact the device, organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats exercise vulnerabilities, which may impact the safety or essential performance of the device.

Interoperability and Data Access

FDLI: Cybersecurity vs. Interoperability: Understanding How They Interrelate and Managing Risk

Jodi Daniel, JD, MPH, Crowell & Moring

Key Takeaways

- Cybersecurity is about protecting the vulnerability of data.
- Interoperability is about facilitating the secure sharing of health data.
  - Entities still must protect against vulnerability to their own system that results from connecting with an application or medical device.
  - Can refuse to share if there is a concern to the security of your own system
  - Interoperability rules acknowledge and build on security requirements in HIPAA.
- Actors need to focus on protecting data in their own systems and cannot use general security concerns of the recipient as an excuse to not share data
- Health tech companies are required to support interoperability and not interfere with access, exchange or use of EHI.

Data Protection vs. Data Access

Data Protection
(*Privacy and security*)

Data Access
(Interoperability)

Regulatory Background

OCR –

HIPAA and HITECH Act

- Covered entities and business associates
- Privacy, Security, Breach Notification

ONC -

21st Century Cures Act and HITECH Act

- Health IT Certification – EHR developers
- Providers, certified health IT developers and health information exchanges and networks (HIE/HINs)
- Interoperability requirements and information blocking prohibition

FTC -

FTC Act

- For profit companies
- Unfair and deceptive trade practices (police privacy and data security); breach notification (all health apps)

Three Primary HIPAA Rules

Privacy Rule

- Limits uses and disclosures of protected health information (PHI)
- Establishes individual rights (e.g., individual access to one's own PHI)
- Imposes various administrative requirements (e.g., policies, training)

Security Rule

- Requires reasonable and appropriate administrative, physical, technical, and organizational security safeguards
- Designed to be flexible and scalable

Breach Notification Rule

- Requires covered entities to notify individuals/OCR/media if PHI is compromised
- Business associates must notify the relevant covered entity

➢ Limited scope:

- Only applies to covered entities (most health care providers, health plans, and health care clearinghouses) and their business associates
- Only applies to protected health information (not de-identified information)

Interoperability, Information Blocking, Patient Access

The Balance Shifts to Access Over Protection

- Concerns
  - Patients have a right to access data under HIPAA but routinely have difficulty in accessing such data
  - Interoperability seemed limited with electronic health information in silos
  - The government invested $34 Billion in adoption of EHRs and have not realized the benefits to health outcomes and efficiencies from easier access to data
  - Data is seen as an asset not to be shared because it is not in data holders' economic interests
- Goals
  - Improve interoperability so data can follow the patient and for a learning health system
  - Improve easy patient access to electronic health information

Interoperability Regulations

- **Information Blocking**
  - New legal prohibition against **information blocking**
  - When an entity knows or should know that a particular practice is unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information
  - Applies to health care providers, health IT developers, and health information exchanges and networks (HIE/HIN)
  - Penalties of up to $1 million per violation for developers and HIE/HINs
- **ONC Regulations Implemented the Rules**
  - Provides exceptions for practices that may be an interference but are not “information blocking” in violation of the rule
  - Shifted the paradigm created by HIPAA
  - Updates to ONC Health IT Certification Program (certification criteria, conditions and maintenance of certification requirements, and oversight of these requirements) – including standardized APIs
  - Promotes patient access to data through third party apps via APIs

ONC Information Blocking Rule Exceptions

- **No violation if an exception is met**
  - Meeting an exception provides a guaranteed protection from CMPs and the other disincentives under the information blocking prohibition.
- **Security Exception (45 CFR 171.203). Generally, the practice must:**
  - Be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.
  - Be tailored to the specific security risk being addressed.
  - Be implemented in a consistent and non-discriminatory manner.
  - If the practice implements an organizational security policy, be directly responsive to security risks and align with consensus-based standards or best practice guidance.
  - If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that the practice is necessary to mitigate the security risk to electronic health information, and there are no reasonable and appropriate alternatives.
- Practice that does not meet the conditions of an exception would not have guaranteed protection from CMPs, for example, but would **not** necessarily mean an actor is engaged in information blocking.
  - Case-by case determination

