

The Unowned Risk: Cybersecurity as a Quality Obligation in GxP Environments



A cGMP Consulting White Paper on Closing the Gap Between Security, Data Integrity, and Regulatory Accountability – October 23, 2026

Cybersecurity | Computerized Systems | Data Integrity | Medical Devices

An educational resource for executive and technical leaders in FDA-regulated life sciences.

Executive Summary

Ask most life sciences organizations who owns the security of their GxP systems and the answer comes slowly. IT owns security. Quality owns GxP compliance. The intersection, where a security control is also a data integrity control and a breach is also a regulatory event, is owned by neither with any clarity. That gap has become expensive, because regulators on both sides of the Atlantic now treat cybersecurity as a quality obligation rather than an IT concern.

The regulatory position has moved decisively. For device manufacturers, Section 524B of the Federal Food, Drug, and Cosmetic Act, added by the Consolidated Appropriations Act of 2023 and effective March 29, 2023, made cybersecurity a statutory premarket requirement for cyber devices, and failure to comply is a prohibited act. The FDA has run a refuse-to-accept policy for submissions lacking required cybersecurity information since October 1, 2023. For manufacturers of medicinal products, the draft revision of EU GMP Annex 11 published on July 7, 2025 introduces cybersecurity as a core requirement, with a security chapter addressing patching, penetration testing, firewalls, and removable media controls, alongside

multi-factor authentication for electronic signatures. The finalized Computer Software Assurance guidance addresses cybersecurity evidence within software assurance.

What makes the risk distinctive in regulated environments is that a compromised GxP system produces two failures at once. It is a security incident, requiring technical containment and remediation. It is also a data integrity failure, because the reliability of the records the system holds is now in question, which reaches product disposition, release decisions, and potentially material already distributed. Organizations that handle these consequences through separate incident processes, owned by separate functions, respond to each half of a single event.

This paper examines how cybersecurity became a quality obligation, what the current frameworks require, why the ownership gap persists, and what leaving it open costs. It sets out practices for integrating security evidence into validation, assigning accountability across the IT and quality boundary, and designing incident response that accounts for regulatory obligations alongside technical ones.

Introduction

Cybersecurity entered regulated life sciences as an IT discipline, concerned with protecting infrastructure, and it grew its own vocabulary, methods, and organizational home. Quality assurance developed separately, concerned with product and patient, with its own vocabulary, methods, and home. For years the two domains barely touched in practice, because the systems that mattered to quality were largely isolated and the systems that mattered to security largely did not hold regulated records.

That separation no longer describes the environment. Manufacturing execution systems, laboratory systems, and quality management platforms are networked, frequently cloud-hosted, and hold the records product release depends on. Medical devices themselves connect to networks and to the internet. The systems a security team protects and the systems a quality unit relies upon are now the same systems, and the controls that protect them are simultaneously security controls and data integrity controls.

Regulators recognized this convergence faster than most organizations have. The statutory cybersecurity requirements for cyber devices, the cybersecurity chapter in the Annex 11 draft, and the cybersecurity evidence expectations in software assurance all treat security as an element of quality rather than as an adjacent technical concern. What has not converged, in most organizations, is ownership. Security stays with IT, GxP compliance stays with quality, and the intersection stays a space each function assumes the other manages.

This paper is for the quality, technology, and compliance leaders who have to close that gap, and for the executives who will discover it exists when an incident produces a regulatory problem their incident response process was never designed to handle.

Industry Background

The path that made cybersecurity a quality obligation ran through both the device and medicinal product sectors, arriving at the same place from different starting points.

On the device side, the growing connectivity of medical devices created patient safety risks that were unmistakably within the FDA's remit. A compromised infusion pump or implantable device is a safety problem, not merely a data problem, which made cybersecurity a device safety question and therefore a quality system question. The agency addressed this through guidance connecting cybersecurity to design controls, treating security as an element of device safety and effectiveness rather than as an IT matter. Congress then made the connection statutory. Section 3305 of the Consolidated Appropriations Act of 2023, signed December 29, 2022, amended the Federal Food, Drug, and Cosmetic Act by adding Section 524B, Ensuring Cybersecurity of Devices, effective March 29, 2023.

