CYBELLUM

THE MDM'S GUIDE TO THE (CYBERSECURITY REGULATION) GALAXY

Table of Contents

Opening Letter

At Cybellum, we've been talking about the rapid increase of medical device standards and regulations, and now we intend to do something about it!

Not the regulations themselves, but the confusion surrounding them.

That's why we are happy to provide you with a medical regulation guide for the rest of us. Within, you'll find a list of regulations broken down by country or sector to help you navigate which apply and when.

Since this is our first edition, We'd love to hear your feedback about how you use the guide, what we may have missed, and suggestions for future editions. Please let us know at **info@cybellum.com**

United States

Medical Device Guidelines

- Quality System Regulation 21 CFR Part 820
  - Ensure that finished devices will be safe and effective and otherwise in compliance with the Federal Food, Drug, and Cosmetic Act
  - Includes language requiring design controls

Medical Device General Design and Development Guidance and Standards

- Design Control Guidance for Medical Device Manufacturers
  - Elaborates on general design control requirements

Medical Device General Software Design and Development Guidance (with cybersecurity elements)

- General Principles of Software Validation
  - Incorporates software security throughout the software development lifecycle

Note: FDA's Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices is an important software design and development guidance in the U.S. It derives from ANSI/AAMI SW68:2001, but it makes no mention of cybersecurity by inclusion or reference. FDA does, however, list IEC 62304:2006/AMD1:2015 as a recognized consensus standard.

Medical Device Cybersecurity Guidance

- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
  - Structured in question-and-answer format
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
  - Categorizes cybersecurity functions based on NIST's Framework for Improving Critical Infrastructure Cybersecurity
  - References as "recognized consensus standards" CLSI AUTO11-A, AAMI/ANSI/IEC TIR 80001-2-2:2012, IEC TS 62443-1-1, IEC 62443-2-1, and IEC TR62443-3-1
- Postmarket Management of Cybersecurity in Medical Devices
  - Recommends incorporation of NIST's Framework for Improving Critical Infrastructure Cybersecurity
  - References as "recognized consensus standards" ISO/IEC 30111:2013, ISO/IEC 29147:2014, and ANSI/AAMI/ISO 14971:2007/(R)2010

Note: FDA has also published several white papers and discussion papers regarding medical device cybersecurity including 'Best Practices for Communicating Cybersecurity Vulnerabilities to Patients and Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities'

EU

Medical Device Guidelines

- Medical Device Regulation (EU) 2017/745
  - Focuses on implantable medical devices
  - Includes language requiring information security for SiMD, SaMD, and IT systems
- General Data Protection Regulation (GDPR) Regulation (EU) 2016/679
  - Although not specific to medical devices, the impact on cybersecurity and private data within the medical device industry, as it relates to EU residents, is profound.

Medical Device General Software Design and Development Guidance (with cybersecurity elements)

- MDCG 2019-11
  - Also known as: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR
  - An important software guidance in the EU; references IMDRF software classification schemes

Medical Device Cybersecurity Guidance

- MDCG 2019-16 -Guidance on Cybersecurity for medical devices
  - References IMDRF/CYBER WG/N 60 (DRAFT Principles and Practices for Medical Device Cybersecurity)

Cyber Resilience Act

- This is a proposal for a regulation on cybersecurity requirements for products with digital elements that is aimed at bolstering cybersecurity rules to ensure more secure hardware and software products.
- It is important to note that as of 2023, the proposal exempts some medical devices - further clarifications are required

Japan

General device guidelines

- MHLW MO169
  - Ministerial Ordinance on Standards for Manufacturing Control and Quality Control for Medical Devices and In-Vitro Diagnostics
  - Realigns Japanese regulations with global standards
  - Includes product realization requirements consistent with ISO 13485:2016

Medical Device Cybersecurity Guidance

- PSEHB/MDED Notification No. 0724-1 - Guidance on Ensuring Medical Device Cybersecurity
  - Published 24 July 2018
  - References IEC 80001-1:2010, IEC TR 80001-2-2:2012, IEC TR 80001-2-8:2016, and NIST SP800-53

Canada

Medical Device Guideline

- SOR/98-282 Medical Devices Regulations
  - Does not include specific product realization or design control language but requires certification to ISO 13485

Medical Device General Software Design and Development Guidance (with cybersecurity elements)

- Software as a Medical Device (SaMD): Definition and Classification
  - References IMDRF software guidance documents

  Note: Canada recognizes IEC 62304:2006 as an acceptable approach for software development.

