सत्यमेव जयते
Ministry of Health & Family Welfare
Government of India

AHWP
Asian Harmonization Working Party
WORKING TOWARDS MEDICAL DEVICE HARMONIZATION IN ASIA

CENTRAL DRUGS STANDARD CONTROL ORGANIZATION
सत्यमेव जयते
MINISTRY OF HEALTH, GOVERNMENT OF INDIA

1927-2017
FICCI
@90

22nd Asian Harmonization Working Party Annual Meeting

MAKE IN INDIA

4-8 December, 2017 I New Delhi

MAKE IN INDIA

सत्यमेव जयते
Ministry of Health & Family Welfare
Government of India

AHWP
Asian Harmonization Working Party
WORKING TOWARDS MEDICAL DEVICE HARMONIZATION IN ASIA

CENTRAL DRUGS STANDARD CONTROL ORGANIZATION
सत्यमेव जयते
MINISTRY OF HEALTH, GOVERNMENT OF INDIA

1927-2017
FICCI
@90

Post Market Considerations for Digital Healthcare

Prevention strategies for Medical Device Manufacturer

John Ramesh, MD (**TUV Rheinland Oman**)
New Delhi, December 2017

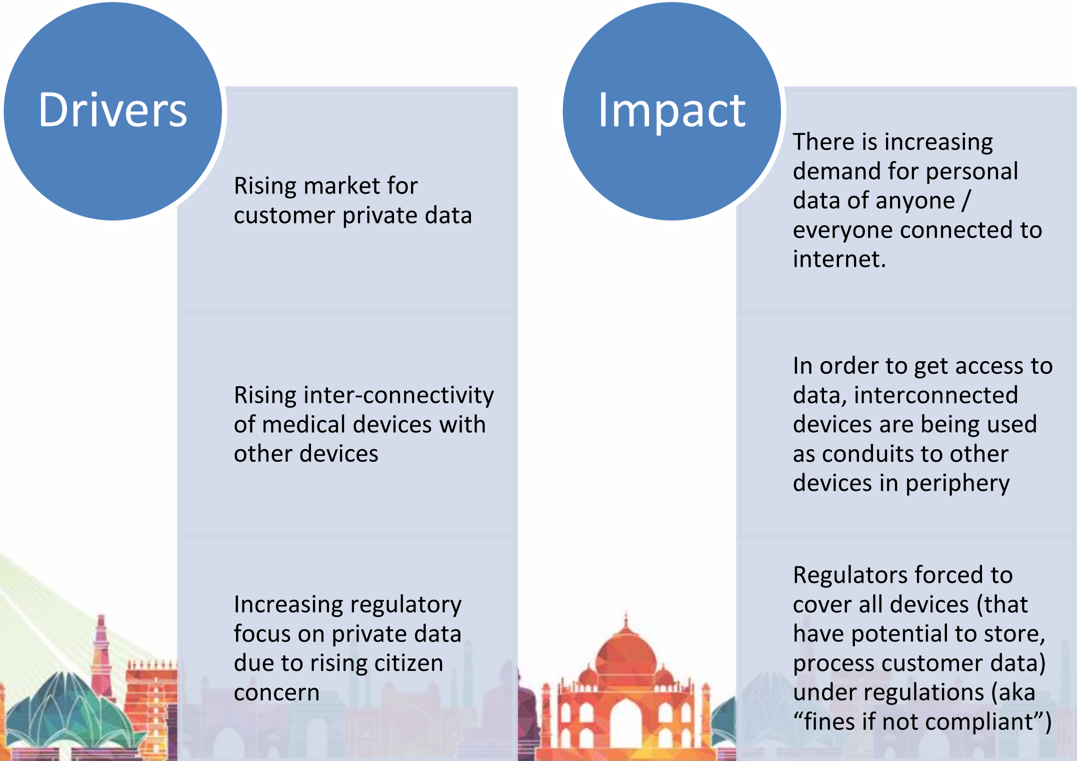
Introduction

John Ramesh, Managing Director & Regional Business Field Manager – ICT & Business Solutions, TUV Rheinland. More than two decades of experience in strategies for Digital Solutions and Cyber Security. With a Post Graduate in Information Systems from India, he's a dynamic leader with very strong expertise in Cyber Security Domain be it Technical, functional or management.

He has hands on experience in the area of Cyber Security for Medical Devices. Further, he's a Technical Committee Member with iHIS Singapore in writing Technical Reference (TR) for Medical Device Security.

WHY ARE WE STILL HERE
JUST TO SUFFER?

Why is FDA concerned about Cybersecurity?



