Assessing the Current Regulatory Framework for Medical Device Cybersecurity

Ngoctran Tran
PharmD Candidate, Class of 2023
M.S. Candidate in Regulatory Science, Class of 2023

Advisor: Eunjoo Pacifici, PharmD, PhD
Overview

1. Background
2. Research Question
3. Methods
4. Results
5. Conclusions
Background

Definition of Medical Device
Section 201(h) of the Food, Drug, and Cosmetics Act

Definition of Cybersecurity
"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"

Consequences of Cybersecurity Breaches
- Compromised device functionality
- Loss of data
- Exposure of other connected devices or networks to security threats

Stakeholders
- Health care facilities
- Medical providers
- Patients
- Manufacturers
Vulnerable Systems

Software that do not meet the definition of a medical device but supports these devices

- Hospital networks
- EHRs/EMRs
- Mobile devices
- Cloud services

Devices capable of connecting to another device, portable media, internet, or other network

- Implantables
- Wearables
- Dialysis machines
Research Questions

What are the areas of weakness in the current regulatory framework for medical device cybersecurity?
And are those needs being addressed?
Objectives

1. Understanding the current regulatory framework for medical device cybersecurity
2. Identifying weaknesses in that framework
3. Assessing whether or not those needs are being addressed
Step 1
Reviewed the following:
- FDA
  - Guidances
  - Yearly budget justifications
  - Advisory committee meetings
- HHS research reports
- Journal articles
- News articles

Step 2
Identified points of weaknesses in the regulatory framework

Step 3
Verified if FDA has addressed those weaknesses
Results

More Common

Healthcare organizations
- For this year,
  - 82 incidents worldwide
  - 48 incidents in U.S.
- Examples:
  - Scripps Health System
  - CaptureRx healthcare service

Less Common

Implantable/wearable medical devices
- 2011: Initial awareness—insulin pumps hacking demo
- 2013: 1st FDA safety communication
- 2017: 1st FDA warning letter and recall
- Since 2013–present:
  - 11 safety communications
  - 5 recalls
  - No patient injuries or deaths
## Weaknesses

- Inadequate integration of cybersecurity into the overall premarket review process
- "Refuse-To-Accept" checklist
- "Smart" checklist

## Recommendations

- Pre-submission meetings
- Cybersecurity documentation criterion
- Cybersecurity element

## Premarket Guidance

- Inadequate integration of cybersecurity into the overall premarket review process
- "Refuse-To-Accept" checklist
- "Smart" checklist

## Postmarket Guidance

- Inadequate processes that fail to address cybersecurity compromises
- Emergency response

- Continually access risks and update plans/strategies
- Establish written procedures and practices
- Formal agreement with agency partners
- Establish recall procedures
Current FDA Perspective

Kevin Fu, Director of Medical Device Cybersecurity, CDRH

- Device unavailability
- Threats e.g., ransomware
- Legacy outdated software
- Need for threat models during the early design

FDA FY21 Budget Justification

- No legal requirement for manufacturers to address cybersecurity

Plans/legislative proposals

- Requiring
  - Updates and Patches
  - Cybersecurity bill of materials (CBOM)
- Updating premarket guidance

FDA FY22 Budget Justification

- Includes funding for cybersecurity initiatives

Plans

- Communicating with patients
- Threat modeling
- Assessing threat severity
- Updating premarket guidance
Next Steps

- Review literature that identify weaknesses
- Continue reviewing FDA guidances
- Verify whether prior FDA proposals have been implemented
References


Thank You!

Contact Information:
Ngoctran Tran
nttran@usc.edu