MEDICAL DEVICE CYBERSECURITY: A TOTAL PRODUCT LIFECYCLE APPROACH

SETH D CARMODY, PHD, HCISPP
CDRH / FDA

PEAC
SEPTEMBER 10, 2019

Key Terms - What is a Medical Device?

- **FD&CA 201(h)** The term "device" **means an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory,** which is—**(1)** recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them,

- **(2)** intended for **use in the diagnosis** of disease or other conditions, or **in the cure, mitigation, treatment, or prevention of disease**, in man or other animals, or

- **(3)** intended to **affect the structure or any function** of the body of man or other animals, and

- which **does not achieve its primary intended purposes through chemical action** within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 360j(*o*) of this title.

Key Terms - What is Cybersecurity?

- **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.

Key Cybersecurity Terms

- **Asset:** The people, property, and information to be protected. In medical device cybersecurity, assets include the patient, the medical device, and data transmitted about the patient.
- **Threat:** Anyone or anything that can exploit a vulnerability, intentionally or accidentally, and steal, damage, or destroy an asset. In medical device cybersecurity, the threat is often an unauthorized person who intentionally accesses and controls a device and uses that access to issue commands to the device.
- **Vulnerability:** A weakness or gap in a security program or protocol that can be exploited by threats to gain unauthorized access to an asset. In medical device cybersecurity, the vulnerability is typically associated with a security gap in the software or firmware used by the device.
- **Risk:** The ***potential*** for loss, damage, or destruction of an asset which occurs when a threat exploits a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities. In medical device cybersecurity, the risk is typically associated with an unauthorized person (threat) accessing the device(s) of one or more patients by exploiting a vulnerability (such as a security weakness in the device's software or firmware). Examples include inappropriate pacing or shocks from a pacemaker or inappropriate dosing from an infusion pump.

Framing the Issue

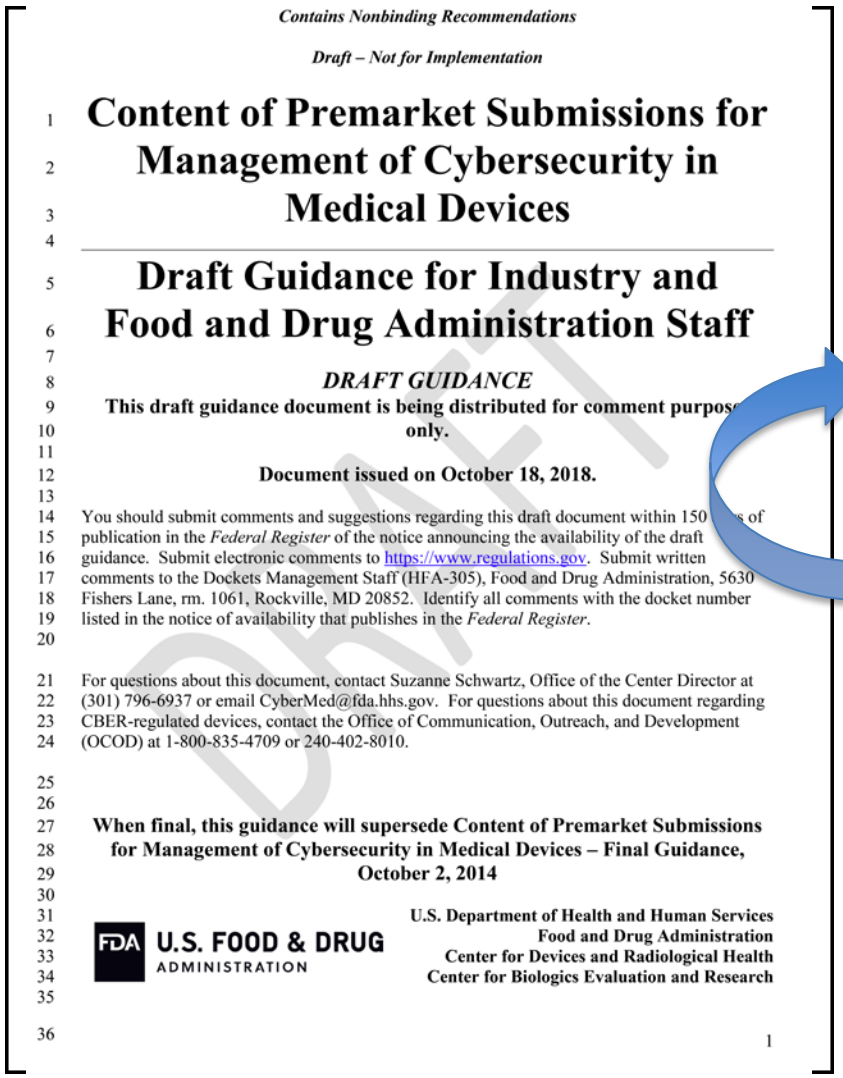
- Connected medical devices, like all other computer systems, incorporate software that are vulnerable to threats
- We are aware of cybersecurity vulnerabilities and incidents that have directly impact medical devices or hospital network operations
- When medical device vulnerabilities are not addressed 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

