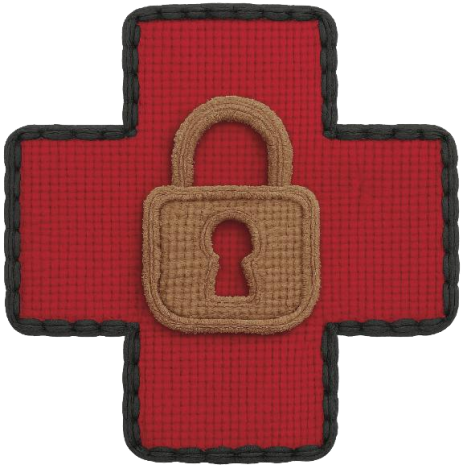
Northeastern University



Medical Device Cybersecurity – Week 7

02/17/2026 – Medical Device Standards

Axel Wirth | Chief Security Strategist | Medcrypt
axel@medcrypt.com

Medical Device Cybersecurity

Overview of applicable standards / guidelines / practices

- General but important thoughts
- FDA Overview (incl. recognized standards)
- Other Global Markets

How Cybersecurity (and Privacy, Safety, …) can be Enforced

- Acts
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Food, Drug & Cosmetics Act
- Regulations (and their interpretation)
  - FDA Quality Management System Regulation (QMSR)
  - FDA Cybersecurity Guidances
- Enforced Standards (through laws)
  - Medical device safety
  - FDA-recognized standards
- Best Practice Standards
  - Not enforced but general accepted and established through evidence
- Audits (against standards, regulation, etc.)
- Best and Leading Practices
  - Whitepapers, technical information
- Procurement mandates
  - U.S. Agencies, South Korea
- User / Consumer Education
  - Product labeling, publications, training

Regulations and Standards: Always Ask

- Is it the right standard / guideline / practice (or regulation, practice, etc.)?
  - E.g., incorrectly applying an IT security standard to product security
- Am I using the standard / guideline / practice correctly (for my case)?
  - E.g., use of an industrial control system standard for medical devices (hint: that may be ok)
- Is the standard / guideline / practice correct
  - E.g., WEP vs WPA
- Does it actually accomplish what it intends?
  - E.g., NIST password guidelines
- Is there a conflict in objectives (e.g., safety vs security)?
  - E.g., FCC disclosure
- Am I focusing on the tool vs. the outcome?
  - E.g., checklist vs real security

Cybersecurity and Privacy - Global Differences

- U.S. has been leading in cybersecurity but also developed evolutionary
  - Complex system of federal and state laws augmented with segment-specific components
  - E.g., no federal privacy law – but HIPAA Privacy & Security Rules for healthcare
  - State laws vary widely, e.g., for residents in general, specific to healthcare, etc.
    see for example here: https://www.datameetsworld.com/us-state-privacy-laws
  - FDA general approach to cybersecurity still rooted in the initial way FDA regulated medicines
- EU: Typically, established by EU followed by country adoption
  - But exceptions exist, e.g., GDPR, MDR
  - MDR/IVDR for medical device safety & effectiveness; recent proposed update created a mess
  - Annex 1 for cybersecurity, interpreted by MDCG-2019-16
  - Others of note:
    - Cyber Resilience Act (CRA) for products with digital elements (Med Dev excluded)
    - Network and Information Security (NIS2): mainly affects operators (incl. hospitals)
    - Radio Equipment Directive (RED): includes secure cyber communications requirements

Medical Device Cybersecurity

Overview of applicable standards / guidelines / practices

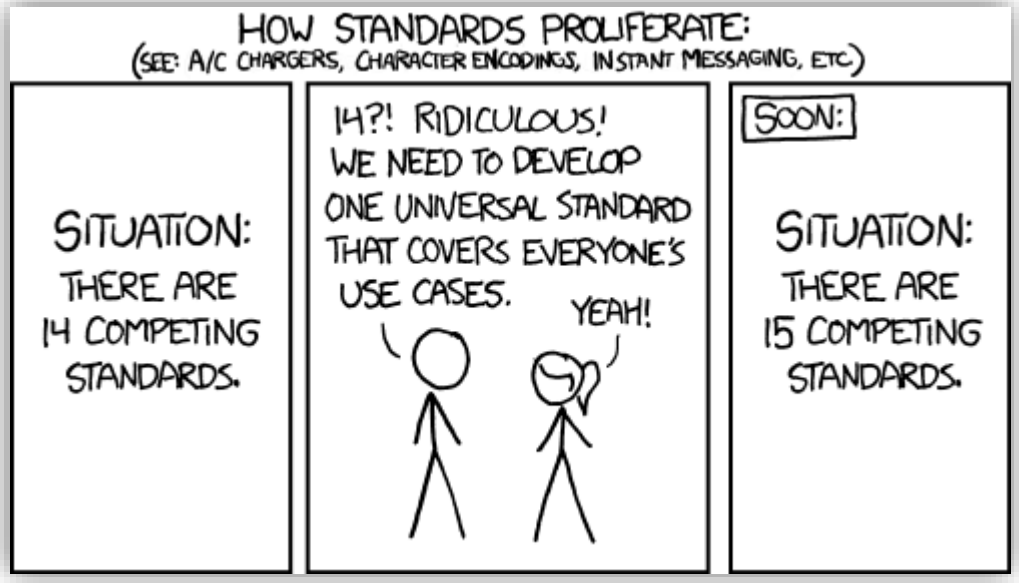
- General but important thoughts
- FDA Overview (incl. recognized standards)
- Other Global Markets

