2025 State of Healthcare Cybersecurity: Systemic Fragility, Regulatory Reckoning, and the Clinical Continuity Imperative

Executive Summary

The year 2025 represents a pivotal epoch in the history of healthcare cybersecurity, characterized not merely by the volume of data comprised, but by a fundamental transformation in the structural integrity of the healthcare ecosystem. Following the seismic disruptions of 2024—most notably the Change Healthcare incident—the industry entered 2025 with a heightened awareness of its fragility. Yet, the data and forensic analysis from the past twelve months indicate that awareness has not yet translated into effective immunity. Instead, the sector has entered a period of "regulatory reckoning" and "adversarial evolution," where the blast radius of cyberattacks has expanded, and the perimeter of defense has effectively dissolved into a complex, unmanageable web of third-party dependencies.

This report offers an exhaustive year-in-review for healthcare cybersecurity in 2025. It synthesizes data from federal breach reports, industry threat intelligence, legislative texts, and forensic case studies to construct a comprehensive picture of a sector under siege. The narrative emerging from this analysis is one of a "Hub-and-Spoke" crisis. Adversaries have largely abandoned the inefficient targeting of individual hospitals (the spokes) in favor of compromising central technology vendors and clearinghouses (the hubs). This strategic pivot has allowed threat actors to maximize their impact, creating cascading failures that paralyze clinical operations across hundreds of providers simultaneously.

Statistically, 2025 witnessed a paradoxical trend. While the raw number of affected individuals decreased from the historic anomalies of 2024, the frequency of "mega-breaches" stabilized at an unacceptably high baseline. As of October 2025, 364 hacking incidents were reported to the U.S. Department of Health and Human Services (HHS), affecting over 33 million individuals.[1] However, the nature of these attacks has shifted. The "encrypt-and-extort" model of ransomware is ceding ground to pure data extortion, a tactic that leverages the immutability of patient health information (PHI) to coerce payments even when operational backups remain intact.[3]

In response to these escalating threats, the U.S. government initiated the most aggressive regulatory overhaul of the healthcare sector in over a decade. The proposed updates to the HIPAA Security Rule in January 2025, aiming to mandate encryption and multi-factor

authentication (MFA), sparked a fierce debate regarding the financial viability of such measures for rural and under-resourced providers.[4] Simultaneously, the reintroduction of the Health Care Cybersecurity and Resilience Act of 2025 sought to balance these mandates with necessary federal support.[6]

This report also identifies a critical intellectual shift in operational resilience: the transition from "Business Continuity" to "Clinical Continuity." The realization that IT recovery does not equate to patient safety has driven hospitals to adopt 30-day downtime standards and revitalize analog workflows to survive prolonged digital blackouts.[7]

The following sections detail the quantitative threat landscape, the mechanics of new supply chain vectors like the Salesloft Drift incident, the economics of the 2025 ransomware market, and the strategic outlook for 2026.

1. The 2025 Threat Landscape: Quantitative Analysis and Breach Demographics

The metrics defining the 2025 cybersecurity landscape reveal a complex and shifting battlefield. While the aggregate number of breached records receded from the catastrophic highs of 2024, the data indicates a normalization of high-severity incidents, suggesting that "mega-breaches" have become a systemic feature rather than statistical outliers.

1.1 Breach Volume and Scope: A Statistical Deep Dive

As of early October 2025, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) received reports of 364 hacking incidents affecting approximately 33 million Americans.[1] To contextalize this figure, it is essential to compare it against the preceding years. The 2024 figure of 259 million affected individuals was heavily skewed by the Change Healthcare incident, which compromised 192.7 million records alone.[1] When removing such outliers, 2025 reveals a persistent, baseline threat level that has not abated.

In August 2025 alone, 58 large healthcare data breaches (affecting 500 or more individuals) were reported to OCR, marking a 13.7% month-over-month increase.[8] This singular month exposed the PHI of nearly 3.8 million individuals, with an average breach size of over 71,000 records.[8] This consistent drumbeat of compromise—averaging nearly two large breaches per day—demonstrates that while defenders may be preventing some encryption events, they are failing to stem the tide of data exfiltration.

Table 1: Comparative Breach Statistics (2023–2025)

Metric	2023	2024	2025 (YTD Oct)	Trend Analysis
Total Hacking Incidents	~500 (Est.)	739	364 (Projected ~500)	Frequency remains high; stabilization of incident count.
Individuals Affected	138 Million	259 Million	33 Million	Decrease in aggregate volume due to absence of single ~200M outlier, but high persistence of mid-sized breaches.
Primary Location	Network Server	Network Server	Network Server / Email	Continued exploitation of core infrastructure and communication channels.
Primary Vector	Ransomware	Ransomware / Supply Chain	Extortion / Supply Chain	Tactical shift from encryption to pure data theft to bypass backup defenses.

