

Cybersecurity in Medical Devices in 5 mins.

The following summarises the FDA's Cybersecurity in Medical Devices guidance and suggest key areas for QA professionals and auditors to focus on when reviewing regulated medical devices.

Introduction

The FDA's June 2025, updated guidance "**Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions**" outlines how medical device manufacturers should integrate cybersecurity into their quality systems and premarket submissions. It emphasises that cybersecurity is essential to device safety and effectiveness and must be considered throughout the device lifecycle. The update (from 2023) was provided in response to the increasing cybersecurity breaches, the need for a cybersecurity lifecycle approach, increased standardisation of QMS' for medical devices globally** and to include the requirements from section 524B, "Ensuring Cybersecurity if Medical Devices, defined in the March 2023 FD&C act.

The guidance discusses how Quality System deliverables that are relevant for Quality System (QS) regulation compliance can also be used to show how a sponsor or manufacturer is addressing cybersecurity considerations relevant to a device within premarket submissions.

Why: There are on average 15 to 20 medical devices per patient bed in the US (Forescout.com, 2022). Medical devices that connect to networks (e.g., infusion pumps, imaging systems, or home-use monitors) contain vulnerabilities susceptible to cyber threats. For example, an 11 year old boy demonstrated the use of a Bluetooth enabled cuddly toy and a Raspberry Pi computer to access the smart phones of the delegates of a security conference to download phone numbers. (Guardian, May 2017).

Risks posed include falsification (change clinical data or switch off the audit trail), ransom (deny access to records) or identity theft of personal identity information.

The impact of the costs of dealing with Healthcare data breaches averages \$9.8 million. The average time to data breach identification and containment is 258 days (Cost of Data Breach Report, IBM, 2024).

The increasingly interconnected nature of medical devices has demonstrated the importance of addressing cybersecurity risks in device design because of the effects on safety and effectiveness.

How: The rapidly evolving landscape, an increased understanding of emerging threats, and the need for the deployment of mitigations throughout the total product lifecycle (TPLC) warranted an updated, iterative approach to device cybersecurity. A lifecycle approach (embedded in the QMS) to cybersecurity risk management, threat modelling and secure software lifecycle (SLC) practices must be applied to medical devices, in addition to the current risk focus on patient safety.

A key inclusion in the guidance document is section 524B(a) of the updated FD&C Act (2023), any person—including a manufacturer—who submits a premarket application or submission via 510(k), PMA, PDP, De Novo, or HDE for a device classified as a "cyber device" (as defined in section 524B(c)), must include the information required by the FDA to demonstrate that the device meets the cybersecurity requirements outlined in section 524B(b). Section 524B(b) defines a device as meeting the following criteria:

1. it includes software that is validated, installed, or authorized by the sponsor as a device or as part of a device;
2. it has the capability to connect to the internet; and
3. it contains technological features, validated, installed, or authorized by the sponsor, that could be susceptible to cybersecurity threats.