It’s all about Context

It is a complex conglomerate of laws, standards, and practices:

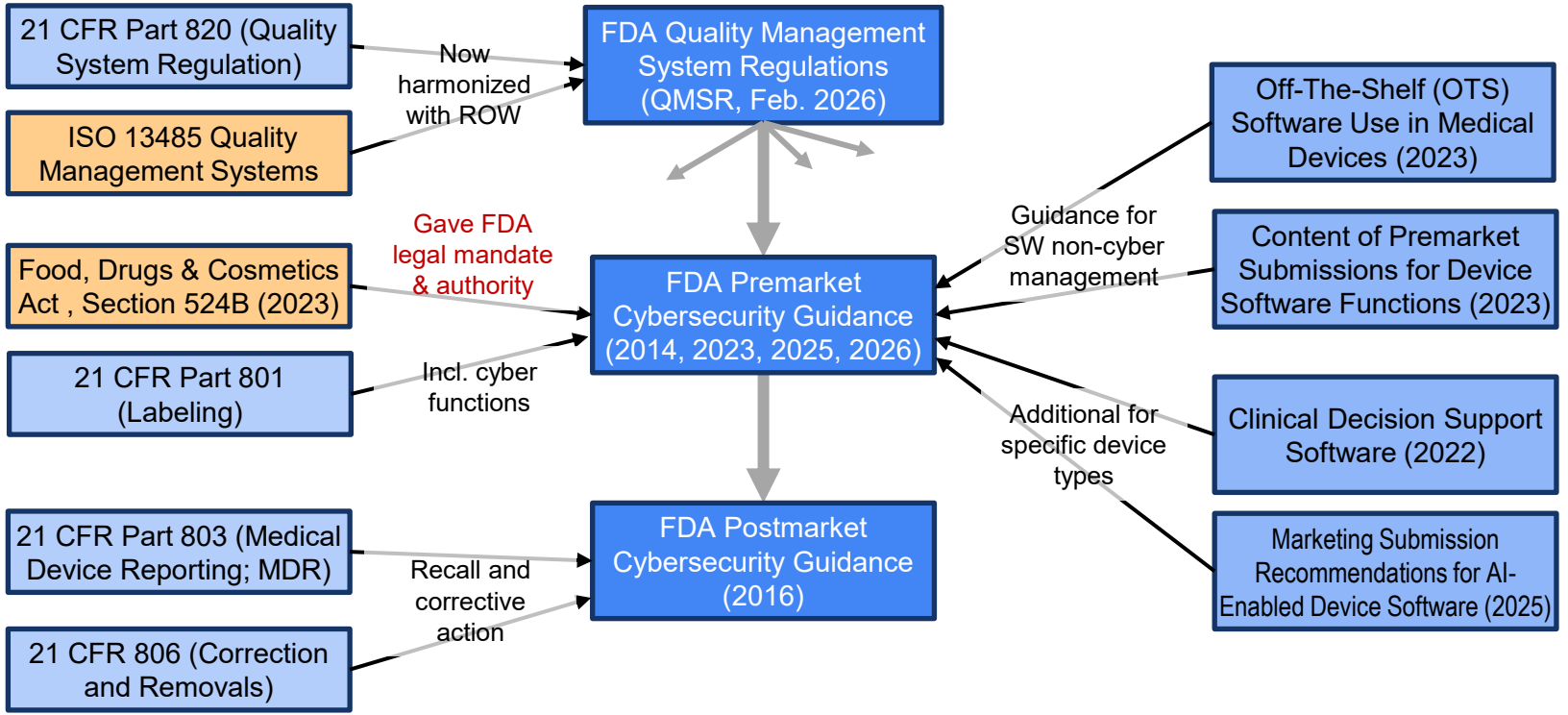
- General software development practices vs. cybersecurity practices
- Cybersecurity is not defined in a vacuum, it is related to and defined by:
  - Safety - FDA
  - Privacy – HHS (HIPAA) and State Laws
  - Useability – FDA
  - Consumer protection – SEC and State Laws
  - Reputation
  - Business needs
  - Risk tolerance