On the medicinal product side, the path ran through data integrity. As regulators intensified their focus on the reliability of electronic records, the controls that protect record reliability, access control, attribution, protection against unauthorized alteration, turned out to be security controls. A shared login credential is a security weakness and an attributability failure at the same time. An unpatched system that permits unauthorized data modification is a vulnerability and a data integrity risk at the same time. The 2011 Annex 11 addressed access and security in general terms suited to its era; the July 2025 draft revision addresses cybersecurity as a core requirement with a substantial dedicated chapter.

The convergence is now explicit in both frameworks. The finalized Computer Software Assurance guidance addresses cybersecurity evidence as part of establishing confidence in software used in production or the quality system. The Annex 11 draft treats computerized systems as core GMP-controlled assets and aligns with information security frameworks including ISO 27001. For device manufacturers, the cybersecurity guidance was retitled to reference quality management system considerations, reflecting alignment with the Quality Management System Regulation that took effect on February 2, 2026. The regulatory message is consistent: security of regulated systems is a quality matter.

Regulatory Landscape

The requirements differ by sector but converge on the principle that security of regulated systems is a quality obligation.

Section 524B and Cyber Devices

Section 524B of the Federal Food, Drug, and Cosmetic Act, added by Section 3305 of the Consolidated Appropriations Act of 2023 and effective March 29, 2023, establishes statutory cybersecurity requirements for cyber devices. A cyber device is defined as one that includes software validated, installed, or authorized by the sponsor, has the ability to connect to the internet, and contains technological characteristics that could be vulnerable to cybersecurity threats. The sponsor of a premarket submission for a cyber device must submit a plan to monitor, identify, and address postmarket cybersecurity vulnerabilities and exploits including coordinated vulnerability disclosure; design, develop, and maintain processes providing a reasonable assurance that the device and related systems are cybersecure and make available postmarket updates and patches; and provide a software bill of materials including commercial, open source, and off-the-shelf components. Failure to comply with these requirements is a prohibited act under the Act.

FDA Guidance and the Refuse-to-Accept Policy

The FDA issued final guidance addressing cybersecurity in medical devices, quality system considerations, and the content of premarket submissions on June 27, 2025, superseding the September 2023 version and finalizing the draft on Section 524B updates issued in March 2024. A subsequent version retitled to reference quality management system considerations reflects alignment with the QMSR. The guidance addresses the secure product development framework, software bill of materials expectations, and documentation supporting Section 524B obligations, and it references ANSI/AAMI SW96 as a consensus standard for security risk management. The agency has run a refuse-to-accept policy since October 1, 2023, under which submissions for cyber devices lacking required cybersecurity information are not accepted for review. The guidance applies broadly, including to devices for which a premarket submission is not required, and generally to the device constituent part of combination products presenting cybersecurity considerations.

Annex 11 and Cybersecurity as a GMP Requirement

The draft revision of Annex 11, published July 7, 2025 with consultation closing October 7, 2025 and final publication expected mid-2026, expands the annex substantially and introduces cybersecurity as a core requirement. The draft's security chapter addresses patching, penetration testing, firewalls, and removable media controls, and the draft treats computerized systems as core GMP-controlled assets rather than supporting tools. Related provisions require multi-factor authentication for electronic signatures and expand audit trail expectations to include data creation events with immutability requirements. The draft aligns with international frameworks including ISO 27001, PIC/S, GAMP 5, ICH Q9, and ICH Q10.

Computer Software Assurance and Data Integrity

The Computer Software Assurance guidance, finalized September 24, 2025 and updated February 3, 2026, addresses cybersecurity evidence within the risk-based assurance of software used in production or the quality system. Separately, data integrity requirements bear directly on security controls: unique user credentials with individual attribution, restricted administrative privileges, and protection of records against unauthorized alteration are simultaneously security controls and integrity controls. The FDA data integrity guidance, along with MHRA, PIC/S, and WHO guidance, addresses these expectations, and the requirement that records be attributable is not satisfiable where credentials are shared.

The frameworks arrive at the same conclusion from different directions. Device regulation reached cybersecurity through patient safety; medicinal product regulation reached it through data integrity. Both now treat the security of regulated systems as a quality obligation, which means it cannot remain solely an IT responsibility.

Current Industry Challenges

The obstacles here are organizational before they are technical, which is why they persist in organizations with capable security teams and capable quality functions.

The Ownership Gap

The central challenge is that GxP system security falls between two functions and is owned by neither. IT security operates on enterprise frameworks, threat models, and risk appetites that were not designed around regulatory record obligations. Quality operates on regulatory frameworks and does not typically have the technical depth to specify or assess security controls. Each function reasonably assumes the other is handling the intersection. The result is a control domain both frameworks now require and no one manages end to end.