Avg. Cost (US)	~$10.9M	~$11M	$7.42M	Decrease in average cost, though still highest of all industries.[9]

Data synthesized from OCR Breach Portal, AHA Cyber Intel Reports, and IBM Cost of Data Breach Reports.[1]

1.2 Geographic Distribution of Threats

The analysis of breach data reveals a distinct geographic concentration of cyber incidents. Throughout 2025, California, Florida, and Texas consistently led the nation in reported large data breaches.[8] For instance, in August 2025, California reported seven large breaches, followed closely by Florida and Texas with six each.[8]

This distribution is not merely a function of population density but reflects the target-rich environments of these states. These regions possess dense concentrations of interconnected health systems, Regional Health Information Organizations (RHIOs), and massive patient populations. The correlation suggests that threat actors are strategically targeting regions where the "hub-and-spoke" model is most developed, maximizing the potential yield of a single intrusion. Furthermore, the high incidence in Florida—a state with a large elderly population and extensive Medicare infrastructure—aligns with attacker preferences for high-value Medicare ID data, which commands a premium on the dark web.[10]

1.3 The "Hub-and-Spoke" Targeting Strategy

A defining characteristic of the 2025 threat landscape is the crystallization of the "hub-and-spoke" targeting strategy. Adversaries have applied an economic logic to their operations: compromising individual hospitals (spokes) is resource-intensive compared to compromising a central technology vendor (the hub).

- **Third-Party Dominance:** Over 80% of stolen PHI records in 2025 did not originate from hospitals directly. Instead, they were exfiltrated from third-party vendors, business associates, software services, and health plans.[1]
- **The Blast Radius Effect:** This strategy creates a "ransomware blast radius." A single intrusion into a vendor cascades across hundreds of client organizations. This was exemplified by attacks on billing services and cloud providers, where hospitals found themselves operationally paralyzed despite having clean internal networks.[7]
- **Case in Point:** The Change Healthcare breach from 2024 cast a long shadow into 2025, serving as the blueprint for this strategy. The aftermath saw attackers actively seeking similar "single points of failure" within the healthcare supply chain, leading to the high

percentage of third-party breaches recorded this year.[11]

1.4 Vector Analysis: The Rise of Non-Hospital Targets

The data further indicates a shift in *where* the data is stolen. Over 90% of hacked health records were stolen outside of the Electronic Health Record (EHR) system.[1] This statistic is critical for defenders. While billions have been spent securing the EHR "fortress," attackers have simply moved to the periphery—targeting unencrypted data stores, backup servers, and third-party data aggregators.

Crucially, 100% of the hacked data reported in major incidents was unencrypted.[1] This was due to two primary factors:

1. **Stolen Credentials:** Attackers used valid, stolen credentials to access encrypted data, rendering the encryption moot (the "front door" attack).
2. **Improper Storage:** Data was found stored in unencrypted formats outside the secure EHR environment, often in legacy databases or temporary staging servers used by vendors.[2]

2. Anatomy of Supply Chain Fragility: The "Hub-and-Spoke" Crisis

The vulnerability of the healthcare supply chain was the central narrative of 2025. The interdependence of modern healthcare delivery—where a typical hospital relies on hundreds of vendors for everything from billing to blood analysis—has created an attack surface that is impossible to defend with traditional perimeter security.

2.1 The "Clean Source" Principle Violation

The theoretical underpinning of the 2025 supply chain attacks is the violation of the "Clean Source" principle. This security axiom states that all dependencies must be as trustworthy as the object being secured. In 2025, we observed repeated violations of this, where "clean" hospital networks were compromised by "dirty" vendor connections.

The most illustrative example of this vulnerability in 2025 was the incident involving **Salesloft Drift**, which impacted numerous organizations across sectors, including healthcare entities relying on Salesforce integrations.

2.2 Case Study: The Salesloft Drift / Salesforce Incident (August 2025)

In August 2025, a sophisticated supply chain attack targeted the Salesloft Drift chatbot integration, a tool widely used for customer engagement and marketing within Salesforce environments.[12] While not a direct attack on a hospital's clinical infrastructure, this incident exemplified the "Hub-and-Spoke" risk for healthcare payers and administrative bodies managing patient engagement.