The Confusing World of Standards



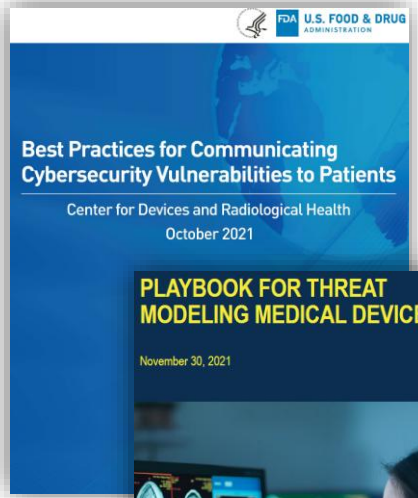
FDA Cybersecurity Regulatory Taxonomy

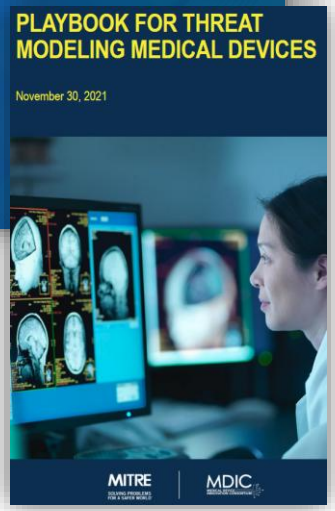
(key cybersecurity elements- of course, there is much more)

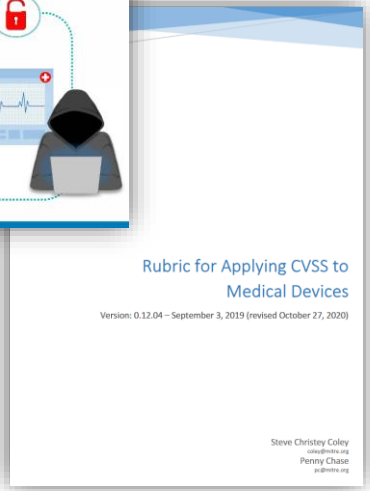


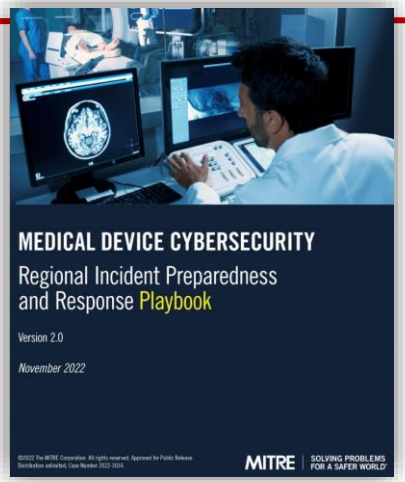
Supporting Best and Leading Practices

(https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity)



