MEDICAL DEVICE PREMARKET GUIDANCE DRAFT OVERVIEW

SETH D CARMODY, PHD, HCISPP

CDRH / FDA

FDA WORKSHOP

JANUARY 29-30, 2019

2018 Premarket Draft Guidance: Revision Background

- New guidance is needed as medical device cybersecurity continues to evolve
- Changes proposed to the guidance based on lessons learned from routine vulnerability management, response activities, engaging stakeholders including working with manufacturers pre- and post-market.
- Examples of recent threats:
  - Malware/ransomware attacks, e.g., WannaCry, notPetya, Meltdown and Spectre

Revision Approach

- Leveraged the 2014 premarket guidance document
  - Kept alignment with NIST 5 core functions
  - Similar structure
  - Maintained focus on documentation related to requirements of the QSR (21 CFR Part 820)

- Provided additional granularity to help manufacturers implement cybersecurity in the premarket setting
  - Expanded on maintaining properties of authenticity, availability, integrity, and confidentiality through design, risk management, and labeling
  - Labeling grounded in statutory and regulatory requirements; for example:
    - Adequate directions for use, 21 CFR 801.5
    - For prescription devices, 21 CFR 801.109(c)

What’s New

- Designing trustworthy devices
- Preventing multi-patient attacks
- Tiering system – information to be provided in premarket submission is geared to level of risk:
  - Tier 1 – higher cybersecurity risk
  - Tier 2 – lower cybersecurity risk
- Cybersecurity Bill of Materials
- System level threat models

Tier Criteria

Tier 1 "Higher Risk"

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

- 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
- 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 Risk"

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

Tiers Drive Submission Content

- For Tier 1 devices documentation should demonstrate how the device design and risk assessment incorporate the cybersecurity design controls described in the guidance.
- For Tier 2 devices documentation should demonstrate through risk-based rationales why certain cybersecurity design controls are not necessary

- Submitted documentation may include the demonstration of comparable and/or additional cybersecurity design controls that may not be described in the guidance.
- We recommend industry utilize the FDA presubmission process to discuss design considerations for meeting adequacy of cybersecurity risk management throughout the device life-cycle.

Medical device cybersecurity is a shared responsibility

Your input is important to us, please submit comments to the Docket!

https://www.regulations.gov/document?D=FDA-2018-D-3443-0001

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

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