Drivers

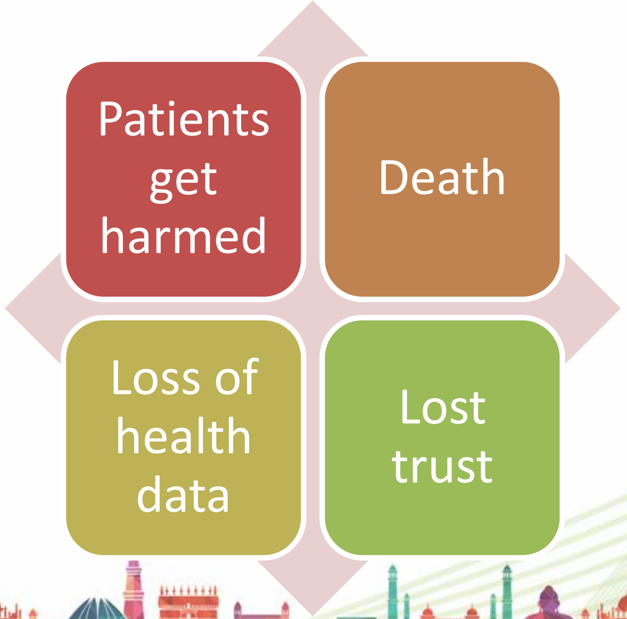
- Rising market for customer private data
- Rising inter-connectivity of medical devices with other devices
- Increasing regulatory focus on private data due to rising citizen concern

Impact

- There is increasing demand for personal data of anyone / everyone connected to internet.
- In order to get access to data, interconnected devices are being used as conduits to other devices in periphery
- Regulators forced to cover all devices (that have potential to store, process customer data) under regulations (aka “fines if not compliant”)

Why is FDA concerned about Cybersecurity?

- If a medical device gets hacked into…



Patients get harmed

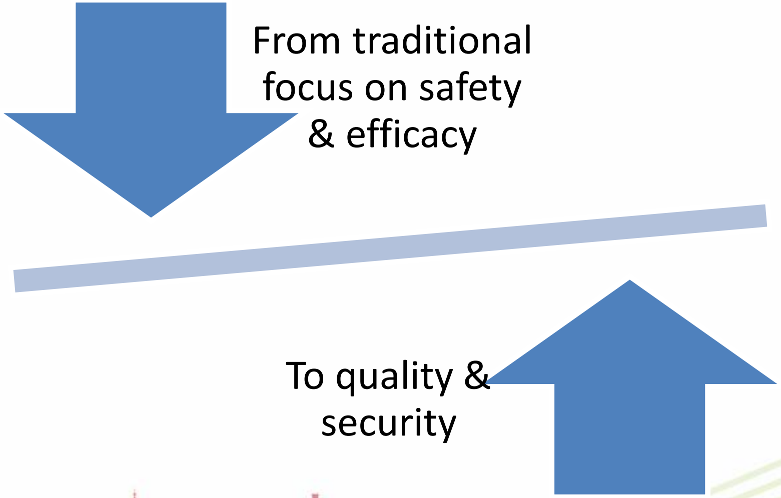
Death

Loss of health data

Lost trust

FDA has also shifted the way it thinks about cybersecurity

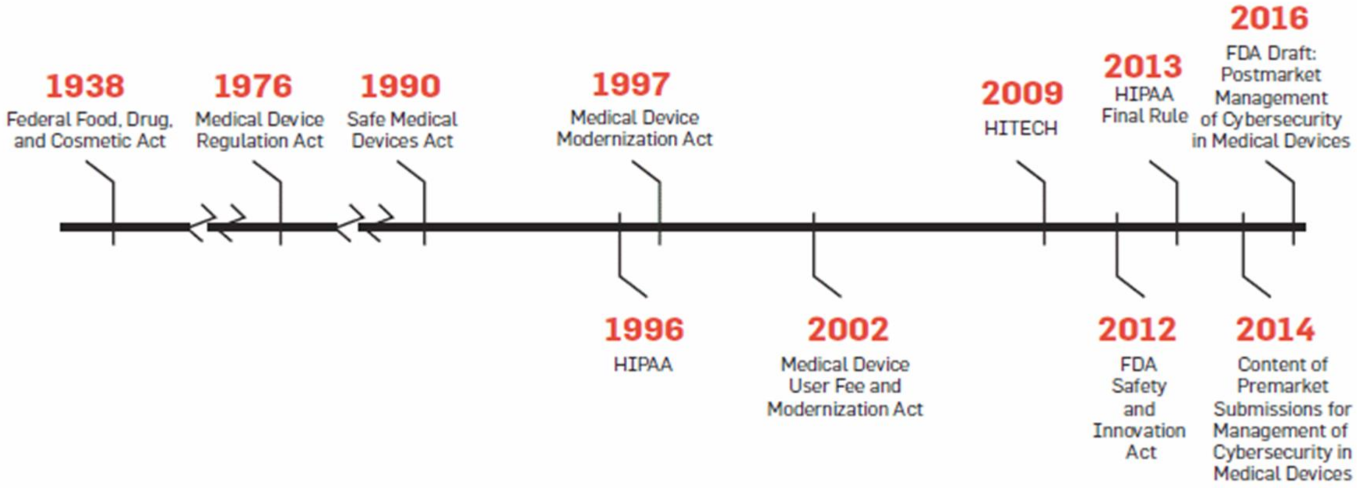
- To reflect the changes in the way industry and customer demands are shaping up …



From traditional focus on safety & efficacy

To quality & security

But Rome wasn't built in a day …



1938 Federal Food, Drug, and Cosmetic Act

1976 Medical Device Regulation Act

1990 Safe Medical Devices Act

1996 HIPAA

1997 Medical Device Modernization Act

2002 Medical Device User Fee and Modernization Act

2009 HITECH

2012 FDA Safety and Innovation Act

2013 HIPAA Final Rule

2014 Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

2016 FDA Draft: Postmarket Management of Cybersecurity in Medical Devices

So what does FDA asks MDM’s, post-market?

1. Implement comprehensive cybersecurity risk management programs and documentation consistent with
   - □ Quality System Regulation (21 CFR Code of Federal Regulations part 820)
   - □ Complaint handling (21 CFR 820.198)
   - □ Quality Audit (21 CFR 820.22)
   - □ Corrective and Preventive action (21 CFR 820.100)
   - □ Software validation and risk analysis (21 CFR 820.30(g))
   - □ Servicing (21 CFR 820.200)

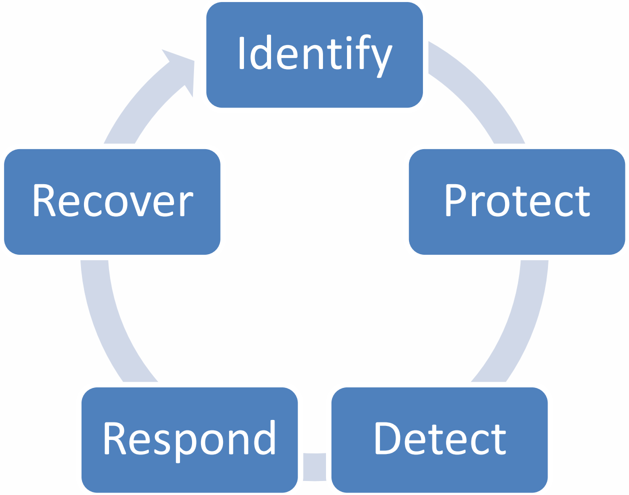
2. Guidelines (to create an effective post-market cybersecurity program) consistent with NIST (National Institute of Standards & Technology, USA) framework for Improving Critical Infrastructure Cybersecurity (Identify, Protect, Detect, Respond, and Recover)

What exactly should we do?

But what exactly should we do?

1. Monitor (cybersecurity information sources for identification of vulnerabilities & risks related to your medical device / components in them)
2. Establish & maintain Secure SDLC, that include (among other things)
   - □ Mechanisms to satisfy the first point above throughout the device's lifecycle (inception to sunset)
   - □ Design verification and validation for software updates and patches that are used to mitigate vulnerabilities, including off-the-shelf software components (if used in your product)
   - □ Use threat modeling to define how to maintain safety and essential performance of the device when a cybersecurity risk materializes
3. Understanding, assessing and detecting presence and impact of a vulnerability;
4. Establishing and communicating processes for vulnerability intake and handling

Create a cybersecurity program in your company that addresses the below elements



Identify

Protect

Detect

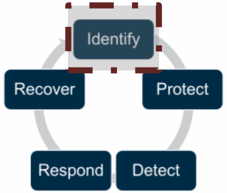
Respond

Recover

1.Maintaining safety and essential performance

❑ Define the safety and essential performance of your medical device if compromised

❑ Use threat modeling as part of your risk assessment process



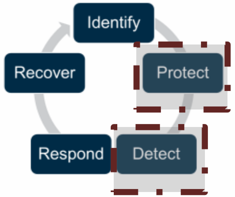
2.Identification of Cybersecurity Signals

❑ Establish a vulnerability disclosure policy / procedure (refer ISO/IEC 29147:2014 & ISO/IEC 30111:2013)

❑ Incidents involving your medical device

❑ Bug bounties?

1. Vulnerability Characterization and Assessment
   - □ Can it be exploited remotely or does it need physical access to device?
   - □ How complicated is this attack? What all does it need to succeed?
   - □ Does the attack need higher privilege to succeed?
   - □ Does it need any action from the user to trigger?
   - □ Is any exploit code present? Does it work?

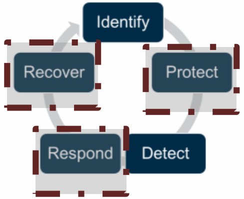


2. Risk Analysis and Threat Modeling
   - □ A procedure for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system

3. Analyze threat sources
4. Incorporate threat detection capability in the medical device (e.g., Microsoft software improvement program)
5. Impact assessment of all devices in a manufacturer’s portfolio

1.Compensating controls’ assessment (Detect / Respond)

□ Build controls inside devices so that they can not only detect threats but can also respond to them (response may also include a note to users that something is wrong with the system and that they should contact the manufacturer)



2.Risk Mitigation of Safety and essential performance

□ No threat should be able to compromise the safety and performance of the medical device (it hurts the trust that the user has on the device)

The sooner you invest in securing your device from ground up (i.e., from requirements) systematically, the more money you can save, not to mention compliance and market differentiation

Questions?