Clauses Relevant to the Quality System

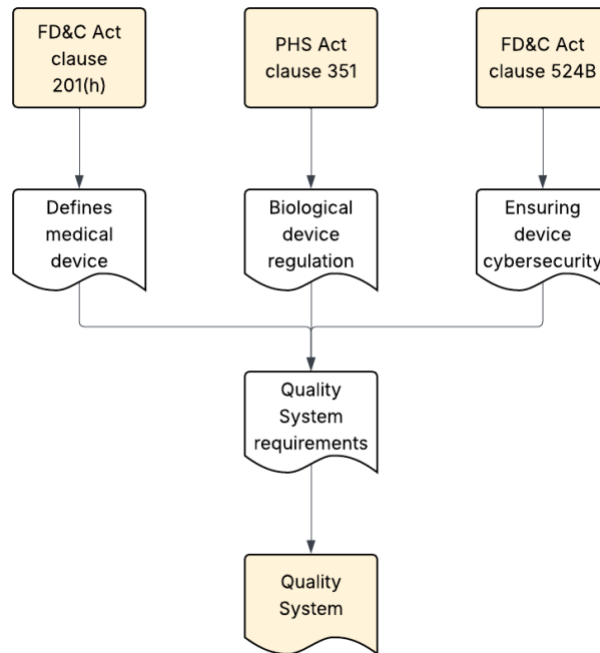


Diagram 1: How the regulations inform a Quality System

Law	Purpose	Example Device Types	Cybersecurity Implications
FD&C Act .201(h)	Defines a <i>medical device</i> under U.S. law. Covers software, hardware, or systems used for diagnosis, treatment, or prevention of disease.	<ul style="list-style-type: none"> - Infusion pumps with Wi-Fi. - Connected insulin pens. - Software as a Medical Device (SaMD). - AI-powered ECG analysers. 	<ul style="list-style-type: none"> - Applies to most medical devices with software/ connectivity. - Must follow Quality System Regulation (QSR). - Requires secure design, threat modelling, and patching of vulnerabilities.
PHS Act .351	Regulates <i>biological products</i> (e.g., vaccines, blood, gene therapies). Relevant when paired with a medical device in combination products.	<ul style="list-style-type: none"> - Autoinjectors for biologics (e.g., adalimumab pens). - Infusion systems for mAbs or gene therapies. - Cold chain monitors. - Wearable drug delivery sensors. 	<ul style="list-style-type: none"> - Devices combined with biologics must address cybersecurity in delivery mechanisms. - Vulnerabilities can affect biologic integrity or safety. - Security controls must protect both drug and device function.
FD&C Act .524B	Establishes cybersecurity requirements for <i>cyber devices</i> (software-based, network-connected, and vulnerable devices). Enforced in premarket review.	<ul style="list-style-type: none"> - Remote patient monitoring tools. - Pacemakers/ neurostimulators with Bluetooth. - Wi-Fi infusion pumps. - MRI systems with remote diagnostics. - Therapy control mobile apps. 	<ul style="list-style-type: none"> - Must provide (post market) monitoring, patching, and disclosure procedures. - Design develop and maintain processes to provide assurance that the device is cyber secure. - Requires Software Bill of Materials “SBOM” (an inventory of software components).

			<ul style="list-style-type: none"> - Modification approach for changes that may/not impact cybersecurity. - Reasonable Assurance of cybersecurity of devices. - FDA can refuse submissions lacking proper cybersecurity documentation
--	--	--	--

Table 1: Summary of clauses relevant to the Quality System

Key Cybersecurity Principles

Section IV of the guide introduces principles relating to device cybersecurity. The guidance focus is on ensuring that devices are designed securely, are capable of mitigating emerging cybersecurity risks throughout the device lifecycle and to provide clarity on the FDA’s recommendations for premarket submission information to address cybersecurity concerns.

Cybersecurity Equals Device Safety: Cybersecurity is not optional. It is a core component of device safety and effectiveness, and the Quality System. Manufacturers must integrate cybersecurity throughout their quality system (lifecycle processes) in accordance with the Quality System Regulation (21 CFR Part 820**). Key elements to attain this is to

- Implement a set of processes to help identify and reduce vulnerabilities across a device lifecycle, from design to decommission.
- Design for Security
- Ensure transparency
- Adequate level of submission documentation (commensurate with risk).

Secure Product Development Framework (SPDF): The FDA encourages manufacturers to implement a SPDF that define the lifecycle processes to manage vulnerabilities across the device lifecycle. (Note: FDA acknowledge other approaches may also allow manufacturers to meet 21 CFR Part 820**).

Section V of the guidance discusses how an SPDF may include the following processes:	
Security Risk Management (Plan and report)	<p>Risk Management is applied throughout the TPLC, and considers:</p> <ul style="list-style-type: none"> • Threat Modelling – identify countermeasures to risks and vulnerabilities. • Cybersecurity Risk Assessment – assess risks and controls for residual risk. • Interoperability Considerations – ability to exchange information through an interface to another device. • Third Party Software Components –inclusion of software component risks for cybersecurity risk assessment. <ul style="list-style-type: none"> ○ Establishment of SBOM – to aid the management of risk within the software ‘stack’. • Security Assessments of Unresolved Anomalies – documented list of anomalies and evaluated impact on safety and effectiveness. • TPLC Security Risk Assessment – risk management throughout the supported device lifecycle.
Security Architecture	Schematics of the to end connectivity of all devices with detailed information for the secure interactions between devices, including:

	<ul style="list-style-type: none"> • Implementation of Security Controls – design requirements and acceptance criteria for security features built into devices. <ul style="list-style-type: none"> ○ Appendix 1 of the guide defines common security control categories and recommendations and implementation guidance for authentication; authorisation; cryptography; code, data and execution integrity; confidentiality; event detection and logging; resiliency and recovery; firmware and software updates. • Security Architecture Views – documentation to help (upgrade/path) impact assessments and associated solution elicitation, including global system view, multi patient harm view, ‘maintainability’ view and security use case view(s).
<p>Cybersecurity Testing</p>	<p>Testing in addition to the ‘standard’ software verification activities:</p> <ul style="list-style-type: none"> • Security requirements verification. • Threat mitigations verification. • Vulnerability testing. • Penetration testing.