Medical Device Cybersecurity Guidance

- Pre-market Requirements for Medical Device Cybersecurity
  - Incorporates full lifecycle cybersecurity guidance
  - References ISO 13485:2016, IEC 62304:2006/AMD1:2015, AAMI TIR57:2016, UL 2900-1:2017, UL 2900-2-1:2018, IEC 8001-1:2010, FDA's Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA's Market Management of Cybersecurity in Medical Devices, ISO 14971, NIST's Framework for Improving Critical Infrastructure Cybersecurity, and NIST's Guide for Conducting Risk Assessments

Australia

Medical device guidelines

- Medical Devices intended for Therapeutic Goods Regulation 2002
  - Part of the Therapeutic Goods act of 1989

Medical Device General Software Design and Development Guidance (with cybersecurity elements)

- Software as a Medical Device (SaMD): Definition and Classification
  - References IMDRF software guidance documents

  Note: Canada recognizes IEC 62304:2006 as an acceptable approach for software development.

Medical Device Cybersecurity Guidance

- Medical device cybersecurity guidance for industry
  - Notes harmonization with medical device cybersecurity guidance from the U.S. FDA, EU MDCG, and IMDRF

Brazil

Medical device guideline

- RDC No. 665 of 30 March 2022
  - Provides for the Good Manufacturing Practices for Medical Products and In Vitro Diagnostic Products
  - Includes language requiring design control and software maintenance

International

Medical Device Guidelines

- ISO 13485:2016
  - Medical device quality management systems
  - Requirements for regulatory purposes
  - Includes product realization requirements for medical devices and security requirements for records

Medical Device General Design and Development Guidance and Standards

- IEC 60601-1
  - Medical electrical equipment – Part 1: General requirements for basic safety and essential performance
  - Addresses information security as a source of safety risk and as an element of software processes
  - References IEC 62304 as the standard for the software development lifecycle
- IMDRF/GRRP WG/N47
  - Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices
  - References IEC 62304 and specifically calls out the need for cybersecurity protections for SiMD, SaMD, and IT systems

Medical Device General Software Design and Development Standards (with cybersecurity elements)

- IEC 62304:2006/AMD1:2015- Medical device software – Software life cycle processes
  - Includes software security requirements during software requirements definition
- IEC 82304-1:2016- Health software – Part 1: General requirements for product safety
  - Incorporates software security throughout the software-only health software lifecycle

Medical Device General Software Design and Development Guidance (with cybersecurity elements)

- AAMI TIR45: 2012 (R2018) - Technical Information Report Guidance on the use of AGILE practices in the development of medical device software
  - References IEC 62304:2006
- IMDRF/SaMD WG/N23 FINAL: 2015 - Software as a Medical Device (SaMD): Application of Quality Management System
  - Incorporates software security throughout the software development lifecycle

Medical Device (and Broader Healthcare) Cybersecurity Standards

- ISO 27799:2016- Health informatics — Information security management in health using ISO/IEC 27002
  - ISO/TC 215 is chaired by ANSI, which includes U.S. FDA representation
- UL 2900-2-1:2018 - Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems
  - Published 1 September 2017
  - Applies to medical devices, accessories to medical devices and medical device data systems
- IEEE Std 11073-40101-2020 - Health informatics—Device interoperability Part 40101: Foundational—Cybersecurity— Processes for vulnerability assessment
  - Applies to personal health devices and point-of-care devices
  - Defines vulnerability assessment process
- IEEE Std 11073-40102-2020 -Health informatics—Device interoperability Part 40102: Foundational—Cybersecurity— Capabilities for mitigation)
  - Applies to personal health devices and point-of-care devices
  - Defines cybersecurity protection measures for incorporation during software design and development
- IEC 81001-5-1:2021 - Software as a Medical Device (SaMD): Application of Quality Management System
  - Maps cybersecurity activities directly to IEC 62304:2006