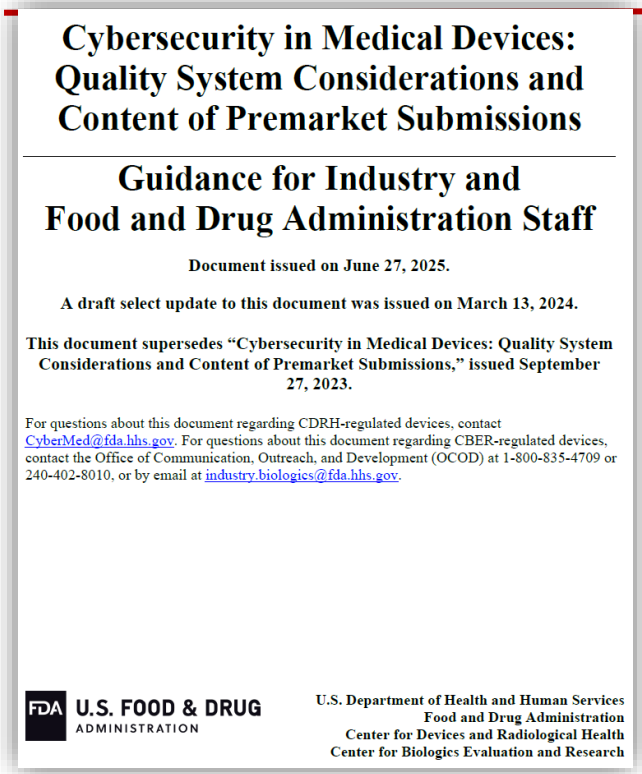






- https://www.fda.gov/media/150144/download
- https://www.fda.gov/media/152608/download
- https://www.mitre.org/sites/default/files/2021-11/pr-18-2208-rubric-for-applying-cvss-to-medical-devices.pdf
- https://www.mitre.org/sites/default/files/2021-11/pr-18-2208-rubric-for-applying-cvss-to-medical-devices.pdf
- https://www.mitre.org/sites/default/files/2022-11/pr-2022-3034-medical-device-cybersecurity-regional-preparedness-response-playbook.pdf

FDA Final Premarket Cybersecurity Guidance Update



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on June 27, 2025.

A draft select update to this document was issued on March 13, 2024.

This document supersedes "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," issued September 27, 2023.

For questions about this document regarding CDRH-regulated devices, contact 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, or by email at industry.biologics@fda.hhs.gov.

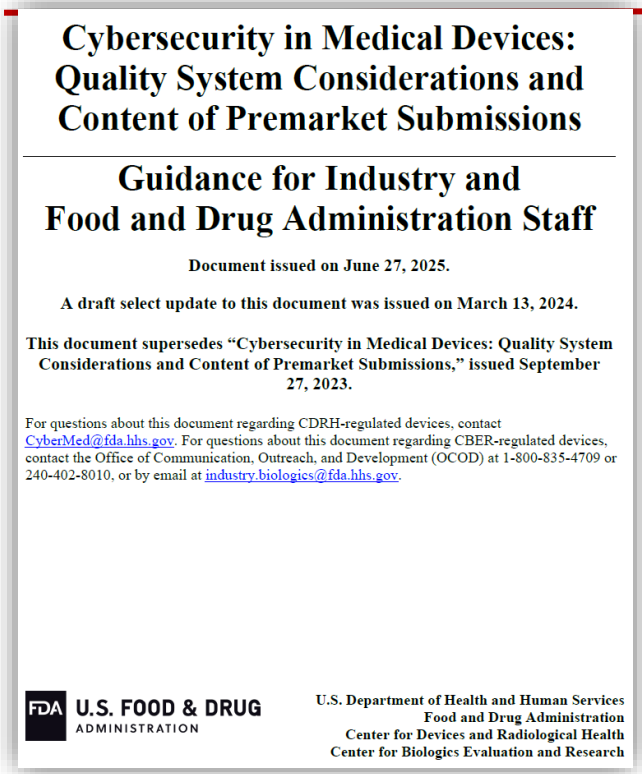
FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

- Released on June, 2025 (replaces 2023 guidance, aligned with QMSR via Feb. 2026 update)
- Secure Development Lifecycle (SDLC):
  - Build secure products
  - Reliably and repeatedly
  - Demonstrate through documentation
- Mainly incorporating Section 524B of the Food Drugs & Cosmetics (FD&C) Act (Oct. 2023) – required capabilities:
  - Vulnerability Monitoring and Management
  - Total Product Lifecycle (TPLC)
  - Software Bill of Materials (SBOM), including commercial, open-source, and off-the-shelf software components
- ► Aligns FDA Guidance with the Law ◄

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

FDA Final Premarket Cybersecurity Guidance Update



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on June 27, 2025.

A draft select update to this document was issued on March 13, 2024.

This document supersedes "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," issued September 27, 2023.

For questions about this document regarding CDRH-regulated devices, contact 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, or by email at industry.biologics@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
Center for Biologics Evaluation and Research

Impact on Postmarket:

- Submit a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits.
- Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address:
  - on a reasonably justified regular cycle, known unacceptable vulnerabilities; and
  - as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;
- Emphasizes EOL / EOS planning and communication.