Divergent Vocabularies and Risk Models

The two functions assess risk differently. Security risk models weigh threat likelihood, asset value, and business impact. Quality risk models weigh patient safety and product quality. A vulnerability rated moderate by enterprise security criteria may be critical when the affected system holds batch release data, and a patch deferred on enterprise change-management grounds may leave a regulated system exposed in ways quality would never accept if quality knew. Without a shared model, the functions reach different conclusions about the same system and neither conclusion accounts for the full picture.

Patch Management Against Validation

Security requires timely patching; validation traditionally treats change as an event requiring assessment. That tension produces regulated systems running unpatched because patching would require revalidation, or patching that proceeds without adequate assessment. The Annex 11 draft addresses patching explicitly, which takes away the option of leaving the tension unresolved. Risk-based assurance offers a path, since a security patch can be assessed proportionately rather than triggering full revalidation, but only where the organization has adopted that thinking and defined the approach.

Legacy Systems and Multi-Factor Authentication

Many GxP environments include systems that cannot support modern authentication. Standalone laboratory instruments, older manufacturing systems, and equipment-embedded software frequently lack the capability for multi-factor authentication or even for individual user accounts. The Annex 11 draft's expectation of multi-factor authentication for electronic signatures makes this a compliance gap rather than a technical inconvenience, and remediation may require system replacement, with capital and timeline implications, rather than configuration.

Incident Response Designed for Only Half the Event

Security incident response is built to contain, eradicate, and recover. It is not built to assess whether the integrity of regulated records was compromised, whether product disposition decisions rested on affected data, or whether regulatory notification obligations arise. When a GxP system is compromised, the security team executes its process and the quality organization frequently learns late, at which point the questions that matter for product and patient have gone unasked while the technical response ran its course.

Vendor and Cloud Security Responsibility

As GxP systems move to cloud and vendor-hosted platforms, security responsibility divides under shared-responsibility models that IT frequently understands and quality frequently does not. The Annex 11 draft specifies contract elements for suppliers, and the FDA guidance expands vendor oversight expectations, which makes the division of security responsibility a documented compliance matter. Organizations that cannot articulate which security controls they own and which the provider owns have a gap both frameworks will expose.

Risks of Poor Implementation

The consequences of the ownership gap are distinctive because a single event produces consequences in two domains at once.

Risk Category	Potential Consequence
Dual-domain incident	A compromised GxP system producing both a security incident and a data integrity failure, with product disposition, release decisions, and distributed material called into question.
Market authorization denial	For cyber devices, submissions refused for lacking required cybersecurity information under the refuse-to-accept policy, delaying or preventing market entry.
Prohibited act exposure	Failure to comply with Section 524B requirements constituting a prohibited act under the Federal Food, Drug, and Cosmetic Act.
GMP inspection findings	Gaps against the Annex 11 security chapter, multi-factor authentication expectations, and audit trail requirements at EU or PIC/S inspection.
Unpatched regulated systems	Systems running with known vulnerabilities because patching conflicts with validation practice, creating both security and compliance exposure.
Retrospective data review	Requirements to assess whether records held by a compromised system remain reliable, potentially across long periods and many products.
Long-lead remediation	Legacy systems unable to support required authentication controls, requiring replacement on timelines that cannot be compressed.

The dual-domain characteristic is what makes this risk category distinctive. Most operational risks produce consequences within one domain and get handled by the function that owns it. A GxP security incident produces consequences in two domains and gets handled, in most organizations, by one function that sees half the event. The technical response may be exemplary while the data integrity assessment never happens, and the organization discovers the second half of the problem when an investigator asks whether the records from the affected period can be relied upon.

The timing risk is also significant. The Annex 11 draft has been public since July 2025 with final publication expected mid-2026, and the gaps it exposes, particularly multi-factor authentication on legacy systems, have remediation lead times measured in quarters. An organization that begins assessment when the final text publishes will be remediating against a live expectation with insufficient time.

Best Practices

Closing the gap takes assigning ownership explicitly, building a shared risk model, integrating security into validation, and designing incident response for the whole event.

Assign Explicit Ownership Across the Boundary

Name who is accountable for the security of GxP systems, covering vulnerability management, patching, access control, penetration testing, and incident response, and make that accountability span the IT and quality functions rather than sit in either alone. Practical approaches include a joint governance body with defined decision rights, or a named owner with authority in both domains. What matters is that the question has an answer, because the current answer in most organizations is that both functions assume the other has it.

Build a Shared Risk Model

Security and quality should assess GxP system risk against a common model that incorporates patient safety and product quality alongside conventional security criteria. A vulnerability affecting a system that holds batch release data should be evaluated with that consequence in view, not solely against enterprise severity ratings. That alignment is what lets patch prioritization, access decisions, and risk acceptance reflect the actual stakes rather than the stakes as one function sees them.

Integrate Security Evidence Into Validation

Because both the FDA guidance and the Annex 11 draft expect security evidence, assurance activities should include it rather than treating security as a parallel activity. That means addressing access controls, authentication, patch status, and vulnerability management within the assurance of a system's fitness for intended use, and documenting that evidence as part of the basis for confidence. Integrating security into validation also resolves the patching tension, because a risk-based assurance approach can accommodate security patches proportionately rather than triggering full revalidation.

Design Incident Response for the Whole Event

Incident response for GxP systems should include, alongside technical containment, an assessment of whether record integrity was affected, which products and decisions relied on the affected data, and whether regulatory obligations arise. Notify quality at the point of detection rather than after technical resolution, and have the response produce a documented conclusion about record reliability. This is a modest addition to an existing process, and it is the difference between responding to an incident and responding to half of one.

Address Authentication and Legacy Systems Early

Inventory GxP systems against the multi-factor authentication expectation, distinguishing those that support it natively, those requiring upgrade, and those that cannot support it at all. That last category presents decisions rather than projects and should reach leadership early, since replacement timelines cannot be compressed. Enterprise identity platforms extended to regulated systems are generally preferable to system-by-system solutions.

Clarify Vendor and Cloud Security Responsibility

For cloud and vendor-hosted GxP systems, document the shared-responsibility division, make sure both functions understand it, and reflect it in agreements consistent with the contract elements the Annex 11 draft specifies and the vendor oversight the FDA guidance expects. You should be able to state which security controls you own and which the provider owns, since an inspection will ask and the answer should not require assembly.

Meet Section 524B Obligations by Design

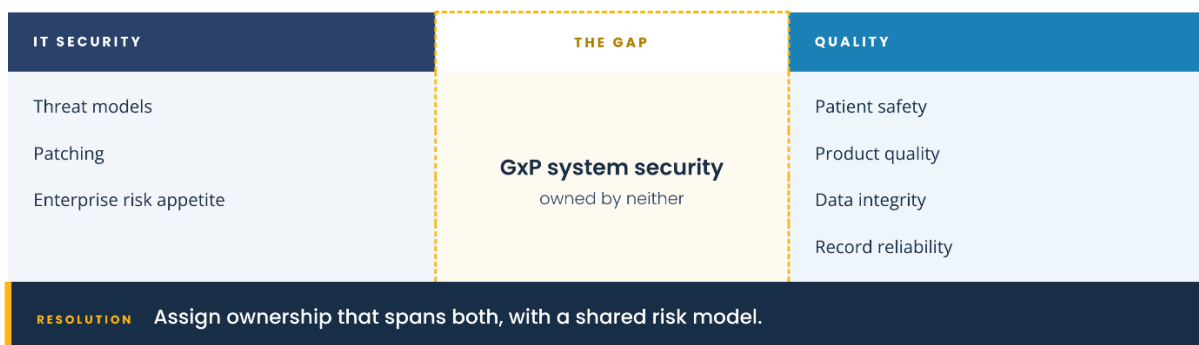
Device manufacturers should build the Section 524B elements into development rather than assembling them at submission: vulnerability monitoring and coordinated disclosure processes, secure development practices providing reasonable assurance of cybersecurity, patch and update capability across the lifecycle, and a software bill of materials covering commercial, open source, and off-the-shelf components. Because the refuse-to-accept policy applies at submission and noncompliance is a prohibited act, these are gating requirements rather than documentation preferences.

Implementation Roadmap

The roadmap below closes the ownership gap and builds security into the quality system rather than alongside it.

FIGURE 1

The GxP Security Ownership Gap



Step 1: Assess the Current State

Inventory GxP systems and determine, for each, who owns its security, what controls exist, what the patch status is, and whether authentication meets emerging expectations. The assessment usually reveals that ownership is assumed rather than assigned.

Step 2: Perform a Gap Assessment

Assess against the applicable frameworks: Section 524B and the cybersecurity guidance for device manufacturers, the Annex 11 draft security chapter and authentication expectations for EU-inspected operations, and the cybersecurity evidence expectations in software assurance. Identify gaps requiring long-lead remediation separately, since these govern the schedule.

Step 3: Assign Ownership and Establish Governance

Name the accountable owner or governance body for GxP system security, with decision rights spanning IT and quality. Define how vulnerability severity, patch priority, and risk acceptance will be decided when the two functions' criteria diverge.

Step 4: Build the Shared Risk Model

Establish criteria that incorporate patient safety and product quality into GxP system security risk assessment, so decisions reflect regulatory consequence rather than enterprise severity alone. Apply the model to the existing vulnerability and patch backlog.

Step 5: Integrate Security Into Assurance

Revise validation and assurance procedures to include security evidence within the basis for confidence, and define how security patches are assessed proportionately rather than through full revalidation. This resolves the patching tension procedurally rather than case by case.

Step 6: Redesign Incident Response

Extend GxP incident response to include record integrity assessment, product and decision impact analysis, and regulatory obligation evaluation, with quality notified at detection. Test the extended process, since an untested response process is a document.

Step 7: Remediate Authentication and Access

Execute the authentication remediation identified in the gap assessment, prioritizing systems that cannot support required controls since these carry the longest timelines. Extend enterprise identity capability to regulated systems where feasible.

Step 8: Monitor, Report, and Sustain

Report GxP security posture to leadership alongside other quality metrics, including patch currency, vulnerability aging, and authentication coverage. Track the final Annex 11 text and update the control set deliberately rather than through a new remediation cycle.

Technology Considerations

The technical work concentrates on identity, patch capability, monitoring, and the cloud arrangements that increasingly host regulated systems.

Identity and access management is the highest-consequence area. The Annex 11 draft's multi-factor authentication expectation for electronic signatures, and the data integrity requirement that actions be attributable to individuals, both depend on identity infrastructure many GxP environments lack. Enterprise identity platforms extended to regulated systems address both requirements coherently, but extension is frequently blocked by systems that cannot integrate, which is why the inventory matters. Shared credentials, still common in laboratory environments, fail both the security and the attributability requirement at once.

Software bill of materials capability has become a gating requirement for cyber devices, and it depends on tooling that inventories software components including transitive dependencies. Because modern devices incorporate large numbers of third-party components and many are pulled in indirectly, manual approaches do not scale. Industry-accepted machine-readable formats are expected, and the SBOM has to support the vulnerability monitoring Section 524B requires across the lifecycle rather than serving as a one-time submission artifact.

Cloud and vendor-hosted systems sit at the intersection of both frameworks' expectations. Shared-responsibility models have to be documented and understood by both functions, and agreements should reflect the contract elements the Annex 11 draft specifies. Evaluate audit rights, data sovereignty, service levels, and exit provisions as compliance matters rather than solely commercial ones. Monitoring and logging capability in cloud environments should support both security detection and the audit trail expectations data integrity requires, since these are the same records serving two purposes.

Future Outlook

The convergence of security and quality will continue, and the near-term milestone is the final Annex 11 text expected mid-2026. Expect the security chapter's direction to hold, since consultation refines rather than reverses such packages, and design against the draft while tracking the final. PIC/S participation means these expectations will propagate to member authorities beyond the European Union.

For device manufacturers, cybersecurity enforcement will deepen as the Section 524B framework matures. The refuse-to-accept policy has already made cybersecurity a gating requirement for market entry, and the prohibited act designation gives the agency enforcement options beyond submission review. Postmarket obligations, including vulnerability monitoring and patch availability across the lifecycle, will get more attention as devices in the field age.

The organizations that manage this well will stop treating GxP system security as an IT matter with regulatory implications and start treating it as a quality obligation with technical execution. That reframing determines who is accountable, what gets measured, and whether an incident is understood as one event or two. The gap between the functions is where the risk lives, and it closes only when someone is named to own it.

How cGMP Consulting Can Help

GxP cybersecurity sits exactly where most organizations lack a function with authority in both domains. cGMP Consulting brings regulatory understanding, technical depth in computerized systems, and practical experience in quality systems and data integrity to close that gap.