Compliance with Information Blocking & HIPAA

Significant Paradigm Shift

- **HIPAA covered entities that are subject to interoperability rules must walk a fine line between old and new requirements**
  - Information blocking rules apply to much of the same health information as HIPAA (although covered actor differ)
  - HIPAA provides for *permissible* disclosures. Information blocking rules *require* disclosure of EHI by Actors where permitted by HIPAA. (E.g., health care operations, research)
- **Exceptions**
  - Security exception generally is aligned with HIPAA. E.g., conducting a security risk assessment and following industry standards
  - Privacy exception is more limited.
- **Patient right of access**
  - Information blocking builds on HIPAA Individual Right of Access
  - Supports patient access via 3rd party app of their choice
  - Actors cannot prohibit access based on privacy policy of app
  - Can only address security if there is risk to the security of the data holder not if the security of the app is lacking
  - Actors are encouraged to educate patients about privacy and security risks of third party applications.

Some Flexibility

- HIPAA Covered Entities and Business Associates are still obligated under HIPAA's Privacy & Security Rule - sufficient flexibility with regard to interoperability requirements
  - Must verify the identity and authority of the recipient
  - May limit data sharing to only permissible purposes
  - May protect security of data holder's system BUT NOT security of the app
  - Encouraged to educate users

FTC Action- Health Breach Notification Rule (HBN)

- The FTC HBN rule has applied only to vendors of personal health records, and PHR-related entities when there is a breach
- FTC’s policy statement (September 15, 2021):
  - Expanded the rule
  - Applies to health apps broadly
  - Applies to privacy – i.e., if there is any sharing of information that is not authorized by the individual

HBN, Title 16 of the Code of Federal Regulations, Part 31

On the Horizon

- Information blocking rule and interoperability requirements will help devices and consumer facing applications connect to EHRs and get access to EHI.
  - Will facilitate development and use of innovative consumer-facing applications and devices to improve health care
  - Will enable greater use of innovative tools for clinicians to support health care delivery
  - Will enable individuals to access their data to share for research of new drugs and devices

Contact

Jodi Daniel

Crowell & Moring

jdaniel@crowell.com

202-624-2908

@jodidaniel

FDA MEDICAL DEVICE CYBERSECURITY

AFTIN ROSS, PHD

CENTER FOR DEVICES AND RADIOLOGICAL HEALTH
FOOD AND DRUG ADMINISTRATION

FDLI

CYBERSECURITY VS. INTEROPERABILITY: UNDERSTANDING HOW THEY INTERRELATE AND MANAGING RISK

2021

Framing the Issue

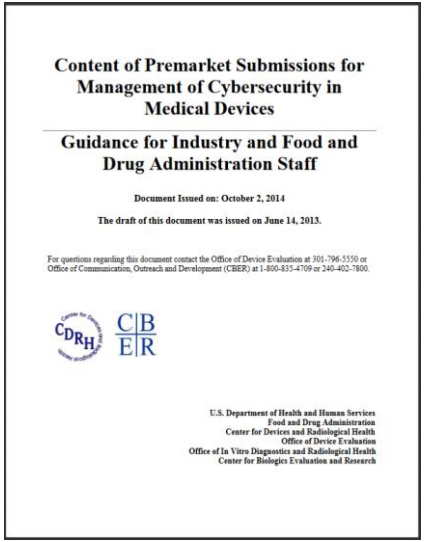
- Connected medical devices, like all other computer systems, incorporate software that are vulnerable to threats
- We are aware of cybersecurity vulnerabilities and incidents that have directly impacted medical devices or hospital network operations
- When medical device vulnerabilities are not addressed and remediated, they can be exploited which can result in:
  - patient harm
  - serve as access points for entry into healthcare delivery organization (HDO) networks
- May lead to compromise of confidentiality, integrity, and availability

Bottom Line Up Front (BLUF)

- Medical device cybersecurity is a patient safety issue
- *“Whole of community/shared responsibility”* approach: Collaboration is key
- Security spans across the total product lifecycle
- Impact on critical infrastructure within and across sectors
- Shifting the mindset:
  - Consider scenarios beyond “intended use”
  - Integrate threat modeling
  - Beware of using probabilistic determinations—these can yield a false sense of security
- Connected devices interoperate and as a result depend on the availability of other devices to function. Cybersecure devices can be enablers of interoperability
- **Medical device cybersecurity is dynamic and FDA continues to adapt and evolve our approaches as new information becomes available**
- Major strides made AND acceleration necessary

FDA has found 510(k) submissions to be “not substantially equivalent” (NSE) and “postmarket approval” (PMA) devices to be not approvable based on cybersecurity concerns alone.