Cybersecurity Total Product Lifecycle (TPLC)

2018 – Premarket revision

2014 – Premarket

2016 – Postmarket



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 purpose only.

Document issued on October 18, 2018.

You should submit comments and suggestions regarding this draft document within 150 s 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*.

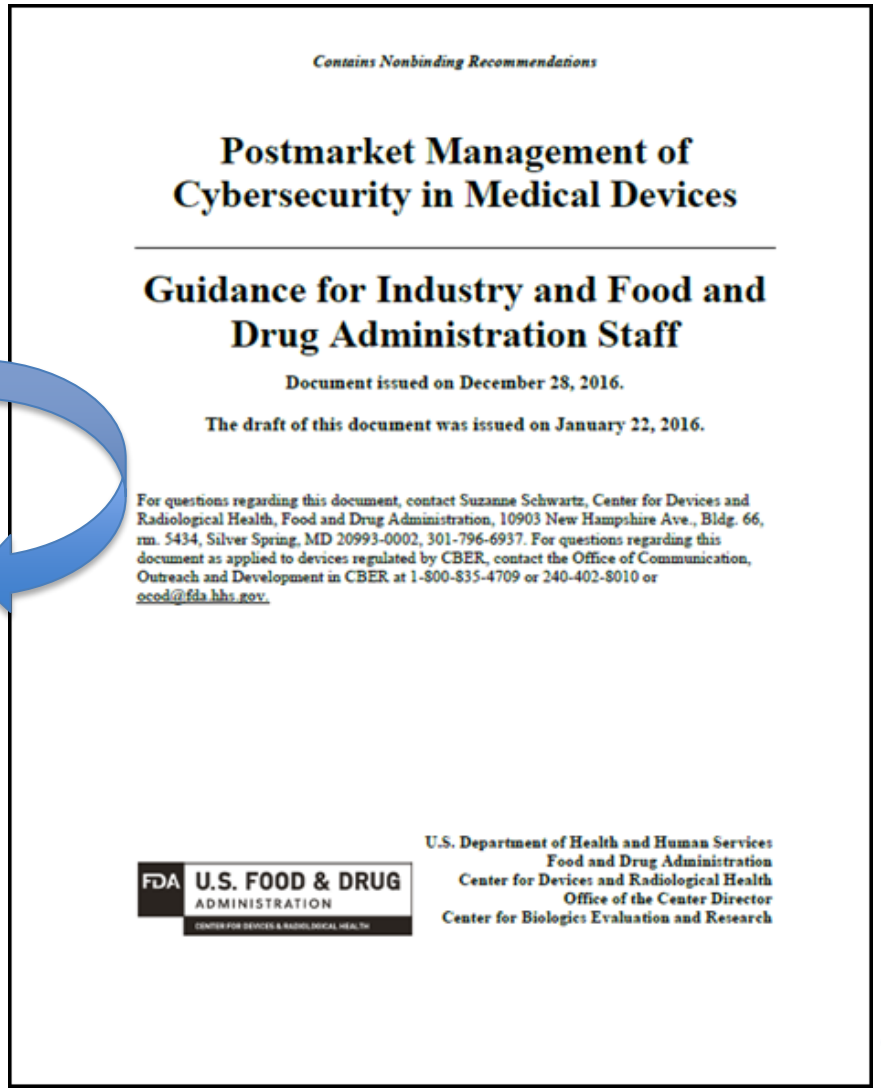
For questions about this document, contact Suzanne Schwartz, Office of the Center Director at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010.