Table 2: SDPF key processes

<p>Section V of the guidance discusses Cybersecurity Transparency. Different user groups (manufacturers, service providers, patients) will have different actions to ensure continued cybersecurity. Transparency is achieved from device labelling and the establishment of manufacturer vulnerability management plans.</p>	
<p>Labelling recommendations</p>	<p>Such as:</p> <ul style="list-style-type: none"> • Device instructions. • Product specifications. • Detailed diagrams • List of network ports and interfaces. • Specific guidance for users. • SBOM • Patch download instructions • User notification and event logging. • Device fault tolerance and hardening description. • Backup and restore. • Configuration retention and recovery. • Secure configuration discussion. • Data breach forensic information retention (very important). • End of life/support discussion, such as, (security) decommissioning practices.
<p>Cybersecurity Management Plans</p>	<p>How to identify and communicate vulnerabilities that manifest after a device release. Topics include:</p> <ul style="list-style-type: none"> • Vulnerability monitoring and disclosure. • Patch timelines. • Third party coordination. • Communication plan.

	<ul style="list-style-type: none"> • Post market surveillance. • Routine testing.
--	---

Table 3: Transparency in Cybersecurity

Section VII of the guide relates to cybersecurity information required for cyber devices to support FD&C 524B – see table 1, summary of clauses relevant to the Quality System, above.

What Manufacturers must do

Device manufacturers must establish and follow quality systems (21 CFR Part 820**) to help ensure that their products consistently meet applicable requirements and specifications.

SPDF Software Product Development Framework may be a way to satisfy the QS regulation as it encompasses all aspects of a product lifecycle, including design, development, release, support and decommissioning.

The primary goal of using an SPDF is to manufacture and maintain safe and effective devices.

Risk Management: This is the kernel of the guidance. It is recommended that cybersecurity information is included in submissions based in cybersecurity risks and not on other criteria of level of risk or concern. As a relatively simple system may yield a high security risk. The recommendations of the guide regarding information submitted to FDA are to address cybersecurity risk:

- Conduct threat modelling to identify potential cybersecurity threats.
- Perform cybersecurity risk assessment (in addition to a safety risk assessment).
- Address interoperability risks (e.g., Bluetooth, WiFi).
- Evaluate third-party software and maintain a Software Bill of Materials (SBOM).
- Assess unresolved software anomalies for security implications.
- Maintain lifecycle risk management.

Manufacturers must document the **Security Architecture**, including:

- Security controls (e.g., authentication, encryption, logging).
- Architecture views, including:
 - Global system view.
 - Multi-patient harm view.
 - Ease of maintainability (Updates/Patches) view
 - Security use case view.

These views should show how the device interacts with networks, users, and other systems.

Cybersecurity Testing: Manufacturers must perform and document:

- Security requirements testing.
- Threat mitigation testing.
- Vulnerability testing (e.g., vulnerability assessments penetration testing).
- Static/dynamic code analysis.
- Software composition analysis.

Principles of good documentation practice, and software validation testing should be applied to ensure testing evidence is clear, correct, and repeatable. As with software validation,

where testing has been performed by a third-party service provider, the original evidence should be retained including assessment of such testing.

Edge Cases

It is important to be mindful of edge cases when considering device cybersecurity.

<p>Connectivity to non-medical device components, if a medical device depends on or interacts with non-device IT components, then:</p>	<p>The manufacturer is expected to identify and assess the risk posed by the broader system environment (e.g., interaction with a hospital router).</p> <p>The FDA encourages manufacturers to define system-level cybersecurity expectations in their documentation.</p> <p>This includes:</p> <ul style="list-style-type: none"> • Expected operating environment. • Security controls assumed to be in place (e.g., network segmentation, firewall rules). • Mitigations required at the system/institution level.
<p>While a hospital router itself isn't FDA-regulated, a medical device that depends on it must:</p> <ul style="list-style-type: none"> • Recognize potential cybersecurity vulnerabilities from that interaction. • Document cybersecurity risk mitigations and expectations. • Include this in threat models and security architecture diagrams. <p>For example, a remote patient monitoring system sends vitals from a wearable device over Wi-Fi to a hospital server.</p> <ul style="list-style-type: none"> • The wearable device and its software is fully regulated under FDA cybersecurity guidance. • The router it connects through is not regulated. • The device manufacturer must: <ul style="list-style-type: none"> • Address how the wearable ensures secure transmission. • Assume possible vulnerabilities in the network. • Document mitigations (e.g., TLS encryption, endpoint authentication, port hardening). 	