Total Product Life Cycle Guidance Approach



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

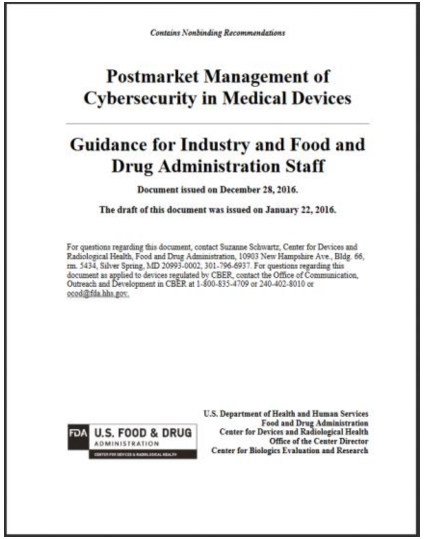
Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

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

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

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



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

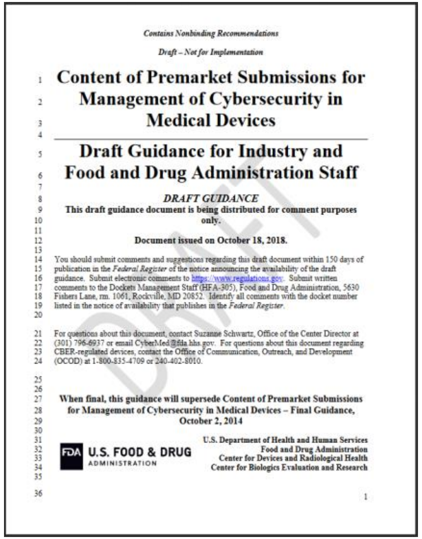
Guidance for Industry and Food and Drug Administration Staff

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.

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



Contains Nonbinding Recommendations

Draft – Not for Implementation

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*.

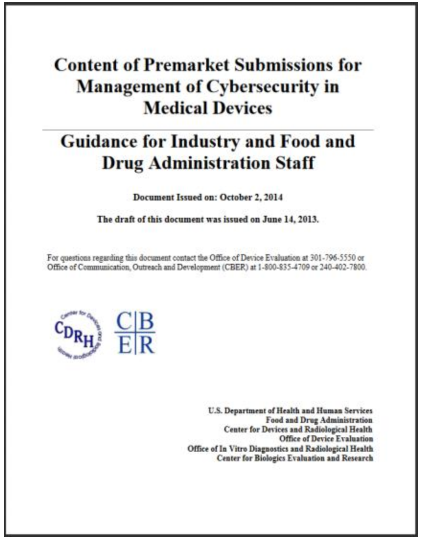
For questions about this document, contact Suzanne Schwartz, Office of the Center Director at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010.

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

1

2014 Premarket Guidance



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

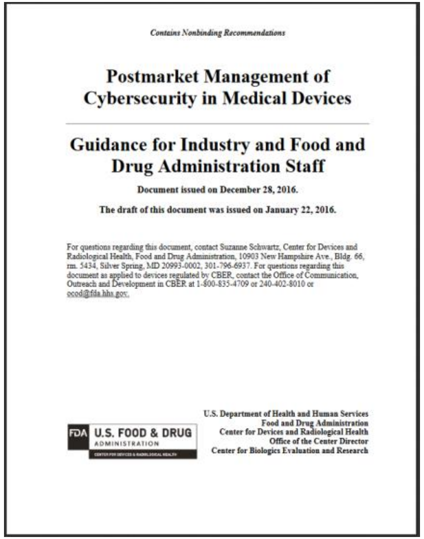
The draft of this document was issued on June 14, 2013.