Our consultants assess GxP system security against the applicable frameworks, including Section 524B and the cybersecurity guidance for device manufacturers, the Annex 11 draft security and authentication expectations for EU-inspected operations, and the cybersecurity evidence expectations within software assurance. We help organizations assign accountability across the IT and quality boundary, build a shared risk model that incorporates patient safety and product quality, and integrate security evidence into

validation so patching and assurance stop working against each other. We help redesign incident response so a GxP system compromise gets assessed as both a security event and a data integrity event, and we support the authentication and legacy system remediation that carries the longest timelines. For device manufacturers, we help build Section 524B obligations into development rather than assembling them at submission.

Our approach is consultative and grounded in how these systems are actually examined by both device and GMP inspectors. We aim to leave organizations with clear ownership and a control set that satisfies the frameworks, rather than a security program and a quality program that never meet.

Conclusion

Cybersecurity has become a quality obligation, and the regulatory frameworks arrived at that conclusion from both directions. Device regulation reached it through patient safety, producing statutory requirements, a refuse-to-accept policy, and prohibited act exposure. Medicinal product regulation reached it through data integrity, producing a security chapter in the Annex 11 draft and cybersecurity evidence expectations in software assurance. The direction is settled even where the final texts are not.

What has not settled, in most organizations, is ownership. IT owns security, quality owns compliance, and the intersection where a security control is also an integrity control and a breach is also a regulatory event stays unassigned. That gap is where a compromised GxP system produces two failures while the organization responds to one.

Closing it takes naming an owner with authority across both domains, building a risk model that weighs patient safety alongside enterprise severity, integrating security evidence into assurance so patching and validation stop obstructing each other, and designing incident response that asks whether the records can still be relied upon. The long-lead gaps, particularly authentication on legacy systems, should be addressed now rather than when the final Annex 11 text makes them urgent. The organizations that assign the ownership will find the technical work manageable. Those that do not will keep discovering, one incident at a time, that nobody was watching the intersection.

If your organization is addressing the security of its GxP systems, preparing for the Annex 11 cybersecurity expectations, or building Section 524B compliance into device development, the experienced consultants at cGMP Consulting can help assess your current state, identify gaps, and develop practical solutions tailored to your business objectives. To start a confidential conversation, complete the Contact Us form at cgmpconsulting.com/contact-us.

References

- Association for the Advancement of Medical Instrumentation. (2023). ANSI/AAMI SW96:2023 Standard for medical device security — Security risk management for device manufacturers. AAMI.
- European Commission. (2011). EudraLex Volume 4: Annex 11: Computerised systems. European Commission.
- European Commission. (2025). EudraLex Volume 4: Annex 11 Computerised systems (Draft revision, published 7 July 2025). European Commission.

- International Medical Device Regulators Forum. (2020). Principles and practices for medical device cybersecurity. IMDRF.
- International Organization for Standardization. (2019). ISO 14971:2019 Medical devices — Application of risk management to medical devices. ISO.
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
- National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce.
- National Telecommunications and Information Administration. (2021). The minimum elements for a software bill of materials (SBOM). U.S. Department of Commerce.
- U.S. Congress. (2022). Consolidated Appropriations Act, 2023, Section 3305: Ensuring cybersecurity of medical devices (adding Section 524B to the Federal Food, Drug, and Cosmetic Act). Public Law 117-328.
- U.S. Food and Drug Administration. (2023). Cybersecurity in medical devices: Refuse to accept policy for cyber devices and related systems under section 524B of the FD&C Act: Guidance for industry and Food and Drug Administration staff. U.S. Department of Health and Human Services.
- U.S. Food and Drug Administration. (2025). Cybersecurity in medical devices: Quality system considerations and content of premarket submissions: Guidance for industry and Food and Drug Administration staff (Docket No. FDA-2021-D-1158). U.S. Department of Health and Human Services.
- U.S. Food and Drug Administration. (2026). Cybersecurity in medical devices: Quality management system considerations and content of premarket submissions: Guidance for industry and Food and Drug Administration staff. U.S. Department of Health and Human Services.
- U.S. Food and Drug Administration. (2016). Postmarket management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff. U.S. Department of Health and Human Services.
- U.S. Food and Drug Administration. (2026). Computer software assurance for production and quality system software: Guidance for industry and FDA staff (Updated February 3, 2026). U.S. Department of Health and Human Services.
- U.S. Food and Drug Administration. (2018). Data integrity and compliance with drug CGMP: Questions and answers; Guidance for industry. U.S. Department of Health and Human Services.
- U.S. Government Publishing Office. (n.d.). Title 21 Code of Federal Regulations Part 11: Electronic records; Electronic signatures. Electronic Code of Federal Regulations.