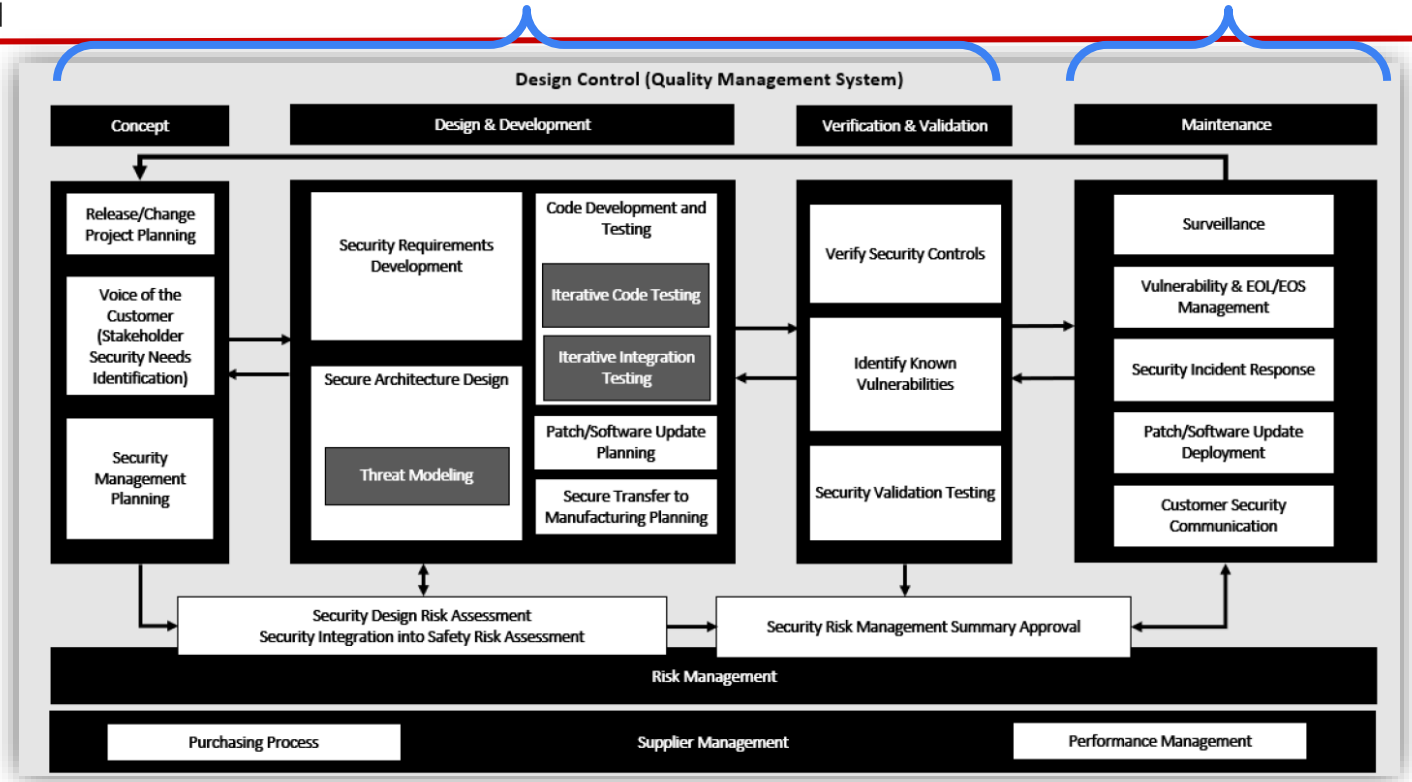
Also see: Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)

Cybersecurity in the Postmarket

Recommended Cybersecurity Measures and Metrics:

- Provide to FDA in Premarket Submissions and PMA annual reports:
  - Percentage of identified vulnerabilities that are updated or patched (defect density);
  - Duration from vulnerability identification to when it is updated or patched; and
  - Duration from when an update or patch is available to complete implementation in devices deployed in the field, to the extent known.
- Note that manufacturers should be tracking these metrics internally even if not submitting to FDA per above