- **The Actor:** The campaign was attributed to a threat cluster tracked as **UNC6395** (also known as GRUB1).[13]
- **The Mechanic - "Identities in Transit":** The attackers did not exploit a vulnerability in Salesforce itself. Instead, they compromised the Salesloft Drift application environment. From there, they exfiltrated **OAuth tokens**. These tokens act as "identities in transit"—digital keys that allow the Drift app to talk to the Salesforce instances of its customers without needing a password.[15]
- **The Execution:** Using these stolen tokens, UNC6395 authenticated against the Salesforce instances of hundreds of organizations. They bypassed Multi-Factor Authentication (MFA) because the OAuth token represents a session that has *already* been authenticated.[14]
- **The Exfiltration:** Between August 8 and August 18, 2025, the attackers systematically exfiltrated data. In the case of Cloudflare (a proxy for high-security victims), the attackers used the token to query Salesforce "Case" objects—support tickets that often contain sensitive data, contact details, and sometimes, inadvertently, API keys or passwords.[13]

Implications for Healthcare:
This incident terrified healthcare CISOs because it bypassed the standard defense stack. A hospital could have perfect firewalls, rigorous MFA for all humans, and updated EDR software, yet still lose data because a third-party marketing tool had a valid OAuth token. This represents a "cross-vendor lateral movement" attack, or a $(B2)^n$ attack, where business-to-business links are exploited to hop from vendor to vendor to victim.16 It forced a reassessment of "Non-Human Identity" (NHI) management, highlighting that API keys and tokens are the new perimeter.

2.3 Other Notable Supply Chain Failures

- **Yale New Haven Health (March 2025):** A breach affecting 5.6 million people was traced to a vulnerability in a third-party file transfer service.[18] This echoed the MOVEit attacks of previous years, proving that secure file transfer remains a critical weak point.
- **Episource (February 2025):** A ransomware attack on this medical billing firm compromised 5.4 million records.[19] As a billing vendor, Episource held aggregated data from multiple providers, acting as a classic "hub" target. The breach exposed Social Security numbers, diagnoses, and insurance details, reinforcing the risk of aggregating high-value data in vendor environments.

3. Evolution of Adversarial Tradecraft: The Extortion Economy

In 2025, cybercriminal syndicates targeting healthcare demonstrated a rational economic shift in their tactics, techniques, and procedures (TTPs). The "encrypt-and-extort" model, while still prevalent, began to cede ground to "extortion-only" attacks, driven by the changing defenses of healthcare organizations.

3.1 The Shift to Pure Extortion

The most significant tactical evolution in 2025 was the decoupling of encryption from extortion. According to Sophos, the percentage of healthcare attacks involving **data extortion without encryption tripled to 12% in 2025**, up from just 4% in previous years.[3] Conversely, the rate of successful data encryption dropped to a five-year low of 34%.[3]

Drivers of this Shift:

1. **Resilience of Backups:** Healthcare organizations have invested heavily in immutable backups (backups that cannot be altered or deleted). This has made encryption less effective as a leverage point because hospitals can restore their systems without paying for a decryption key.[3]
2. **Speed and Stealth:** Encrypting thousands of endpoints is a noisy process that triggers EDR alarms and requires significant "dwell time" on the network. Exfiltrating data can be done quieter and faster, reducing the chance of detection before the damage is done.
3. **Leverage via Privacy:** The threat of leaking sensitive medical history (e.g., mental health, HIV status, oncology, addiction treatment) exerts immense pressure on healthcare boards. The reputational damage and regulatory fines associated with a HIPAA breach often outweigh the cost of operational downtime.[22]

3.2 Ransomware Economics and Payment Trends

The healthcare sector demonstrated increased resistance to ransom demands in 2025. Only **36% of healthcare providers paid a ransom**, a sharp decline from 61% in 2022.[3] This makes healthcare one of the sectors least likely to pay, a testament to improved backup strategies and a hardened stance against funding criminal enterprise.

However, the economics are nuanced:

- **Demand vs. Payment:** The average ransom *demand* plummeted 91% to $343,000 (down from $4 million in 2024). This drastic drop likely reflects a "volume-based" strategy by attackers—targeting smaller entities (clinics, rural hospitals) with lower, more "affordable" demands to ensure payment, rather than swinging for multi-million dollar payouts from large systems that have the resources to refuse.[3]

- **Double Layered Extortion:** Despite the drop in payments, "double-layered extortion" (ransomware coupled with data theft) remained standard operating procedure. Threat groups like **Blackcat/ALPHV**, **Qilin**, and **RansomHub** continued to utilize this tactic, ensuring they had two avenues for monetization.[1]

3.3 The Dark Web Marketplace for PHI

The economic engine driving these attacks is the high value of Protected Health Information (PHI) on the dark web. Unlike credit card numbers, which can be cancelled, medical histories and Social Security numbers are immutable.

- **Pricing:** A complete PHI package (SSN + Medical History) commanded prices up to **$1,200 per record** in 2025.[10] In comparison, credit card data often sells for $5-$15.
- **Utility:** This data enables long-term fraud, including medical identity theft (obtaining expensive services/drugs), tax fraud, and sophisticated social engineering. This 80x value differential explains why healthcare remains the primary target for data theft.[10]

3.4 AI-Driven Social Engineering and "Quishing"

2025 saw the weaponization of Artificial Intelligence in social engineering campaigns, increasing the success rate of initial access attempts.