Table 4: Connectivity to a non-medical device

<p>If a combination product (21 CFR 3.2(e)) includes a cyber device component, then:</p>	<ul style="list-style-type: none"> • The device component must comply with the Quality System Regulation (QSR) under 21 CFR Part 820 • This is enforced via 21 CFR 4.2, which links combination products to applicable device GMPs • Therefore, the cybersecurity expectations outlined in the FDA Cybersecurity Guidance apply to combination products through QSR compliance.
--	--

Table 5: Combination product including a cyber device component.

What Auditors Should Look For

When auditing a medical device manufacturer's cybersecurity practices, consider challenging the following areas of the Quality System:

Area	What to Verify
Design Controls	Cybersecurity is integrated in design controls - 21 CFR Part 820.30: planning, design input, design output, design review, design verification, design validation, design transfer, design changes, design history file.
Risk Management	Robust cybersecurity risk assessments considering both safety <u>and</u> security risks. Cybersecurity risk management plan. Purchasing Controls: Supplier controls address third-party software risks (21 CFR Part 820.50).
Secure SLC	Secure software lifecycle practices, (such as defensive coding, use of OWASP Web Application Security Risks).
SPDF	Secure procedures and controls are in place to cover the device lifecycle.
SBOM	Complete and available, including: <ul style="list-style-type: none"> - all commercial, open source and of the shelf components. - identifier, name, version, supplier and license type. - known vulnerabilities at date of SBOM. -
Testing	Thorough records and outcome, including activities such as, vulnerability testing and penetration testing. Defect Management.
Labelling	Transparent and clear for the device end user. Includes, <ul style="list-style-type: none"> - Device network interface and intended network configurations. - User responsible cybersecurity controls. - Frequency and process of patches. -
Post Market Plan	Includes monitoring, maintenance patching and breach disclosure. Cybersecurity vulnerability monitoring process. Plan for vulnerability disclosure. Patching process. Description of how updates are validated and deployed.

Conclusion

In the ever increasing challenges facing medical devices, the FDA recognizes that medical device cybersecurity is a shared responsibility among interested parties throughout the use environment of the medical device system, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices.

The guidance highlights the FDA's expectation that embedded cybersecurity is critical to device safety and must be addressed throughout the device lifecycle. Key elements are:

- Risk management
- Threat modelling

- Secure lifecycle practices (design, implementation, configuration, monitoring, training).
- Ensuring devices remain safe and secure throughout their lifetime in the face of evolving cyber threats.
- Continuously monitor and mitigate cybersecurity vulnerabilities.

QA professionals must understand how to verify that devices meet these expectations, including not just during design, throughout the product's lifecycle.

Note: "Regulation, 21 CFR Part 820, is to [align more closely with international consensus standards for devices \(89 FR 7496\)](#). This final rule will take effect on February 2, 2026. Once in effect, this rule will withdraw the majority of the current requirements in Part 820 and instead [incorporate by reference the 2016 edition of the International Organization for Standardization \(ISO\) 13485, Medical devices - Quality management systems – Requirements for regulatory purposes, in Part 820](#). As stated in the final rule, the requirements in ISO 13485 are, when taken in totality, substantially similar to the requirements of the current Part 820, providing a similar level of assurance in a firm's quality management system and ability to consistently manufacture devices that are safe and effective and otherwise in compliance with the FD&C Act. When the final rule takes effect, FDA will also update this guidance, including the references to provisions in Part 820 in this guidance to be consistent with the rule." [Cybersecurity in Medical Devices, Quality System Considerations and Content of Premarket Submissions](#).

Authors:

Barry McManus, Principal Consultant, Empowerment Quality Engineering, an IT Quality Consultancy and **John Cheshire**, CSV Consultant, Headway Quality Evolution Ltd, a GxP Quality Consultancy, on behalf of the **RQA IT Committee**.