Security Lifecycle – the Big Picture

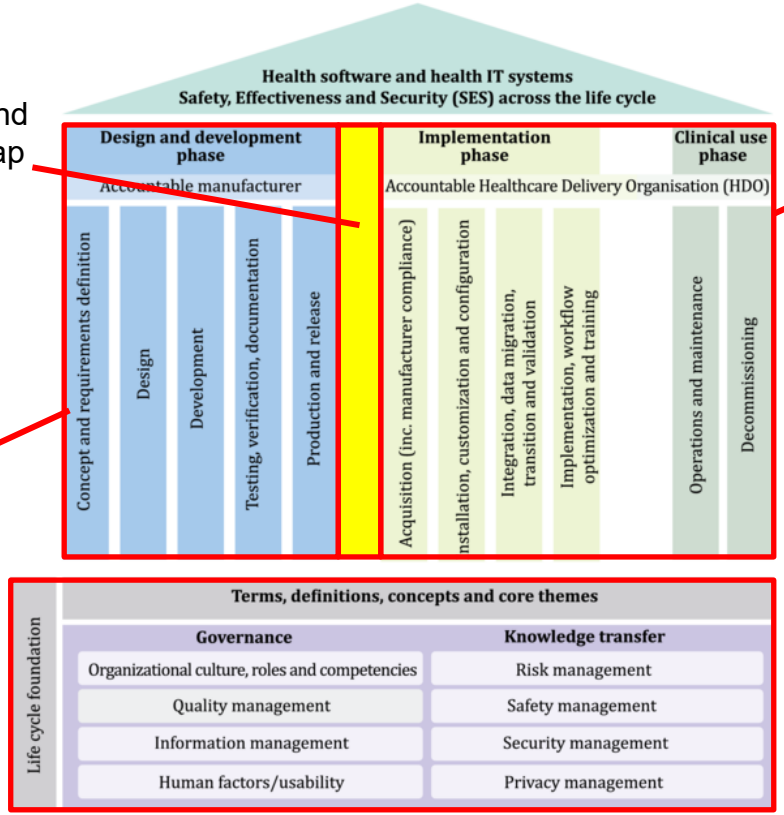


https://healthsectorcouncil.org/jsp2/

Example: ISO 81001-1

Responsibility and accountability gap that we are starting to address

FDA-Regulated

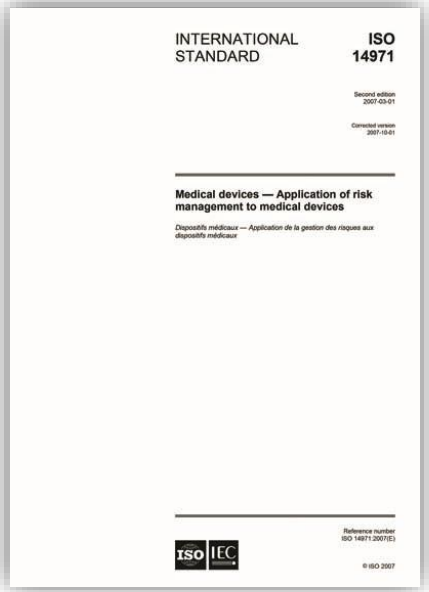


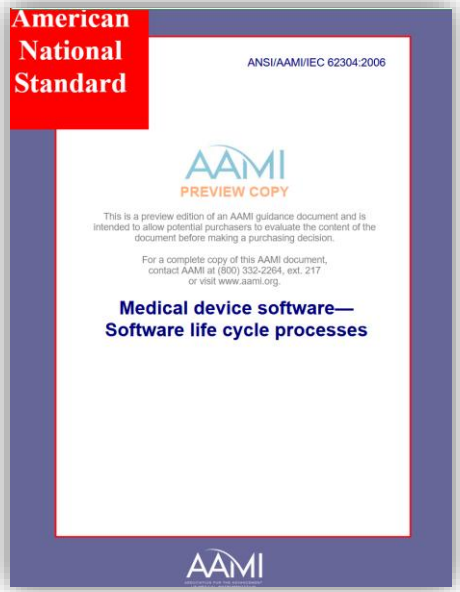
Covered in more detail under ISO/IEC 80001 series

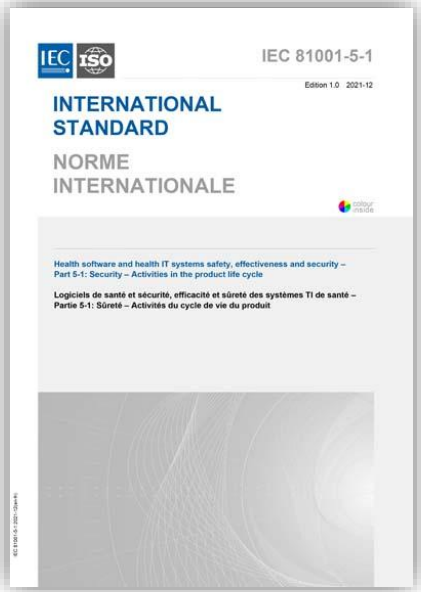
ISO 81001-1:2021 "Health software and health IT systems safety, effectiveness and security, Part 1: Principles and concepts"

Figure 1 — Life cycle framework addressing safety, effectiveness and security of health software and health IT systems

