ASCLEPIUS

CYBERSECURITY
FOR HEALTHCARE

EU Cyber Resilience Act

Impact on Healthcare Supply Chain

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Co-funded by
the European Union

Contents

Co-funded by the European Union

1. Executive Summary

The European Union's Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for products with digital elements. For the healthcare sector – which relies heavily on connected medical devices, smart pharma systems, and digital health tools – the CRA is strategically important. High-profile cyberattacks on hospitals and pharmaceutical supply chains have revealed risks to patient safety and care continuity.

By setting baseline security standards across a product's lifecycle, the CRA aims to strengthen the resilience of healthcare's complex supply chain and build trust in digital technologies. Beyond legal compliance, it offers healthcare leaders a chance to enhance patient safety, protect sensitive data, and minimize costly disruptions.

Complementing existing regulations like the MDR, GDPR, and NIS2, the CRA positions cybersecurity as a board-level priority. It promotes secure product design and risk-aware supply chains, ensuring that healthcare IT systems and connected devices are protected against evolving threats.

Co-funded by the European Union

2.Introduction

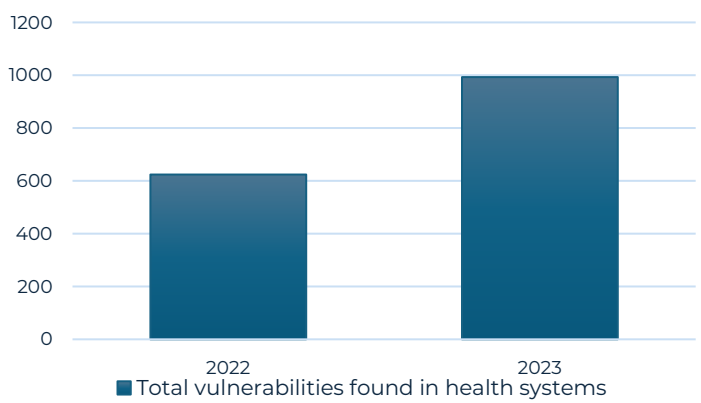
Healthcare is classified as critical infrastructure, yet it has been a prime target for cyberattacks in recent years. Ransomware and supply-chain breaches have hit hospitals, pharmaceutical distributors, and even pharmacy chains, leading to treatment delays and risks to patient safety. For example, a 2023 cyberattack on Alliance Healthcare in Spain forced a shutdown of ordering systems and caused drug delivery delays to pharmacies. Such incidents underscore why regulators are pushing for stronger cyber resilience. The Cyber Resilience Act, which entered into force in December 2024, is the EU's answer to these threats, introducing common cybersecurity rules for products across all sectors. Though the main obligations apply from late 2027, healthcare organizations and their suppliers must act now to prepare. This white paper provides both an executive overview and a technical deep dive into how the CRA will affect the healthcare sector's supply chain, from device manufacturers to pharmacies. We also examine how the CRA's certification framework (including Common Criteria-based evaluations) applies, real-world examples of industry preparation, and the implications for risk management, procurement, and regulatory alignment. Healthcare leaders and technical teams can use this paper to understand the CRA's impact and to chart a proactive compliance strategy.

"Modern healthcare has made incredible advances through digital transformation, which has meant citizens have benefited from better healthcare. Unfortunately, health systems are also subject to cybersecurity incidents and threats. That is why we are launching an Action Plan to ensure that healthcare systems, institutions and connected medical devices are resilient. Prevention is better than cure, so we need to prevent cyber-attacks from happening. But if they happen, we need to have everything in place to detect them and to quickly respond and recover."

- Henna Virkkunen,
Executitve Vice-President for Tech Sovreignty, Security and Democracy

3. Cybersecurity Vulnerabilities in Healthcare

Healthcare remains a top target for cyberattacks, with a significant rise in vulnerabilities across medical devices and IT systems. These trends highlight why compliance with the EU Cyber Resilience Act (CRA) is essential to protect healthcare supply chains.



Surge in Reported Software Flaws: A 2023 industry report (covering 117 medical device and health application vendors worldwide) identified *993 new vulnerabilities in healthcare products in 2023*, a 59% increase from the 624 vulnerabilities found in 2022.

3.1. Vulnerabilities in Connected Medical Devices (IoMT)

Connected medical devices (IoMT), such as infusion pumps, monitors, pacemakers, and insulin pumps, are increasingly vulnerable to cyber threats. Key findings include:

- **Prevalence of Device Vulnerabilities:** Over half of connected medical devices in hospitals carry serious flaws. A January 2022 study found *53% of connected medical devices and other IoT devices in hospitals had at least one known critical vulnerability*
- **Device Types at Risk:** Common life-sustaining devices often harbor vulnerabilities. For example, *73% of IV infusion pumps* (which make up ~38% of a hospital's IoT device fleet) were found to have a security issue that could jeopardize patient safety or data if exploited
- **Legacy Systems and Default Credentials:** A significant portion of medical IoMT runs outdated software or insecure configurations. Approximately *19% of connected medical devices still run legacy*

Co-funded by the European Union

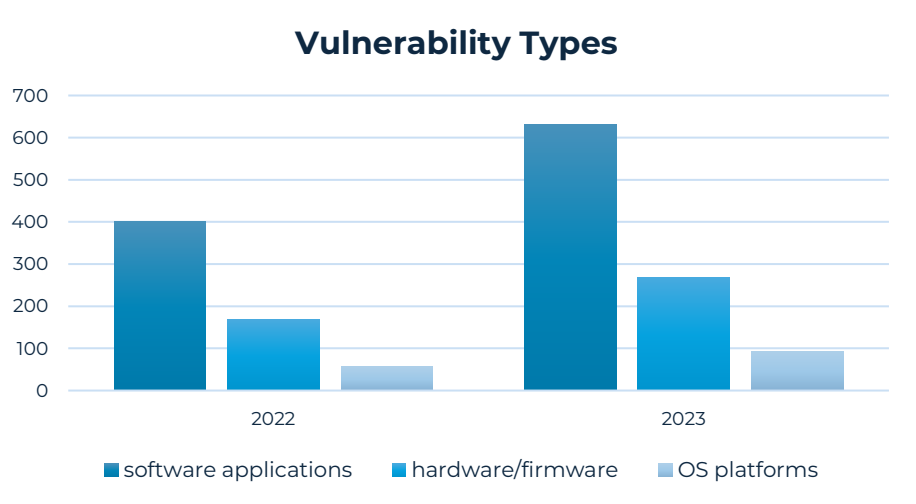
operating systems with no available security patches, and over *40% of medical devices at end-of-life stage receive little to no security updates*

- **Rising Disclosure of Device Flaws:** Recent years have seen more vulnerabilities reported in medical devices through coordinated disclosure programs. As an example, U.S. CISA ICS medical advisories (public disclosures for regulated device flaws) have enumerated dozens of CVEs each year.

Despite a dip in 2022 advisories, the overall trend from 2020 to 2022 was a 144% jump in reported industrial/ICS vulnerabilities (all sectors). This reflects growing research and reporting of medical device CVEs as regulators and firms improve coordinated vulnerability disclosure (CVD) processes.

For instance, notable recent disclosures in the EU included five zero-day flaws reported in April 2022 affecting a hospital autonomous robotic cart system (TUG Homebase Server) – exploitable for full remote control of the robots or denial-of-service – and a critical password weakness in BD's Alaris infusion system disclosed in 2023. These examples show how proactive vulnerability discovery (often via SBOM analysis or researcher coordination) is bringing to light hidden risks in devices before attackers exploit them.

Critical Vulnerability Types: Among the 2023 flaws, researchers flagged a sharp rise in the most dangerous bug types. Remote code execution (RCE) and privilege escalation vulnerabilities – which allow attackers to gain control over systems – jumped to 43 cases in 2023, up 437% from just 8 such critical exploits in 2022.



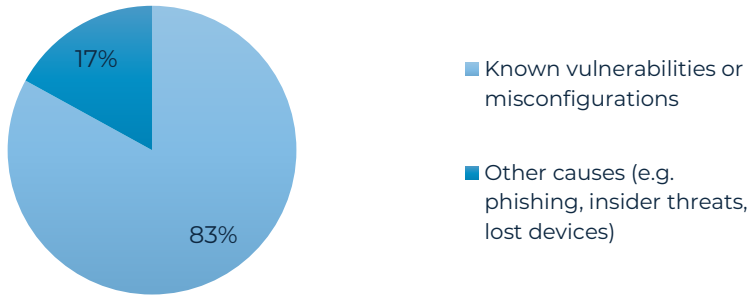
3.2. Vulnerabilities in Medical & Pharmaceutical Software

Beyond the devices themselves, the software applications used in healthcare – electronic health record (EHR) systems, health management platforms, pharmacy and lab systems, and even pharmaceutical manufacturing software – are riddled with vulnerabilities. Several widely-used medical software packages have accumulated multiple CVEs.