Medical Device Cybersecurity Guidance for SDOs and Industry Stakeholders

- IEC/TR 80001-2-2:2012 -Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the communication of medical device security needs, risks and controls
  - TS/SC 62A includes ANSI representation
- AAMI TIR57:2016 - Principles for medical device security – Risk management
  - Working group included U.S. FDA and Department of Veteran Affairs representation
- AAMI/IEC TIR80001-2-8:2016 - Application of risk management for IT networks incorporating medical devices—Part 2-8: Application guidance—Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
  - Working group includes the U.S. FDA representation

- IEC TR 80001-2-9:2017 - Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities
  - Working group includes the U.S. FDA representation
- NIST Special Publication 1800-1 - Securing Electronic Health Records on Mobile Devices
  - Provides detailed technical guidance for EHR cybersecurity on mobile devices
- NIST Special Publication 1800-8 - Securing Wireless Infusion Pumps in Healthcare Delivery Organizations
  - Provides detailed technical guidance for infusion pump cybersecurity
- HSCC Medical Device and Health IT Joint Security Plan
  - HSCC Joint Cybersecurity Working Group includes U.S. FDA representation
- AAMI TIR97:2019 - Principles for medical device security – Postmarket risk management for device manufacturers
  - Working group co-chaired by U.S. FDA representative
- ANSI/NEMA HN 1-2019 - American National Standard – Manufacturer Disclosure Statement for Medical Device Security
  - Maps to IEC TR 80001-2-2:2012, ISO/IEC 27002:2013, and NIST 800-53 r4
- IMDRF/CYBER WG/N60 FINAL:2020 - Principles and Practices for Medical Device Cybersecurity
  - As noted above, IMDRF member countries include regulatory representatives from 11 countries plus Argentina and the WHO as observers
- NIST Special Publication 1800-24 - Security Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector
  - Provides detailed technical guidance for PACS cybersecurity
- Playbook for Threat Modeling Medical Devices (MITRE/MDIC)
  - Published under contract with the U.S. FDA
- HSCC Model Contract-language for Medtech Cybersecurity
  - HSCC Joint Cybersecurity Working Group includes U.S. FDA representation
- Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook (MITRE)
  - Published under contract with the U.S. FDA

General Cybersecurity Standards and Guidance

- NIST Special Publication 800-115 - Technical Guide to Information Security Testing and Assessment
- NIST Special Publication 800-66 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- NIST Special Publication 800-144 -Guidelines on Security and Privacy in Public Cloud Computing
- NIST Special Publication 800-30 - Guide for Conducting Risk Assessments
- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary
- Framework for Improving Critical Infrastructure Cybersecurity (NIST)
  - Establishes a core framework consisting of five framework functions (Identify, Protect, Detect, Respond, and Recover), with categories and subcategories under each function to aid in implementation
- ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure
- NIST Special Publication 800-37 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- ISO/IEC 30111:2019
- NIST Special Publication 800-128 - Guide for Security-Focused Configuration Management of Information Systems
- NIST Special Publication 800-207 - Zero Trust Architecture
- NIST Special Publication 800-53
- NIST Special Publication 800-160, Volume 2 - Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
- NIST Special Publication 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities
- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls
- NIST Special Publication 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Industrial Control Cybersecurity Standards and Guidance for Medical Device Facilities and Operators

- IEC TS 62443-1-1:2009 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models
- IEC TR 62443-3-1:2009 -Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems
- IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
- ISO/IEC 62443-3-3:2013 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- NIST Special Publication 800-82 - Guide to Industrial Control Systems (ICS) Security
- ISO/IEC 62443-4-1:2018 - Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
- ISO/IEC 15408-2:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components
- ISO/IEC 15408-3:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components
- ISO/IEC 15408-4:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities
- ISO/IEC 15408-5:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Predefined packages of security requirements
- ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model

ABOUT CYBELLUM

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Top ten medical device manufacturers trust Cybellum's Product Security Platform to execute and manage the main aspects of their cybersecurity operations across teams, product lines, and business units. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

TO LEARN MORE VISIT **WWW.CYBELLUM.COM**