Layered Relationships

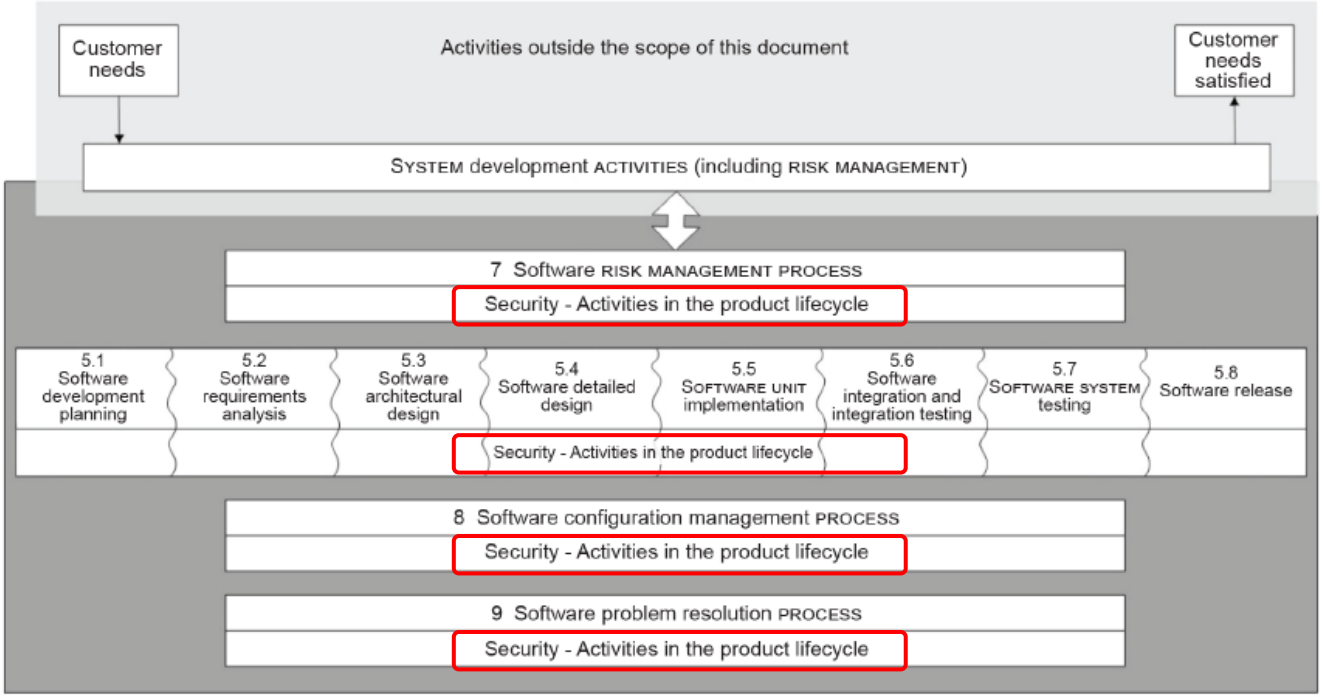






Secure Software Lifecycle

IEC 81001-5-1:2012 “Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle”



The Secure Development Lifecycle (SDLC) Context

- General Premarket Activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches

HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

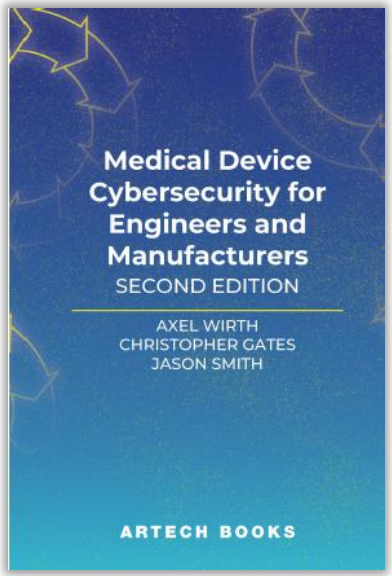
- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

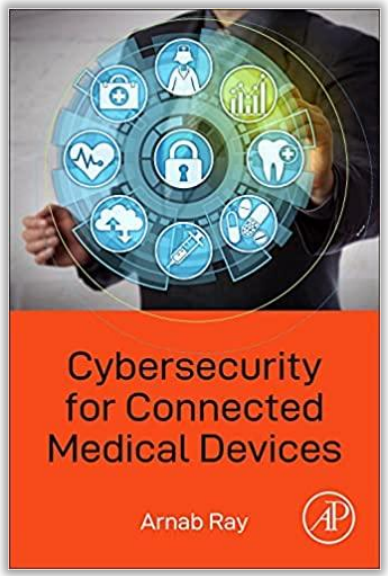
- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

Thank you!