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

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

- High-level guidance: allows for agency evolution alongside industry as understanding of cybersecurity throughout the sector has grown
- Stressed importance of cybersecurity and risk management as part of Quality System Regulations (QSRs)
- Created a structure that allows for reviews to evolve over time, in parallel to the technology and products being evaluated
- Laid groundwork for future agency work on cybersecurity in devices

2016 Postmarket Guidance



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.

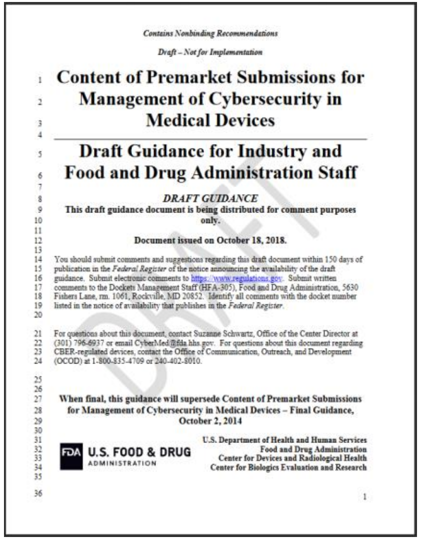
For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by 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.

FDA U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

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

- Coordinated Vulnerability Disclosure
- Part 806 Reporting Enforcement Discretion if meet criteria outlined in guidance
- Focus on cybersecurity risk assessments being about severity and exploitability
- Criticality of transferring lessons learned from postmarket to design/review decisions in premarket

2018 Draft Premarket Guidance



Contains Nonbinding Recommendations

Draft – Not for Implementation

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. FOOD & DRUG ADMINISTRATION

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

- Greater focus on criticality of security throughout the total product lifecycle
- Includes software supply chain transparency and Cybersecurity Bill of Materials (CBOM)
- Security architecture and security control recommendations to “build in” rather than “bolt on” security
- Increased focus on security testing
- Identification and discussion of organizational and procedural needs with respect to cybersecurity

Premarket Guidance Update re: Comments

- Better aligns with a Secure Product Development Framework (SPDF); e.g.,
  - Medical Device and Health IT Joint Security Plan (JSP)
  - ANSI/ISA 62443-4-1 Security for industrial automation and control systems
- Removed Tiers
- Changed Cybersecurity Bill of Materials to Software Bill of Materials (SBOM)

Cybersecurity Interoperability: Dependency Considerations

- Cloud:
  - Use steadily increasing. Increased focus during the COVID-19 pandemic (e.g., more remote monitoring and remote services)
  - While having medical device functionality in the Cloud has many benefits, it is not without risks
  - Dependency concerns arise about what happens should the Cloud be unavailable or be impacted by a cybersecurity incident
- Network/Connection:
  - For example, network connections can be enabled via wired ethernet connections, wirelessly through WiFi, or can include Bluetooth or other radiofrequency communications
  - Examples of potential intersections between cybersecurity and interoperability related to network connectivity include:
    - Networks can be disconnected due to ransomware at the facility, fail due to the network being overloaded
    - Other connections can fail due to software, hardware, or cybersecurity incidents

Collaborations: Threat Modeling

- FDA provided funding to MDIC and MITRE to develop and host "bootcamps" to do two things:
  - "Train **facilitators**" to develop individual experts within the industry who can train others to do threat modeling.
  - Host bootcamps to provide opportunity for "**facilitators**" to train others within industry.
- Threat modeling playbook also being funded as an educational resource
  - MDIC hosted a webinar on the playbook (https://mdic.org/event/playbook-for-threat-modeling-medical-devices-webinar/)

Patient Safety depends upon Cyber Safety

FDA contacts:

Suzanne.Schwartz@fda.hhs.gov
Aftin.Ross@fda.hhs.gov
Jessica.Wilkerson@fda.hhs.gov
Kevin.Fu@fda.hhs.gov
Linda.Ricci@fda.hhs.gov

Or email the team:

CyberMed@fda.hhs.gov

Visit the FDA Cybersecurity Webpage:

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm