Take Steps Now To Safeguard Your Devices From Cyberattacks

Lauren White
Director, IT and Security

Dan Goldstein
Senior Director, Quality Assurance

MCRA

OMTEC

About Us

Dan Goldstein
Senior Director
of Quality Assurance

Highlights

- *21 years in Medical Device Quality Assurance.*
- *Experience in bringing new devices to market and keeping experienced manufacturers in compliance with FDA and Notified Bodies.*
- *Creates new Quality Systems and updates existing QSs for business and regulatory changes; runs recalls, gap assessments, mock FDA inspections, Form 483 remediations, manufacturing transfers, and Design History Files.*

Lauren White, MBA, CISSP
Director of I.T and Security

Highlights

- *12+ years of I.T and Security experience in healthcare and medical device security.*
- *Experience in the field of Identity and Access Management with expertise in privilege access management, incident response plan development, and contractual review of security language.*
- *Notable success in planning, analysis, and implementation of organizational security initiatives*

OMTEC®

Objectives

To Review:

- Integrate cybersecurity early in the device lifecycle and across the quality system
- The importance of a comprehensive cybersecurity risk management program
- Implement the key recommendations in FDA's draft guidance


Zoll Medical
Siemens PLCs
Trinity Health
MRI Devices
Texas Tech University
Cerebral Inc
Bone & Joint Clinic S.C.
Zoll Medical
Pain Pumps
Anton Paar
Pacemaker
Baptist Medical Center
Atlantic General Hospital
Insulet
Insulin Pump
Cerebral Inc
Cardiac Telemetry
Anton Paar
Insulin Pump
MRI Devices
New Mexico Department of Health
Shields Healthcare Group
Insulin Pump
Zoll Medical
Atlantic General Hospital
Cardiac Telemetry
BD
Insulin Pump
BD
Cerebral Inc
Insulet
Siemens PLCs
Texas Tech University
Bone & Joint Clinic S.C.
Pain Pumps
Medstar Health
Shields Healthcare Group
Siemens PLCs
Pacemaker
Intracardiac defibrillators
Texas Tech University
Insulet
BD
BD
Pacemaker
Anton Paar
Pacemaker
Medstar Health
Insulet
MRI Devices
Trinity Health
Shields Healthcare Group
Anton Paar
Cardiac Telemetry
Medstar Health
Wearable Health Devices
Medstar Health
Intracardiac defibrillators
Trinity Health
Baptist Medical Center
Pain Pumps
Baptist Medical Center
Cerebral Inc
Siemens PLCs
Wearable Health Devices
Anton Paar
New Mexico Department of Health
Intracardiac defibrillators
Atlantic General Hospital

OMTEC

Security in Device Design and Development

- Integration of Security in Quality Management Systems
- Secure Software Development
- Threat Modeling
- Risk Management
- Vulnerability Management Plans
- Maintenance Planning
- Labeling

Refuse to Accept Policy

Plan to track and address vulnerabilities

Procedure for quick patches and updates

Software Bill of Materials

Draft Guidance – April of 2022

Secure Software Development Framework

Prepare the Organization

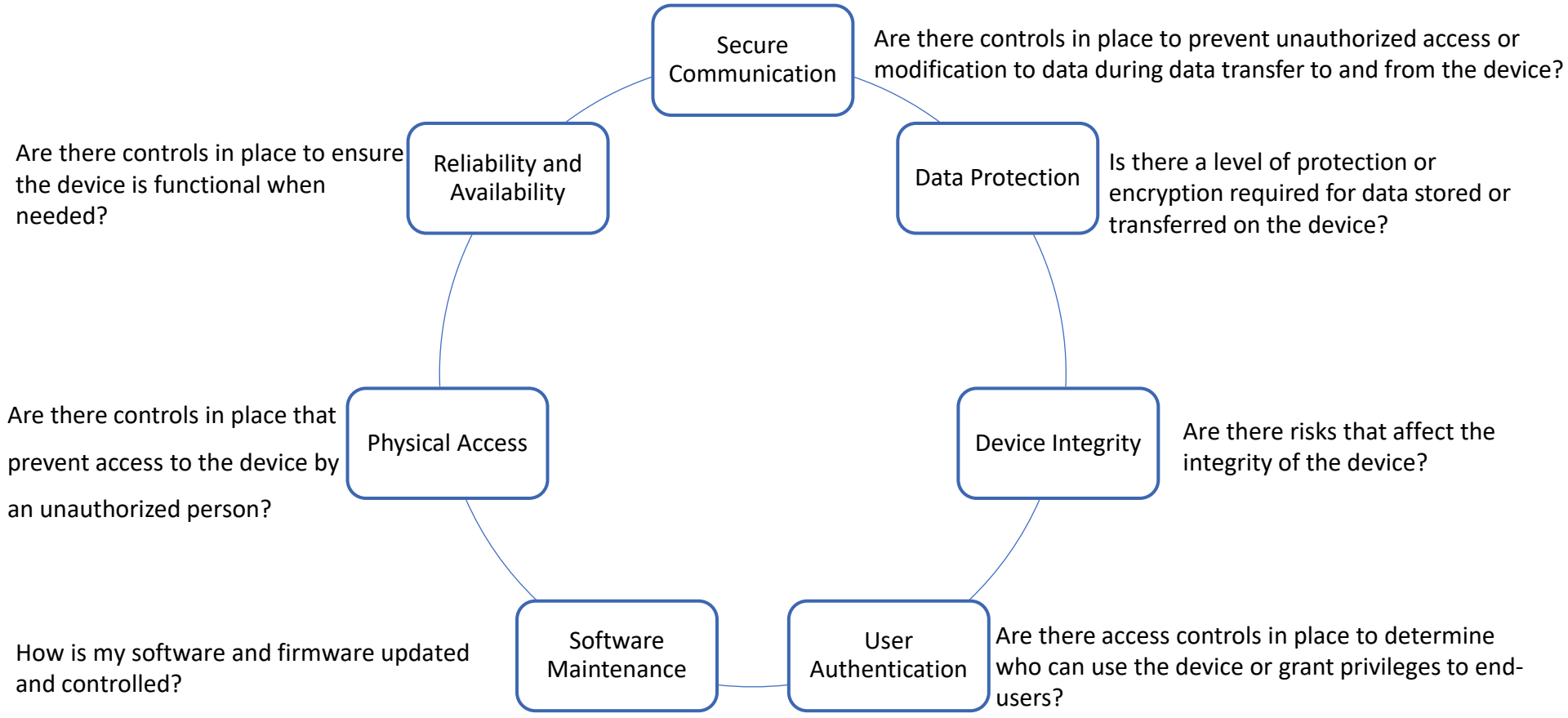
Protect the Software

Produce Well-Secured Software

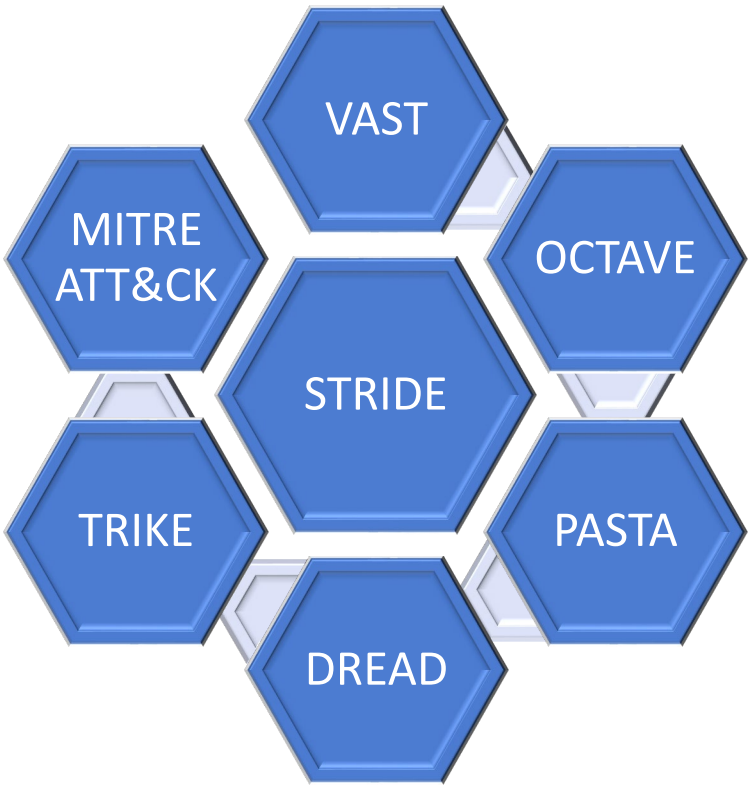
Respond to Vulnerabilities

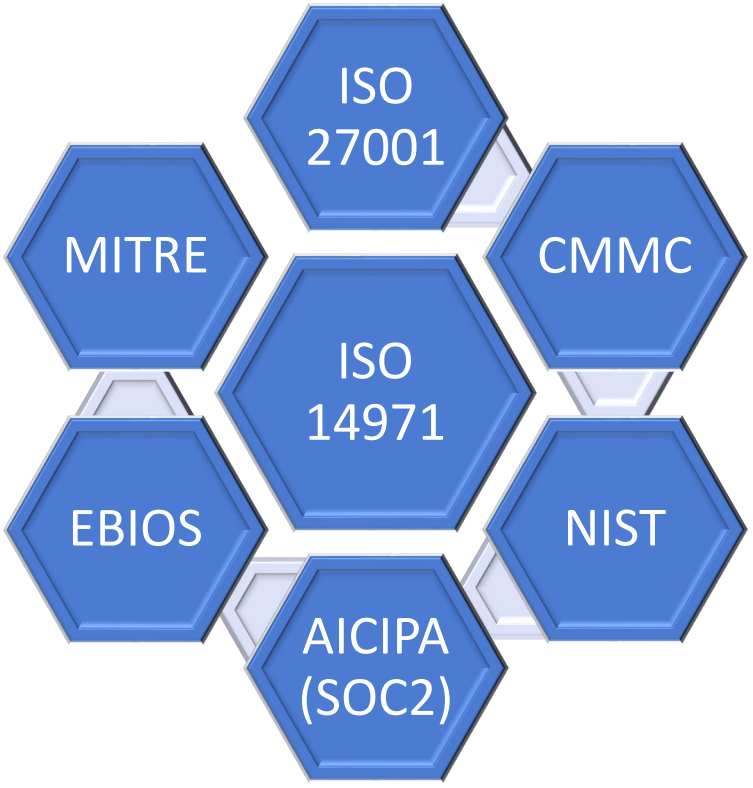
Security by Design:

Device manufacturers should integrate effective cybersecurity plans during the early stages of development and maintain security throughout the device lifecycle.



Threat Modeling and Risk Frameworks





FDA Guidance and Device Security

Pre-Market

- Identification of assets, threats, and vulnerabilities
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients
- Assessment of the likelihood of a threat and of a vulnerability being exploited
- Determination of risk levels, mitigation strategies and assessment of residual risk and risk acceptance.

Post-Market

- Monitoring cybersecurity information sources for identification and detection of vulnerabilities and risk
- Understanding, assessing and detecting presence and impact of a vulnerability
- Establishing and communicating processes for vulnerability intake and handling (CVD)
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from cybersecurity risk
- Deploying mitigations that address cyber early and prior to exploitation
- Including security language in labeling

Future of Security & FDA

- Threat modeling will be key for 510k, DeNovo ,Pre-Market Approval and IDE submissions
- An FDA goal is to have MDMs create consistent & robust documentation of medical device security through Quality management systems, threat modeling, security risk assessments and post-market maintenance.
- It doesn’t have to be complicated; your security documentation should scale with the risk level of the device.
- Holistic Security: Think of the entire lifecycle of the medical device (development, maintenance, end of life).
- Plan, Do, Check, Act (Improve & mature these processes)

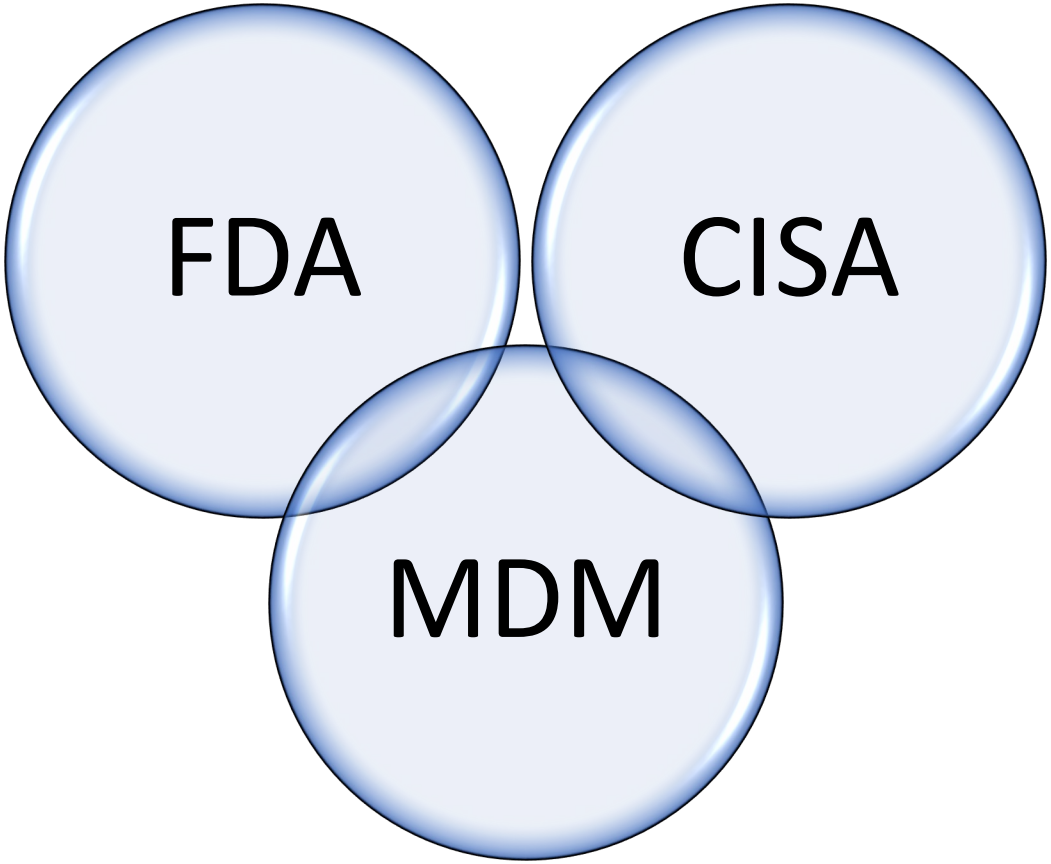
Medical Device RTA Policy: What does it mean?

What is a cyber device?	Includes software validated, installed, or authorized by the sponsor as a device or in a device
	Has the ability to connect to the internet
	Contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats

Refuse to Accept Policy: Core Requirements

Plan	Plan to monitor, identify, and address cybersecurity vulnerabilities and exploits.
Design, develop, and maintain	Design, develop, and maintain processes and procedures pre and post market to ensure the device is cybersecure.
Provide	Provide a software bill of materials, including commercial, open-source, and off-the-shelf software components.
Comply	Comply with such other requirements through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

Refuse to Accept Policy Cont..



Quality System Considerations and Content of Premarket Submissions (Draft Guidance)

- Now the whole QS is in play:
  - Title change from 2014 final guidance and 2018 draft guidance ("Content of Premarket Submissions for Management of Cybersecurity in Medical Devices").
  - 2022 draft guidance specifies: Complaint handling, quality audits, CAPAs, software validation and risk analysis, servicing, production processes, purchasing controls, and the DMR.
  - "Including but not limited to"!

Quality System Considerations and Content of Premarket Submissions (Draft Guidance)

- Secure Project Development Framework (SPDF):
  - Security Risk Management: Distinct from safety risk management under ISO 14971:2019.
  - Security Architecture: Device concepts like design processes, design requirements, and acceptance criteria are applied outside the device.
  - Cybersecurity Testing: Integration of known, non-medical-device cybersecurity testing structures into device design verification and validation (V&V).

Quality System Considerations and Content of Premarket Submissions (Draft Guidance)

- Other changes from previous draft guidance:
  - No more Risk Tiers: All devices start at the same level of review for cybersecurity considerations.
  - No More CBOM: Software Bill of Materials must incorporate cybersecurity.
  - SBOM should incorporate the full software package (homegrown, COTS, and connected)… but it's ***missing*** from the new draft guidance for medical device software (next slide).

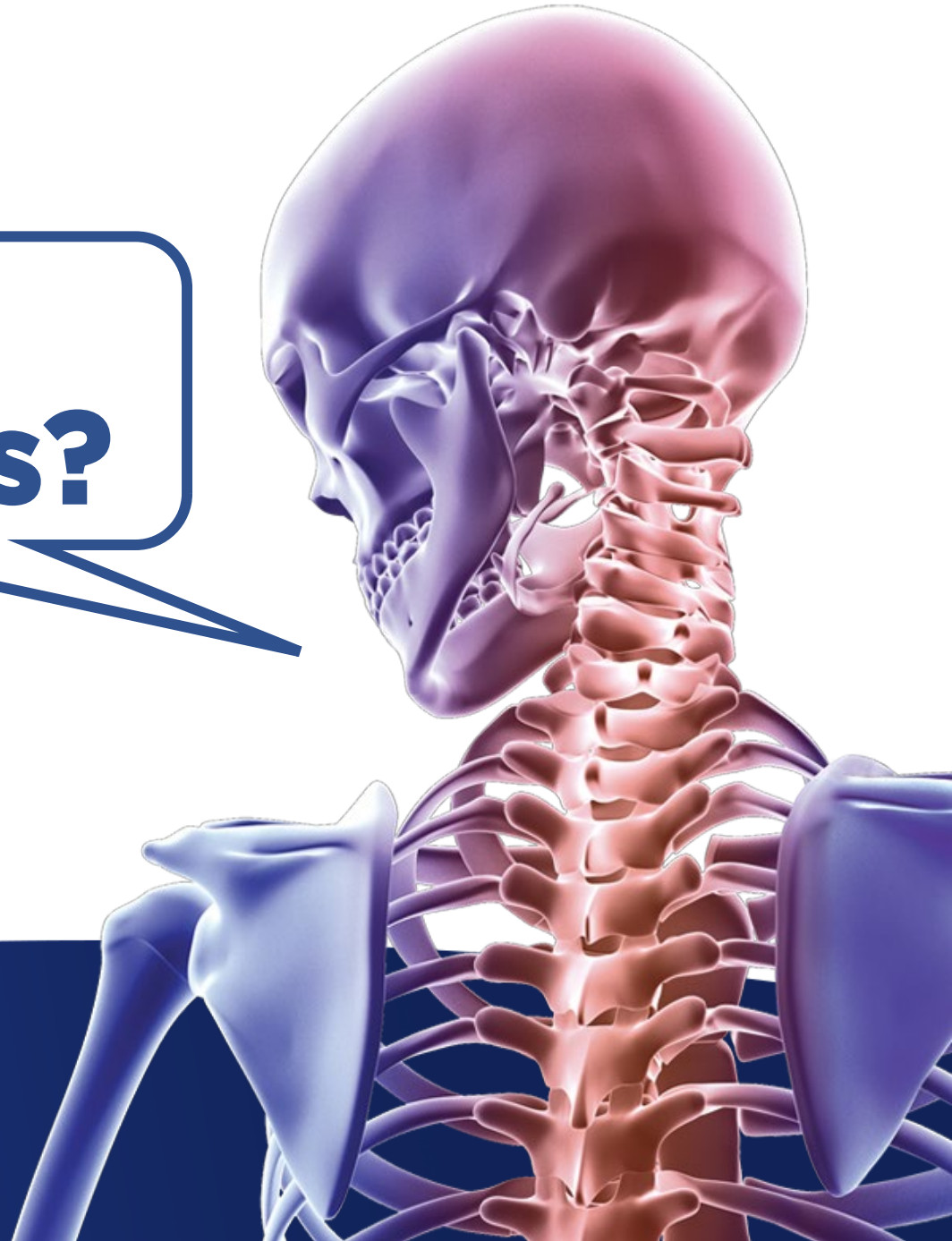
Quality System Considerations and Content of Premarket Submissions (Draft Guidance)

- FDA will apply cybersecurity across the whole QS, just as ISO 13485:2016 applies risk.
- Contemporaneous with, but ***disconnected*** from:
  - Feb. 2022 Proposed Final Rule to replace QSR with QMSR.
  - Nov. 2021 draft guidance, “Content of Premarket Submissions for Device Software Functions.”
  - Sept. 2022 draft guidance, “Computer Software Assurance for Production and Quality System Software.”

Quality System Considerations and Content of Premarket Submissions (Draft Guidance)

- Where to apply the new draft guidance?
  - Across the whole QS.
- ***When*** to apply the new draft guidance to the QS?
  - When the final guidance is released…
  - … even if the draft guidance is applied earlier to device submissions.
- When will FDA examine cybersecurity in the whole QS?
  - During PMA reviews… onsite inspections… also MDSAP?

Any Questions?



OMTEC

Thank You!

Lauren White lwhite@mcra.com
Dan Goldstein
dgoldstein@mcra.com

OMTEC