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

FDA 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

1



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.

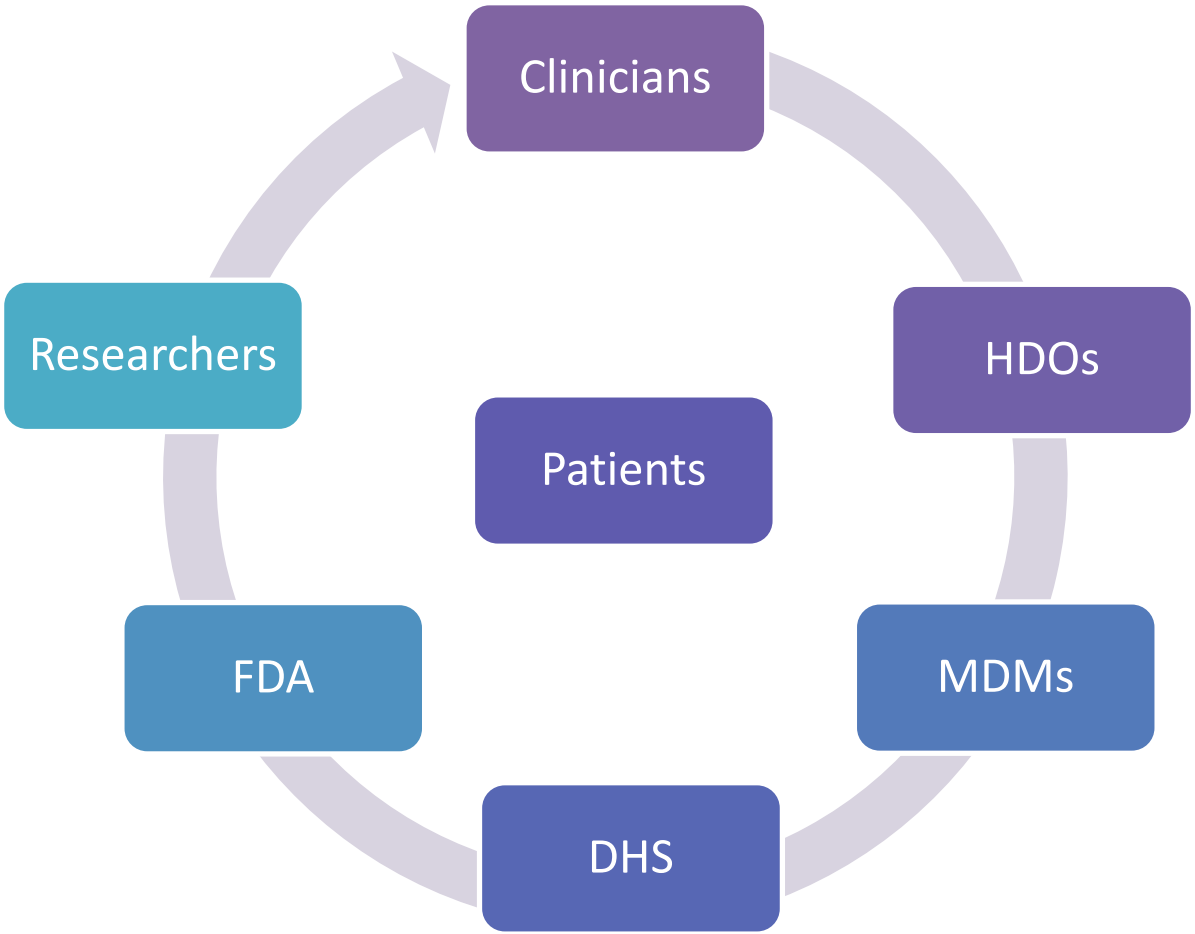
For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by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

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 Cybersecurity Safety Communications and Disclosures

The FDA is not aware of any reports of patient injuries or deaths associated with cybersecurity incidents, nor are we aware that any specific devices or systems in clinical use have been purposely targeted



Medical device cybersecurity is a shared responsibility

FDA contacts:

Suzanne.Schwartz@fda.hhs.gov
Seth.Carmody@fda.hhs.gov
Aftin.Ross@fda.hhs.gov

Or email the team:

CyberMed@fda.hhs.gov

Visit the FDA Cybersecurity Webpage:

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