axel@medcrypt.com

General Resources - For Medical Device Manufacturers

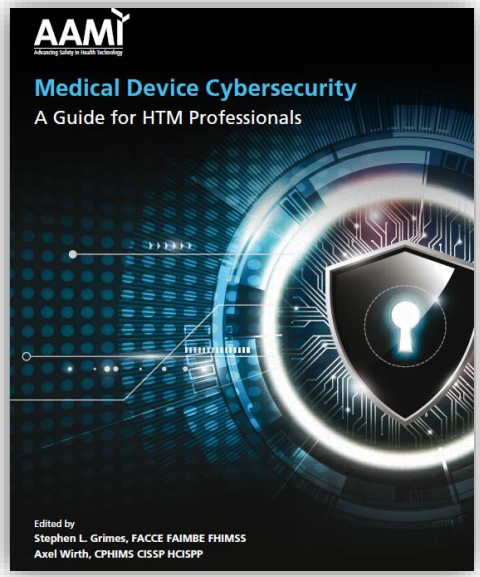




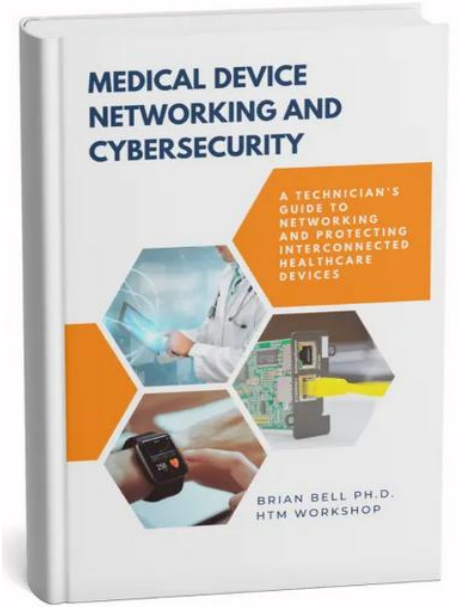
US: https://us.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2416.aspx
UK: https://uk.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2354.aspx

https://www.amazon.com/Cybersecurity-Connected-Medical-Devices-Arnab/dp/0128182628/ref=sr_1_4

General Resources - For Healthcare Delivery Organization

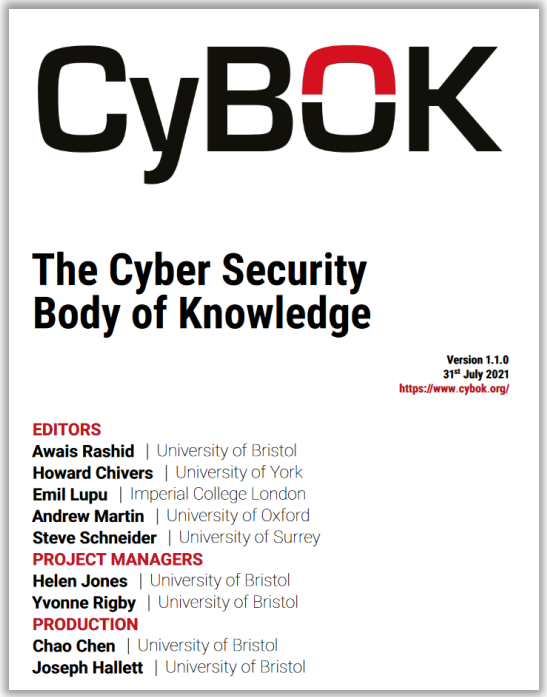


https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA



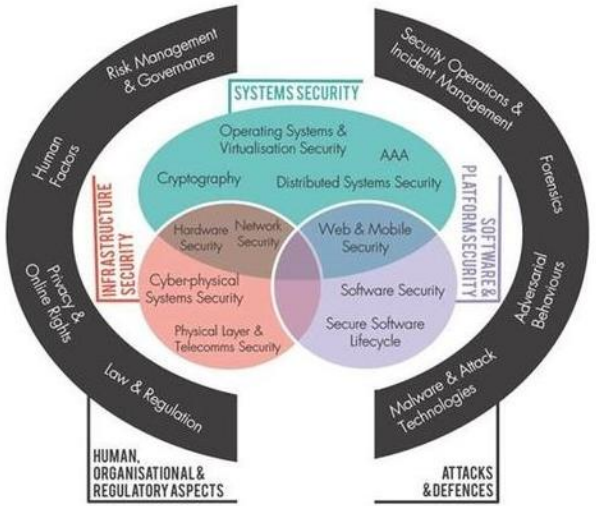
https://htm-workshop.com/shop/medical-device-networking-and-cybersecurity/

General Resources - CyBOK



The Cyber Security Body of Knowledge v1.1,
https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

CyBOK Knowledge Base
https://www.cybok.org/knowledgebase1_1/



Staying Informed on the Day-to-Day

- Security briefs and threat alerts via Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- US Department of Homeland Security's Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT) medical device alerts (ICSMA) https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A96
- Healthcare and Public Sector Highlights - Cybersecurity (via HHS) https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare
- CISA HPH Sector https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector