# WHY HEALTHCARE CYBERSECURITY IS STILL HARD

## A 2026 UPDATE ON THE CONSTRAINTS OF HEALTHCARE CYBERSECURITY

Five years ago, Medcrypt published "Why Healthcare Cybersecurity Is Hard" (Seth D. Carmody, March 2021), arguing that healthcare's cybersecurity problem is not primarily a technology gap; it is a structural, economic one. The paper identified six constraints that, left unaddressed, would keep producing the same outcome regardless of how much any single organization spent on security:

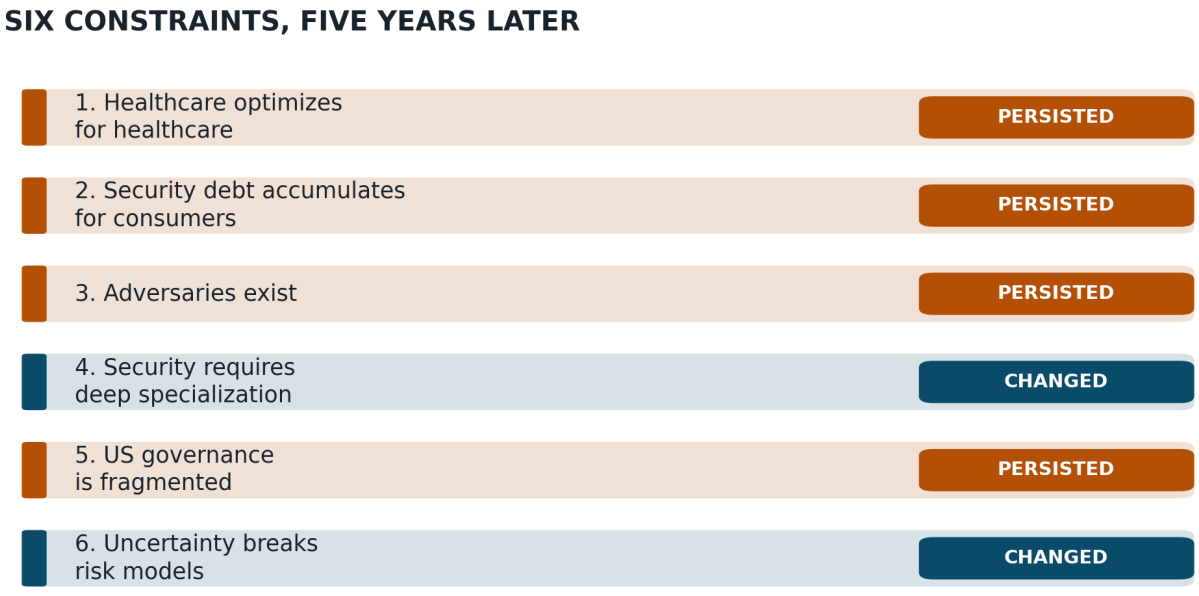
- Healthcare optimizes for healthcare.
- Security debt accumulates and lands on consumers.
- Adversaries exist.
- Security requires deep specialization.
- U.S. governance of healthcare technology is fragmented.
- Uncertainty breaks the existing regulatory risk model.

This update revisits each constraint against five more years of evidence, from 2021 through mid-2026, to ask one question of each: has it persisted, changed, or gone away? Each constraint below restates its 2021 baseline in full, so this update stands on its own.

***Of the six constraints identified in 2021, four have persisted, and by most measures intensified. Two have genuinely changed. None have gone away.***

## AT A GLANCE: SIX CONSTRAINTS, FIVE YEARS LATER

*The chart below shows where each constraint landed after five more years of data. The sections that follow walk through the evidence behind every verdict in full, with sourcing.*



CONSTRAINT 1

# HEALTHCARE OPTIMIZES FOR HEALTHCARE

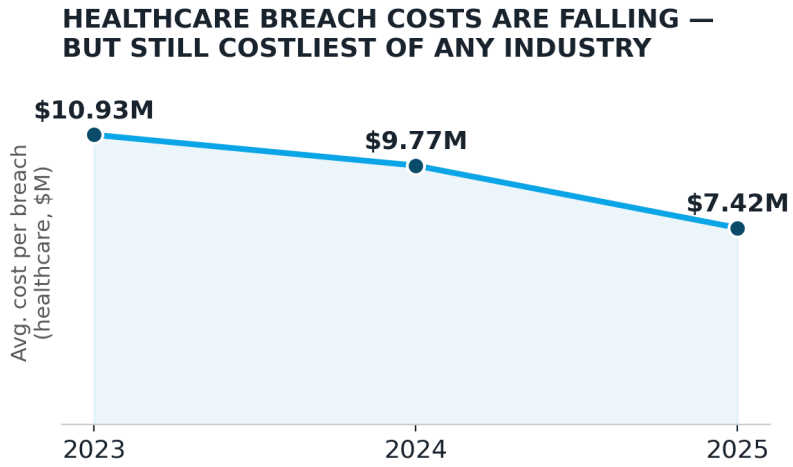
### 2021 BASELINE

*Medical device manufacturers (MDMs) are rational actors who invest in clinical features that drive revenue, not security features with indirect ROI. Healthcare Delivery Organizations (HDOs) spent an estimated $10–20B/year on cybersecurity yet still underperformed on security metrics. A 2019 Vanderbilt study linked breach-remediation controls to worse clinical outcomes.*

### 2026 UPDATE

HDO security spending has kept climbing, to roughly 13.3% of IT budget, up from a historical baseline under 10%, with cumulative sector spend approaching $125B for 2020–2025. [1,2]

Yet outcomes haven't followed the money: healthcare continues to incur the highest breach cost for the fourteenth consecutive year, at $7.42M on average, and still takes longer to detect and contain a breach than any other sector, at 279 days. The one bright spot is a trend rather than a single data point: healthcare's average breach cost has fallen three years running, which IBM attributes to faster detection and containment, not to fewer or smaller breaches. [3]




Source: IBM, Cost of a Data Breach Report, 2023–2025 editions.
Healthcare has ranked the costliest industry for 14 consecutive years; detection and containment still take the longest of any sector (279 days).

The clearest evidence that this is a patient-safety story, not just a balance-sheet one, comes from a University of Minnesota study of Medicare claims data, peer-reviewed in the American Economic Journal: Economic Policy in February 2026 and methodologically stronger than the 2019 Vanderbilt study the 2021 paper cited. It found that ransomware attacks raised in-hospital mortality among admitted patients by 34–38%, an estimated 42–67 additional Medicare deaths from 2016 to 2021 alone. That reinforces rather than undercuts the 2021 paper's claim about patient harm. [4,5]

And where investment has actually moved, it's largely because regulation forced it: FDA's Section 524B cybersecurity mandate, effective in 2023, is now compelling manufacturer security investment that market incentives alone never produced. That is a real shift, but an externally imposed one, not a change in what the market rewards. [6]

**2026 VERDICT: PERSISTED**

Spending is up, but outcomes haven't followed. Healthcare still ranks worst-in-class on breach cost and detection speed, and newer, more rigorous research strengthens the link between security debt and patient harm rather than weakening it.

CONSTRAINT 2

## SECURITY DEBT ACCUMULATES & PROBLEMS MANIFEST FOR CONSUMERS

### 2021 BASELINE

*Producers create security debt; consumers (largely HDOs) spend roughly $20B/year managing, not reducing, that debt through network and perimeter defenses. Three problems: high variance in perimeter robustness across organizations, insufficiency of perimeter defense alone, and a perimeter that is dissolving as cloud and telehealth spread.*

### 2026 UPDATE

Some of the shift-left mechanisms the 2021 paper called for now exist in regulation. FDA's SBOM mandate and its finalized Premarket Cybersecurity guidance, issued in 2023 and updated in 2026, are the first real requirement that manufacturers build security in before a device ships, but they apply only to newly submitted "cyber devices," leaving the much larger population of legacy, already-marketed devices untouched. [7,8]

Voluntary efforts haven't filled that gap either: CISA's Secure by Design pledge explicitly excludes medical devices and IoT, and a 2025 industry survey found that 93% of device makers still prioritize speed-to-market over security. [9]

The dollars still mostly flow to managing debt rather than eliminating it. The product-level medical device security market, worth roughly $8.3B in 2025, remains an order of magnitude smaller than the compensating-controls market it's meant to replace. Healthcare's spend on managed detection and response is growing about 26.6% annually, faster than product security itself. [10,11]

Independent benchmarking bears this out: KLAS and the American Hospital Association found medical-device-security coverage the weakest practice in their Healthcare Industry Cybersecurity Practices framework for the third year running, at just 48% adoption, even as telehealth (growing roughly 24% a year) and remote patient monitoring (now over 71 million users) continue to dissolve the traditional network perimeter. [12,13]

The February 2024 Change Healthcare breach, traced to a portal that lacked multi-factor authentication, is the starkest recent proof that upstream debt detonates downstream: it cost UnitedHealth over $2.45B in 2024 alone, with later disclosures putting the total higher still. [14]

**2026 VERDICT: PERSISTED**

Early shift-left mechanisms now exist, but they're voluntary or narrowly scoped, legacy-device debt is openly unaddressed, and the dollars still flow mainly to managing debt rather than eliminating it. By ransomware-rate and breach-cost measures, this constraint has intensified.

---

CONSTRAINT 3

## ADVERSARIES EXIST

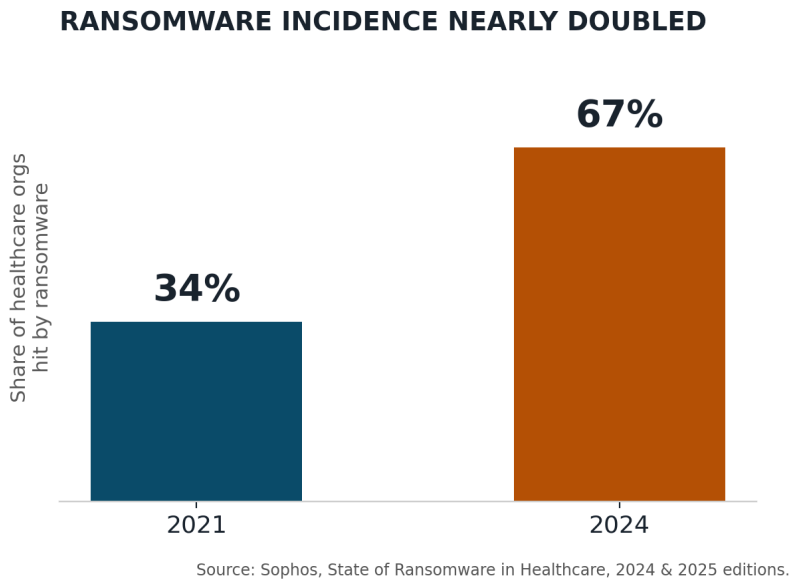
### 2021 BASELINE

*Cyberattacks are a public health risk: WannaCry disrupted the NHS and diverted patients; NotPetya cost Merck roughly $1.4B individually and roughly $10B in collective global damage across all industries; a string of 2020 U.S. hospital ransomware incidents (UHS, Vermont/UVM, Erie County, a Los Angeles hospital) showed the pattern was widespread and accelerating during COVID-19, even as HDO budget cuts reduced organizations' ability to respond.*

### 2026 UPDATE

Every 2021-era benchmark for this constraint has since been dwarfed. The February 2024 Change Healthcare/UnitedHealth attack is now the largest healthcare breach on record: 192.7 million individuals affected per HHS's final count, $2.46B+ in company costs disclosed for 2024 alone, and disruption to an estimated 67,000 pharmacies nationwide. [15,16]

Three months later, the May 2024 Ascension ransomware attack hit a health system of roughly 140 hospitals in 19 states, forcing many facilities back to paper charts, with documented near-miss medication errors and ambulance diversions; 5.6 million individuals were confirmed affected. CommonSpirit Health's 2022 incident hit 164 facilities, exposed data on more than 623,700 patients, and cost $160M in business interruption and remediation. Taken together, large breaches, those affecting 500 or more records, have exceeded 700 a year since 2021, and 2024 and 2025 both set records (772 for 2025 at year-end, a number HHS keeps revising upward as late reports arrive). [17,18,19]




The human cost keeps pace with the financial one: the same research cited under Constraint 1 found that ransomware raised in-hospital Medicare mortality from 3.7% to 4.5%, an estimated 42–67 additional deaths from 2016 to 2021. And the trend is not turning. Tactics are evolving, with more extortion without encryption and fewer ransom payments, but overall attack volume rose through 2025. [4,20,21]

**2026 VERDICT: PERSISTED**

Every 2021-era benchmark, from WannaCry to NotPetya to the 2020 hospital incidents, has been dwarfed by 2022–2026 events. This constraint hasn't just persisted; it has unambiguously intensified.

---

CONSTRAINT 4

# SECURITY REQUIRES DEEP SPECIALIZATION

### 2021 BASELINE

*Security is a specialized discipline, and trying to make healthcare experts into security experts (or the reverse) produces worse outcomes at both. MDMs traditionally solved problems in-house because commercial, healthcare-specific security solutions were immature or unusable, forcing costly, error-prone, "roll-your-own" approaches that were a hard sell against clinical feature investment.*

### 2026 UPDATE

Where this constraint has genuinely moved is the market. A consolidated, well-funded commercial ecosystem now exists where one barely did in 2021: Claroty's acquisition of Medigate (2022), Forescout's acquisition of CyberMDX (2022), Axonius's acquisition of Cynerio (2025, for more than $100M), and ServiceNow's pending $7.75B acquisition of Armis, announced in December 2025 and explicitly covering medical devices. Medical device security has become an investable, scalable category rather than a build-only problem. [22,23,24]

Medcrypt itself is now used by 8 of the top 10 global medical device manufacturers, direct evidence that "buy" has become the mainstream option it wasn't five years ago. Procurement behavior is following the same path: industry surveys find that 83–84% of device buyers now write cybersecurity requirements into their RFPs, and as many as 56% have rejected a device on cybersecurity grounds alone. [25,26]

What hasn't moved is the underlying talent and culture problem. The global cybersecurity workforce gap reached 4.8 million people in 2024, 94% of healthcare respondents report ongoing skills gaps, and one 2024 survey found that 93% of MDMs still say they prioritize time-to-market over security, despite the new market and the new regulation. A market for buying expertise has emerged; the shortage of the expertise itself has not gone away. [27,28,29]

**2026 VERDICT: CHANGED**

The "no market exists" half of this constraint is resolved: a funded, consolidating vendor ecosystem now makes "buy" viable. The "hard to staff and culturally hard to prioritize" half has not resolved, and by some measures has worsened.

---

CONSTRAINT 5

## US HEALTHCARE TECHNOLOGY GOVERNANCE IS FRAGMENTED

### 2021 BASELINE

*No single authority governs the cybersecurity of healthcare technology. Oversight is split across FDA, CMS, OCR, DOJ, state boards, and dozens of other bodies. Technology that doesn't meet the legal definition of a "medical device" or contain protected health information can fall into a regulatory gap despite being an equally viable attack vector.*

### 2026 UPDATE

Real progress happened, but only at the device level. Section 524B of the Federal Food, Drug, and Cosmetic Act, effective in 2023, gave FDA an explicit legal mandate and the authority to enforce cybersecurity requirements, closing a genuine gap for products that meet the legal definition of a "cyber device." But Change Healthcare, a claims clearinghouse entirely outside FDA's authority, suffered the sector's worst incident anyway in 2024. [30,6]

Above the device level, the picture looks much like it did in 2021. HHS's overhaul of the HIPAA Security Rule (mandatory encryption, multi-factor authentication, penetration testing) was proposed in December 2024 and remains unfinalized as of mid-2026, with HHS's own regulatory agenda pushing final action out to 2027. CMS's promised hospital cybersecurity Conditions of Participation, floated in a December 2023 HHS concept paper, still hasn't even been formally proposed. [31,32]

The government's own auditors agree the gaps remain. GAO's November 2024 review found that HHS, the sector's own designated lead agency, hadn't adequately assessed IoT/OT risk across the sector and had identified conflicting cybersecurity requirements between CMS and other federal agencies. Congress has introduced bills to consolidate oversight: HIPAA in 2024, and the Health Care Cybersecurity and Resiliency Act, which advanced out of the Senate HELP Committee 22–1 in February 2026. Neither has been enacted. [33,34,35]

Meanwhile, states are adding to the patchwork rather than simplifying it: New York (October 2025) and California (2025–2026) each layered new cybersecurity and breach-notification requirements on top of federal rules rather than replacing them. [36]

**2026 VERDICT: PERSISTED**

Real progress happened at the device level. But enterprise- and clearinghouse-level fragmentation, the exact gap that let Change Healthcare happen, remains open, and every proposal to consolidate oversight is still pending.

---

CONSTRAINT 6

# UNCERTAINTY BREAKS EXISTING RISK MODELS

### 2021 BASELINE

*FDA's device regulatory model was built for static products like pills, assessed once at time of sale under current Good Manufacturing Practices. Software-driven medical devices are dynamic "systems of systems" with continuously evolving risk that the model couldn't handle. FDA officials had said the model needed a fundamental rethink; the Digital Health Software Precertification pilot was underway as one possible fix.*

### 2026 UPDATE

This is the constraint where the regulatory model itself has genuinely changed. Section 524B, effective in 2023, is the first explicit statutory requirement for continuous postmarket risk management: mandatory software bills of materials, coordinated vulnerability disclosure, and a 60-day clock for remediating critical vulnerabilities. FDA's final premarket guidance, issued in September 2023 and reissued in February 2026, formally adopts a Total Product Lifecycle and Secure Product Development Framework approach; CDRH's own cybersecurity director now describes security as something that "spans across the total product life cycle… not a secondary consideration." [6,37,38]

Section 524B did not arrive alone, and the pairing was deliberate. The same omnibus, the Food and Drug Omnibus Reform Act of 2022, added two provisions to the FD&C Act three sections apart: §3305 created Section 524B, and §3308 created Section 515C. Section 515C(a)–(c) gave FDA explicit statutory authority to review and authorize predetermined change control plans, so a manufacturer can make pre-agreed changes to an approved or cleared device without filing a new submission each time. Read together, the two sections formalize the same premise from opposite directions: a device will change after it ships. Section 515C reduces the regulatory burden of that change and creates a planned pathway for it. Section 524B ensures that as the device changes, the stakeholders who depend on it, from patients and clinicians to HDOs and payers, keep receiving assurance of safety, effectiveness, and security. One removes the friction from changing a device; the other keeps change from quietly eroding trust. Neither works without the other. FDA's 2024 PCCP guidance for AI/ML-enabled devices operationalizes that authority for the fastest-moving category of all. [40,42]

| OLD MODEL: PRE-2023 | NEW MODEL: 2023–2026 |
|---|---|
| Assessed once, at time of sale | Assessed continuously, across the product lifecycle |
| No cybersecurity-specific postmarket mandate | Section 524B: mandatory SBOMs, coordinated disclosure, 60-day remediation clock |
| A new submission for every device change | Section 515C: predetermined change control plans |
| 1996 cGMP-style Quality System Regulation | QMSR / ISO 13485, effective February 2026 |
| Digital Health Software Precertification pilot (ended 2022) | Statutory fix delivered via Sections 515C and 524B |

There is a second admission buried in that pairing. Devices have to change to deliver innovative care, which is the premise underneath 515C, and the agency is now willing to build the frameworks that let them. That is a genuine shift in posture. But it also puts both impulses inside the same statute, where the tension between them is finally visible: the pathway that makes clinical innovation faster is the same pathway that has to carry the security assurance. Constraint 1 says what happens when that pairing is left to the market. Clinical innovation supersedes security every time, because that is what the market rewards. Legislating the two authorities together is Congress's way of ensuring innovation is not allowed to override security.

The Quality Management System Regulation, finalized in February 2024 and effective in February 2026, retires the 1996 cGMP-style Quality System Regulation in favor of ISO 13485, a direct modernization of the static, "pill-era" chassis the 2021 paper criticized. [39]

Notably, the fix didn't come the way the 2021 paper expected. The Digital Health Software Precertification pilot referenced in 2021 ended in September 2022, when FDA concluded it wasn't workable under existing statutory authority; the eventual fix came through Congress, via Sections 515C and 524B, not through precertification. One gap remains open by FDA's own admission: legacy devices already in the field. CDRH's cybersecurity director called this "an unsolved challenge" as of December 2024. [41,38]

That challenge is unsolved for a reason that is not technical. Legacy devices are a remnant of an earlier era, designed and cleared when no one expected a device to change after it left the factory. Making a fielded device updatable on a reasonable timeline is therefore not a patch. It is a cultural, organizational, and operational change inside each manufacturer, touching engineering, service, regulatory, and support at once. Which puts the legacy problem back on Constraint 1: absent an economic incentive large enough to justify it, companies will not spend the capital, and the installed base stays where it is. It is the clearest remaining case where regulation has named a problem it has not yet priced.

**2026 VERDICT: CHANGED**

Devices are still cleared on a snapshot basis, so the static, one-time-clearance model has not gone away, but the regime around it is modernizing. Section 524B, the QMSR, and the PCCP framework all push toward continuous, total-product-lifecycle risk management; whether that becomes the basis of a genuinely new regulatory model only time will tell. Two things remain unresolved: legacy devices already in the field are still governed by the old assumptions, which FDA itself acknowledges, and the premise underneath the model, that the risk of a software system can be fully defined at a point in time, is still false.

---

## CONCLUSION: FIVE YEARS ON, THE ROOT CAUSES REMAIN

| 4 | 2 |
|---|---|
| CONSTRAINTS PERSISTED | CONSTRAINTS CHANGED |

Four of the six constraints identified in 2021 have not just persisted through 2026, they have intensified by nearly every measure we could find: breach cost, breach volume, detection time, and documented patient harm are all higher today than in 2021.

Two constraints have genuinely changed, both for the better, and both because of the same forcing function: hard regulatory mandates (principally FDA's Section 524B and its associated guidance) rather than market incentives. That is what the 2021 paper predicted: cybersecurity is a classic negative externality, so the incentive has to be injected by a regulator. The benefit is societal, even though each manufacturer, as Constraint 1 describes, is rewarded for building clinical features instead. A real commercial market for medical device security now exists where one barely did in 2021, and FDA's regulatory model has begun moving from static, one-time premarket clearance toward continuous, total-product-lifecycle risk management for newly submitted devices, though clearance itself remains a snapshot. Neither change resolves the underlying economics: MDMs still compete on clinical features, not security; legacy devices already in the field remain outside the new framework; and no single authority yet governs the technology, and the data, that sit outside the legal definition of a "medical device."

**None of the six constraints have gone away. The extent to which healthcare achieves a sufficient state of security and resilience remains proportional to how well the supply chain reduces security debt at the source, not to how much any single organization spends managing the debt it inherits.**

## LOOKING AHEAD

*This data points to a harder truth than "buy more security tools." Point solutions, even good ones, chip away at one constraint at a time, one device at a time. They don't tell a manufacturer how its entire portfolio compares to peers, and they don't tell an executive who isn't a security expert what an unresolved vulnerability is actually worth in dollars, which is exactly the language Constraint 1 says security must speak to compete for budget against clinical features.*

*That's the problem Medcrypt itself has spent the better part of a decade working on. Our original product embedded cryptographic identity and behavioral monitoring directly into individual devices: real progress against Constraint 4, one device and one manufacturer at a time. It didn't solve the portfolio-wide, executive-facing version of the problem: manufacturers with dozens or hundreds of devices had no consistent way to benchmark security posture across their business, or to translate it into a number a CFO could act on. In 2025 we launched Medcrypt Security Intelligence to close that gap. A follow-up paper will lay out that shift in full: what the original model got right, where it hit a ceiling, and what portfolio-wide, board-level intelligence required.*

---

Original analysis: Seth D. Carmody, PhD, Medcrypt, Inc. (published March 2021).
2026 update prepared by the Medcrypt team, July 2026.
*Disclosure: The authors of this paper are employed by Medcrypt Inc., a medical device cybersecurity software developer.*

# SOURCES & ENDNOTES


**1.** HIMSS, "2025 Healthcare Cybersecurity Survey." himss.org/resources/himss-healthcare-cybersecurity-survey/

**2.** Censinet, "Cybersecurity Spending: Healthcare vs. Other Industries"; Cybersecurity Ventures, "Healthcare Industry To Spend $125 Billion On Cybersecurity From 2020 to 2025." censinet.com/perspectives/cybersecurity-spending-healthcare-vs-other-industries ; cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/

**3.** IBM, "Cost of a Data Breach: The Healthcare Industry" (2025); IBM Cost of a Data Breach Report, 2023 & 2024 editions. ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry ; ibm.com/reports/data-breach

**4.** McGlave, Neprash & Nikpay, "Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients" American Economic Journal: Economic Policy 18(1), Feb. 2026; working paper posted to SSRN, Oct. 2023; STAT News, Nov. 17, 2023. aeaweb.org/articles?id=10.1257/pol.20240594 ; papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292 ; statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/

**5.** Choi et al., 2019 Vanderbilt study on data breach remediation and hospital quality (the 2021 paper's source, retained for comparison). pubmed.ncbi.nlm.nih.gov/31506956/ ; pmc.ncbi.nlm.nih.gov/articles/PMC6736905/

**6.** FDA, "Cybersecurity in Medical Devices: Frequently Asked Questions" (Section 524B). fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

**7.** Federal Register, "Refuse to Accept Policy for Cyber Devices," March 30, 2023. federalregister.gov/documents/2023/03/30/2023-06646

**8.** FDA, Final Guidance, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," Sept. 27, 2023. fda.gov/media/173984/download

**9.** Forbes Technology Council (Christian Espinosa), "A Look Back At The Medical Device Cybersecurity Trends Of 2025," Dec. 4, 2025. forbes.com/councils/forbestechcouncil/2025/12/04/a-look-back-at-the-medical-device-cybersecurity-trends-of-2025-where-are-things-now/

**10.** Coherent Market Insights / GlobeNewswire, "Medical Device Security Market to Hit USD 15.02 Billion by 2032," Sept. 4, 2025. globenewswire.com/news-release/2025/09/04/3144680/

**11.** Fortune Business Insights / market.us, healthcare MDR market sizing and CAGR data (2025).

**12.** HIPAA Journal, coverage of the KLAS/Censinet/AHA Healthcare Cybersecurity Benchmarking Study 2025, April 2025. hipaajournal.com/healthcare-cybersecurity-benchmarking-study-2025/

**13.** ElectroIQ, "Remote Patient Monitoring Statistics and Facts (2025)." electroiq.com/stats/remote-patient-monitoring-statistics/

**14.** IBM, "Change Healthcare Attack Expected to Exceed $1 Billion in Costs"; Krebs on Security, Oct. 2024. ibm.com/think/news/change-healthcare-cyberattack-exceeds-1-billion-costs ; krebsonsecurity.com/2024/10/change-healthcare-breach-hits-100m-americans/

**15.** Forbes, "UnitedHealth Group Cyberattack Costs to Eclipse $2.3 Billion This Year," July 16, 2024. forbes.com/sites/brucejapsen/2024/07/16/unitedhealth-group-cyberattack-costs-to-eclipse-23-billion-this-year/

**16.** HIPAA Journal, "2025 Healthcare Data Breach Report." hipaajournal.com/2025-healthcare-data-breach-report/

**17.** NPR/KFF Health News, June 19, 2024; HIPAA Journal, "Ascension Cyberattack 2024." npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses ; hipaajournal.com/ascension-cyberattack-2024/

**18.** HIPAA Journal, "CommonSpirit Health Increases Ransomware Attack Cost Estimate to $160 Million." hipaajournal.com/commonspirit-health-increases-ransomware-attack-cost-estimate-to-160-million/

**19.** HIPAA Journal, "2024 Healthcare Data Breach Report" and "2025 Healthcare Data Breach Report." hipaajournal.com/2024-healthcare-data-breach-report/ ; hipaajournal.com/2025-healthcare-data-breach-report/

**20.** Sophos, "The State of Ransomware in Healthcare 2024." sophos.com/en-us/press/press-releases/2024/09/two-thirds-healthcare-organizations-hit-ransomware-four-year-high

**21.** Sophos, "The State of Ransomware in Healthcare 2025." sophos.com/en-us/blog/the-state-of-ransomware-in-healthcare-2025

**22.** Claroty, "Claroty Completes Acquisition of Healthcare IoT Security Leader Medigate," Jan. 10, 2022. claroty.com/press-releases/claroty-completes-acquisition-of-healthcare-iot-security-leader-medigate

**23.** Axonius, "Axonius Acquires Medical Device Security Specialist Cynerio," July 2025. axonius.com/newsroom/press-release/axonius-acquires-medical-device-security-specialist-cynerio

**24.** ServiceNow, "ServiceNow to Acquire Armis," Dec. 23, 2025. newsroom.servicenow.com/press-releases/details/2025/ServiceNow-to-acquire-Armis-to-expand-cyber-exposure-and-security-across-the-full-attack-surface-in-IT-OT-and-medical-devices-for-companies-governments-and-critical-infrastructure-worldwide/default.aspx

**25.** PR Newswire, "MedCrypt Expands Platform Capabilities as Demand for Medical Device Cybersecurity Solutions Surges," May 29, 2025. prnewswire.com/news-releases/medcrypt-expands-platform-capabilities-as-demand-for-medical-device-cybersecurity-solutions-surges-302468836.html

**26.** RunSafe Security, Medical Device Cybersecurity Index, 2025 & 2026 editions. prnewswire.com/news-releases/runsafe-security-releases-2025-medical-device-cybersecurity-index-amid-surge-in-threats-to-patient-critical-devices-302484559.html

**27.** (ISC)², "2024 Cybersecurity Workforce Study." isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

**28.** (ISC)², "2025 Workforce Study: A Focus on Skills." isc2.org/Insights/2025/12/a-focus-on-skills-isc2-workforce-study

**29.** Cybellum, "The State of Medical Device Security in 2024," Nov. 11, 2024. cybellum.com/blog/the-state-of-medical-device-security-in-2024-challenges-trends-and-ownership-shifts/

**30.** U.S. Government Accountability Office, GAO-25-107755, "Healthcare Cybersecurity: HHS Continues to Have Challenges as Lead Agency," Nov. 13, 2024. gao.gov/products/gao-25-107755

**31.** Alston & Bird, "HIPAA Security Rule: Still on Track for Finalization," Nov. 2025; Federal Register NPRM, Jan. 6, 2025. alston.com/en/insights/publications/2025/11/hipaa-security-rule-overhaul ; federalregister.gov/documents/2025/01/06/2024-30983

**32.** American Hospital Association, coverage of HHS's December 2023 healthcare cybersecurity concept paper. aha.org/news/headline/2023-12-06-hhs-releases-cybersecurity-strategy-health-care-sector

**33.** (See note 30, GAO-25-107755.)

**34.** Congress.gov, S.5218 (HISAA), 118th Congress, introduced Sept. 26, 2024. congress.gov/bill/118th-congress/senate-bill/5218

**35.** Congress.gov, S.3315, Health Care Cybersecurity and Resiliency Act of 2026, 119th Congress. congress.gov/bill/119th-congress/senate-bill/3315/text

**36.** Nixon Peabody, "New York Cybersecurity Regulations for General Hospitals Take Effect October 2, 2025," Sept. 29, 2025. nixonpeabody.com/insights/alerts/2025/09/29/new-york-cybersecurity-regulations-for-general-hospitals-take-effect-october-2-2025

**37.** FDA, Final Premarket Cybersecurity Guidance (see note 8), reissued June 27, 2025. federalregister.gov/documents/2025/06/27/2025-11669

**38.** MedTech Dive, interview with CDRH cybersecurity director Nastassia Tamari, Dec. 16, 2024. medtechdive.com/news/cdrh-cybersecurity-director-regulations-legacy-devices/735225/

**39.** FDA, Quality Management System Regulation, final rule, Feb. 2, 2024. fda.gov/medical-devices/postmarket-requirements-devices/quality-management-system-regulation-qmsr

**40.** FDA, "Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles." fda.gov/medical-devices/software-medical-device-samd/predetermined-change-control-plans-machine-learning-enabled-medical-devices-guiding-principles

**41.** Regulatory Affairs Professionals Society (RAPS), "FDA Acknowledges Shortcomings of Pre-Cert Pilot," Oct. 2022. raps.org/News-and-Articles/News-Articles/2022/10/FDA-acknowledges-shortcomings-of-Pre-Cert-pilot-in

**42.** Food and Drug Omnibus Reform Act of 2022, Pub. L. 117-328, div. FF, tit. III, §3305(a) (adding FD&C Act §524B, 21 U.S.C. §360n-2) and §3308 (adding FD&C Act §515C, 21 U.S.C. §360e-4), Dec. 29, 2022. uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title21-section360n-2 ; federalregister.gov/documents/2024/03/15/2024-05473