For example, an analysis of NVD data (2001–2022) shows LibreHealth EHR (open-source EHR platform) had 21 distinct vulnerabilities, GE Healthcare's Centricity (clinical information system) had 11, and Oracle Argus Safety (pharmacovigilance software used in pharma) had 10 CVEs over that period.

EU-Specific Insights: European healthcare software faces similar issues. ENISA reported that *vulnerabilities in health IT and medical software are an "emerging threat,"* noting that 80% of surveyed EU healthcare organizations said over 61% of their security incidents in recent years were caused by software or hardware vulnerabilities

Types of Incidents



Volume of Incidents Tied to Vulnerabilities: In the EU, 76% of healthcare data breaches in 2021 were caused by vulnerability exploitation (e.g. web attacks, intrusions), rather than internal errors or device loss.

3.3. Healthcare IT Infrastructure & Networks

Healthcare IT infrastructure – including hospital networks, electronic health record platforms, telemedicine systems, and other enterprise IT in healthcare – has seen a steady rise in both the volume of vulnerabilities disclosed and the exploitation of those weaknesses by attackers:

- **Network and EHR Vulnerabilities:** In 2023, 75% of healthcare-related vulnerabilities (741 out of 993) were found in general IT systems—not regulated medical devices—highlighting the scale of the risk beyond clinical equipment. Disclosure and Response Trends: Public and private actors are increasing efforts

Co-funded by the European Union

to flag weaknesses. For example, the U.S. HC3 now issues monthly bulletins detailing critical vulnerabilities in hospital IT products.

- **Most Affected Technologies:** Vulnerabilities in remote access tools and VPNs (e.g. Citrix, Fortinet) have been heavily exploited by ransomware groups. EHR (Electronic Health Record) platforms have also been affected—such as a 2022 case where a bug chain in an open-source system allowed remote code execution.

These patterns confirm that healthcare IT infrastructure is a key attack surface and must be secured with the same rigor as medical devices—especially as CRA and NIS2 demand improved resilience across the entire digital ecosystem.

3.4. Importance of CRA Compliance for Healthcare Supply Chains

The above statistics paint a clear picture – vulnerabilities in medical devices, healthcare software, and IT systems are widespread and growing—directly contributing to cyberattacks that endanger patient safety and data. Many healthcare breaches stem from unpatched systems or known flaws, with hundreds of new critical vulnerabilities disclosed each year across the sector. This reality underpins the EU Cyber Resilience Act (CRA), which sets mandatory cybersecurity requirements for digital products. For healthcare, CRA means stronger security in device design, software maintenance, and IT procurement—including SBOMs, secure development, and patching processes.

With 83% of cyberattacks on EU healthcare providers linked to known vulnerabilities or misconfigurations, CRA's focus on proactive resilience is both necessary and urgent. By adhering to CRA and related frameworks (NIS2, MDR for medical devices), stakeholders in global and EU healthcare supply chains can mitigate the alarming trends highlighted above – shrinking the window of exposure from newly found vulnerabilities, improving coordinated disclosure of flaws, and ultimately protecting patient safety and trust in the digital health ecosystem.

Co-funded by the European Union

4. CRA Impact on Healthcare Supply Chain Stak

The implementation of the EU Cyber Resilience Act (CRA) marks a significant shift in how cybersecurity is regulated across the healthcare supply chain. While certain entities, such as medical device manufacturers governed by MDR/IVDR, are formally excluded from CRA's direct scope, they operate within digital ecosystems that are fully covered by the regulation. This chapter explores how four key stakeholder groups—medical device manufacturers, pharmaceutical distributors, smart pharmacies, and healthcare IT vendors—are strategically and operationally affected by the CRA.

4.1. Medical Device Manufacturers

Scope and Strategic Importance:

Although MDR/IVDR-regulated devices are excluded from CRA's formal scope, manufacturers are still affected. Their products operate within digital ecosystems (software, cloud, hardware) covered by the CRA. The EU is also reviewing MDR to align with "state-of-the-art" cybersecurity, possibly reflecting CRA principles. While not mandatory, adopting CRA practices supports patient safety and brand trust. The 2025 Health Cybersecurity Action Plan encourages voluntary incident reporting via ENISA, signaling clear regulatory expectations.

Technical Requirements and Challenges:

Key areas include secure-by-design development, SBOM management, vulnerability policies, and supplier assurance. Components like microcontrollers must be CRA-compliant if part of the product. While CRA doesn't apply directly, many manufacturers align their practices voluntarily—especially as MDR and NIS2 already demand cybersecurity maturity and supply chain risk management.

4.2. Pharmaceutical Distributors

Scope and Strategic Importance:

Distributors rely on digital systems (e.g. IoT sensors, logistics software) to manage medicine flow. If such tools are marketed or have connectivity, they fall under CRA. A cyberattack can delay drug deliveries, as seen in the 2023 Alliance Healthcare case

Co-funded by the European Union

in Spain. CRA compliance boosts trust among partners and aligns with NIS2 obligations for “essential entities.”

Technical Requirements and Challenges:

Distributors must ensure CRA-compliance in the tools they use or supply—this includes requiring CE-marked equipment, securing SBOMs from vendors, and updating procurement processes. In-house developed software triggers full CRA obligations. Legacy systems may need upgrading to avoid becoming vulnerabilities. Distributors should prepare for dual incident reporting under CRA and NIS2.

4.3. Smart Pharmacies

Scope and Strategic Importance:

Modern pharmacies use connected devices like dispensing robots, smart fridges, and patient apps—all likely within CRA’s scope. Cyber incidents can impact medication accuracy or expose patient data. CRA-aligned technology enhances resilience and mitigates such risks.

Technical Requirements and Challenges:

Pharmacies must verify CRA compliance for new equipment and maintain support contracts for regular security updates. Internally developed apps must meet CRA standards if distributed. Integrating SBOMs into IT processes and aligning CRA with GDPR reporting are key operational shifts. Pharmacies and distributors rely on digital systems for inventory and dispensing. A cyber incident can disrupt medication supply or compromise patient data. Ensuring that pharmacy automation devices, software, and IoT sensors meet CRA cybersecurity standards will help prevent operational outages and safeguard public health.

4.4. Healthcare IT Vendors

Scope and Strategic Importance:

This includes EHR providers, telehealth platforms, and other digital health software companies. Nearly all of their products qualify as “products with digital elements” and must meet CRA standards. As hospitals adopt NIS2 compliance, CRA certification will become a vendor selection criterion.

Co-funded by the European Union

Technical Requirements and Challenges:

Vendors must implement CRA Annex I requirements: secure defaults, vulnerability handling, access controls, and full documentation. SBOMs are essential for transparency and risk response. Depending on product risk classification (Class I/II), self-assessment or third-party certification may be required. Post-market surveillance and structured security teams will become the norm.

Co-funded by the European Union

5.Common Criteria and CRA's Tiered Certificatio Framework

The Cyber Resilience Act introduces a tiered conformity assessment system based on the cybersecurity risk associated with a product. All digital products must meet CRA's essential requirements, but the level of scrutiny increases by product class:

Default Category

The majority of products (those not listed as Class I, II, or Critical) are in the default category. Manufacturers can self-assess these products for compliance, meaning they internally verify and declare that the product meets CRA requirements. A technical file documenting the risk analysis, security measures, and an SBOM is required, but no third-party auditor is mandatory. Many healthcare IT applications and general-purpose devices used in healthcare (e.g. a basic vital signs mobile app or a clinic's Wi-Fi printer) will likely fall in this default group.

Important Class I

This class includes moderately high-risk products explicitly listed in CRA Annex III, such as identity management systems, VPNs, antivirus tools, operating systems, and network equipment. In healthcare, this may include hospital SSO platforms or routers linking medical devices.

Manufacturers can use self-assessment, but only if they follow a recognized "conformity path"—by applying a Harmonized Standard, an EU Common Specification, or using an approved EU cybersecurity certification scheme. If no such framework applies, third-party assessment becomes mandatory.

This approach encourages the use of emerging standards to streamline compliance. Healthcare buyers may increasingly encounter references to such standards or certifications when evaluating solutions. Regardless of the assessment route, the CE marking and Declaration of Conformity must indicate Class I status and confirm full CRA compliance.

Co-funded by the European Union

Important Class II

This class covers products with a higher cybersecurity impact and always requires third-party conformity assessment. Examples from Annex III include firewalls, IDS/IPS systems, hypervisors, and tamper-resistant chips.

In healthcare, Class II products may include firewall appliances protecting hospital networks or secure chips embedded in medical devices. Manufacturers must engage an accredited Conformity Assessment Body (CAB) to conduct audits and testing before market placement—similar to the Notified Body process under MDR.

Healthcare organizations procuring Class II products should request formal certification documents (e.g. an EU declaration or CAB-issued certificate) to confirm CRA compliance. This ensures independent validation of critical cybersecurity features.

Critical Class

This class includes the most cybersecurity-sensitive products, such as secure hardware modules, smart cards, smart meters, and advanced cryptographic components, as listed in CRA Annex III.

These products must undergo European Common Criteria (EUCC) certification, based on the ISO/IEC 15408 framework. Certification must be conducted by a licensed security lab and approved by a national cybersecurity authority, typically at the Substantial or High assurance level.

In healthcare, Critical Class components are often used indirectly, such as encryption chips in medical devices or secure enclaves in cloud services. Manufacturers using such components must ensure they are EUCC certified.

The Common Criteria process provides strong assurance but also involves longer lead times, so it should be factored into early development planning.

6.Implications and Recommendations for Health Stakeholders

As the EU Cyber Resilience Act (CRA) redefines cybersecurity responsibilities across the healthcare landscape, organizations must adopt a more comprehensive approach—one that extends beyond IT infrastructure to include the full lifecycle security of every digital product they use or procure. This section outlines how CRA transforms traditional risk management and procurement practices by placing accountability for product-level cybersecurity directly on healthcare providers and their vendors. It highlights the critical steps organizations should take to assess third-party security, embed CRA requirements into procurement workflows, and prepare for the regulation's phased compliance deadlines..

6.1. Recommendations

Risk Management and Third-Party Security

CRA shifts the focus from internal IT security to full lifecycle product security. Healthcare organizations must assess the cybersecurity posture of every connected device and software in use. This includes maintaining an inventory of all "products with digital elements," checking CRA compliance, and demanding SBOMs and vulnerability disclosure programs from vendors.
Key actions:

- Update vendor questionnaires to include CRA-related questions.
- Include cybersecurity clauses in contracts (e.g. 24h incident notice).
- Establish a cross-functional cyber risk committee.
- Treat product security risks on par with clinical and financial risks.

Procurement Practices

CRA compliance must be built into procurement workflows. Hospitals and clinics should:

- Require CRA compliance in RFPs and tenders.
- Ask for CE markings and EU Declarations of Conformity.
- Include SBOM submission as part of product delivery.

Co-funded by the European Union

- Ensure contracts cover security support over the product lifecycle. Procurement becomes a strategic tool to drive cybersecurity maturity across the sector.

Compliance Timelines and Readiness

Key CRA deadlines:

- Sept 2026: vulnerability reporting begins.
- Dec 2027: full compliance required for products on the market.

Recommendations:

- By 2025: audit digital products and engage vendors.
- By 2026: implement reporting and product upgrades.

By 2027: finalize compliance. Ongoing CRA conformity (e.g. patching, updated SBOMs) must be integrated into regular operations and SDLCs. Participate in pilot programs where possible.

6.2. Regulatory Alignment

MDR/IVDR (Medical Device Regulations):

While MDR-regulated medical devices are exempt from the CRA to avoid double regulation, many supporting components (e.g. mobile apps, cloud platforms, embedded software) do fall under the CRA. This creates a dual compliance landscape:

- Manufacturers should align MDR-required processes like risk management (per ISO 14971) and secure design (per IEC 81001-5-1) with CRA expectations to reduce duplication.
- In the future, MDR may be amended to directly reference CRA-style cybersecurity criteria.
- In practice, procurement teams may need to check for two CE marks: one for medical safety under MDR and another for cybersecurity under CRA.

NIS2 Directive:

CRA focuses on securing the product itself; NIS2 governs the cybersecurity posture of the organization using it.

Co-funded by the European Union

- Healthcare providers (as “essential entities”) and medtech firms (as “important entities”) must implement NIS2-mandated risk management and incident response.
- CRA-compliant suppliers help healthcare organizations meet NIS2’s supply chain security requirements.
- Incident coordination is critical: a product vulnerability may trigger CRA reporting for the manufacturer and NIS2 reporting for the healthcare provider.

GDPR (General Data Protection Regulation):

While CRA improves product-level cybersecurity, GDPR governs the protection of personal data—especially critical in healthcare.

- Vulnerabilities in products (covered by CRA) may lead to data breaches (governed by GDPR).
- Manufacturers should support customers (e.g. hospitals) in GDPR breach notifications if their product is at fault.
- CRA’s requirements for secure defaults, encryption, and patching support GDPR’s “data protection by design and by default.”
- Both frameworks require documentation (technical for CRA, processing records for GDPR) – aligning content can reduce compliance burden.

Other Regulations/Standards:

- The upcoming European Health Data Space (EHDS) will require interoperability and secure data sharing; CRA-compliant products must align with these expectations.
- Manufacturers following international standards (e.g. ISO/IEC 81001 series or US FDA cybersecurity requirements) will already cover many CRA elements.
- Ongoing coordination between ENISA, CEN/CENELEC, and other bodies is expected to yield unified guidance for cross-regulation compliance.

Co-funded by the European Union

7.Conclusion

The EU Cyber Resilience Act (CRA) marks a fundamental shift in how cybersecurity is treated across the healthcare supply chain – elevating it to a core component of product quality, compliance, and patient safety. This paper has shown how CRA requirements impact key players: from medical device manufacturers and pharmaceutical distributors to smart pharmacies and healthcare IT vendors. Across the board, one message is clear: early preparation matters.

Organizations that proactively adopt CRA principles – such as secure design, SBOMs, robust testing, and structured incident response – will not only meet regulatory deadlines but also gain a competitive edge by reducing risk and building trust. Delayed action may lead to costly retrofits, lost contracts, or even loss of market access post-2027.

Importantly, CRA is more than a compliance task. It's an opportunity to embed security by design, enabling innovation in a safer, more resilient environment. Aligning CRA implementation with existing frameworks like MDR, NIS2, and GDPR can streamline compliance and create a unified, risk-based governance approach.

The next few years offer a unique window to act: train staff, update procurement policies, build internal expertise, and participate in collaborative forums like European Health ISAC. Cybersecurity in healthcare has too often been reactive. CRA enables a shift to preventive, resilient, and strategic security.

Ultimately, the CRA calls for a shared responsibility model. It provides a clear roadmap for healthcare stakeholders to strengthen Europe's digital health ecosystem – protecting both operations and the patients who depend on them.

Co-funded by the European Union

Bibliography

1. **ENISA.** (2023). *Threat Landscape 2023: Healthcare Sector Overview*. https://www.enisa.europa.eu/publications
2. **European Commission.** (2022). *Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*, COM(2022) 454 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454
3. **European Commission.** (2025). *Action Plan on the Cybersecurity of Hospitals and Healthcare Providers* [Working Draft].
4. **European Parliament and Council.** (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
5. **European Parliament and Council.** (2019). *Regulation (EU) 2019/881 (Cybersecurity Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881
6. **U.S. Cybersecurity & Infrastructure Security Agency (CISA).** (2022). *ICS Medical Device Advisories – CVEs and Impact*. https://www.cisa.gov
7. **U.S. Food and Drug Administration (FDA).** (2022). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and FDA Staff*. https://www.fda.gov
8. **Cynerio.** (2022). *The State of IoT Security in Healthcare*. https://cynerio.com/resources/reports
9. **Securin / Finite State / Health-ISAC.** (2023). *Cyber Insecurity in Healthcare: 2023 Report on Device & Software Vulnerabilities*. https://health-isac.org
10. **McKinsey & Company.** (2022). *Securing the Pharmaceutical Supply Chain*. https://www.mckinsey.com
11. **Swisslog Healthcare.** (2022). *Cybersecurity Advisory for Automated Pharmacy Systems*.
12. **FBI.** (2022). *Private Industry Notification: Threat Actors Targeting Healthcare Infrastructure*. https://www.ic3.gov
13. **LibreHealth.** (2023). *CVE Database – Open Source EHR Vulnerabilities*. https://cve.mitre.org
14. **MITRE.** (2023). *Common Vulnerabilities and Exposures (CVE®)*. https://cve.mitre.org
15. **HHS Health Sector Cybersecurity Coordination Center (HC3).** (2023). *Monthly Vulnerability Bulletin – Healthcare IT Threats*. https://www.hhs.gov
16. **MedTech Europe.** (2024). *Cybersecurity Position Papers*. https://www.medtecheurope.org
17. **PwC.** (2023). *Pharmaceutical Cybersecurity and the Digital Supply Chain*. https://www.pwc.com
18. **SANS Institute.** (2023). *Securing Smart Hospitals: Research Report*. https://www.sans.org
19. **National Health Executive (UK).** (2023). *Case Study: Alliance Healthcare Cyberattack*. https://www.nationalhealthexecutive.com