- **Phishing at Scale:** AI tools allowed attackers to generate perfectly localized, typo-free phishing emails at scale. This nullified traditional security training that taught staff to look for poor grammar or awkward phrasing.[24]
- **"Quishing" (QR Phishing):** The use of malicious QR codes in emails (to bypass email security scanners) became a prominent vector.
- **Deepfake Threats:** Physical security was challenged by AI-generated deepfake badges and voice cloning. Attackers used voice cloning to bypass IT helpdesk verification protocols, resetting passwords for high-privilege accounts.[25] Furthermore, "fake IT worker" scams proliferated, where North Korean and other nation-state actors used AI to pass interviews and gain employment at healthcare tech firms, providing them insider access.[26]

---

4. High-Profile Incidents of 2025: Case Studies in Fragility

While the Change Healthcare shadow loomed large, 2025 had its own roster of significant breaches that illustrated the diversity of the threat landscape.

4.1 Ascension Health System (May 2025)

In May 2025, Ascension, one of the nation's largest non-profit health systems operating 140 hospitals, suffered a significant ransomware attack.[11]

- **Operational Impact:** The attack forced the diversion of ambulances and the postponement of elective procedures. Crucially, it forced clinical staff to revert to manual, paper-based charting for an extended period.
- **The "Human Element":** Reports indicate the breach began with a single employee downloading a malicious file. This highlighted that despite millions spent on technology, the "human firewall" remains a critical point of failure.[22]
- **Lesson:** The incident underscored that "business continuity" (restoring IT) is distinct from "clinical continuity" (treating patients safely without IT).

4.2 Yale New Haven Health (March 2025)

This breach impacted 5.6 million patients. Hackers accessed a network server, copying names, birthdates, and medical record numbers.[19]

- **The Third-Party Link:** The breach was traced to a vulnerability in a third-party file transfer service. This was a direct echo of the CL0P/MOVEit attacks, reinforcing that secure file transfer remains a persistent weakness in the sector.
- **Legal Consequences:** Yale New Haven Health agreed to an **$18 million settlement** regarding allegations of inadequate cybersecurity controls, setting a high benchmark for liability in 2025.[18]

4.3 Blue Shield of California (April 2025): The Pixel Problem

Not all breaches were hacks. Blue Shield of California suffered a data leak impacting 4.7 million records due to a **Google Analytics misconfiguration**.[18]

- **The Mechanic:** Improper tagging in the GA4 tracking scripts meant that sensitive member data (names, policy numbers, demographic details) was being transmitted to third-party analytics endpoints.
- **The Lesson:** This incident highlighted the risks of "Shadow IT" and marketing technologies. It demonstrated how the aggressive use of data analytics can inadvertently lead to massive HIPAA violations if not rigorously governed by privacy engineers.

---

5. The Regulatory Tsunami: Legislative and Rulemaking Shifts

If 2024 was the year of the breach, 2025 was the year of the regulator. The federal government, losing patience with the voluntary adoption of cybersecurity standards, moved aggressively toward mandatory requirements, sparking intense friction with the provider community.

5.1 HIPAA Security Rule Update (Proposed Jan 2025)

On January 6, 2025, HHS published the first major update to the HIPAA Security Rule since 2013.[4] The proposal aimed to transition "addressable" implementation specifications to "required" ones, effectively removing the wiggle room that organizations had used for a decade.

Key Mandates:

1. **Universal Encryption:** The proposal mandated encryption for *all* electronic Protected Health Information (ePHI) both at rest and in transit. Previously, this was often treated as "addressable," allowing organizations to use alternative measures if encryption was deemed technically unfeasible.[4]
2. **Multi-Factor Authentication (MFA):** Required for *all* systems accessing ePHI, eliminating flexibility.
3. **Asset Inventory:** Mandatory maintenance of detailed technology asset inventories and network maps—a direct response to the "shadow IT" problem.[27]
4. **Strict Timeline:** A compliance window of just 240 days post-finalization.[5]

Industry Pushback (The CHIME Letter):
The proposal faced vehement opposition. Over 100 hospital systems and associations, led by the College of Healthcare Information Management Executives (CHIME), signed a letter to HHS Secretary Robert F. Kennedy Jr. on December 8, 2025, demanding the withdrawal of the rule.5

- **The Argument:** They argued the "one-size-fits-all" approach would bankrupt rural providers. They estimated compliance costs at **$34 billion over five years** (vs. HHS's $9 billion estimate), arguing this unfunded mandate would force existential choices between buying cybersecurity tools and keeping the emergency room open.[4]
- **Rural Impact:** The letter highlighted that a 15-bed rural clinic cannot sustain the same cybersecurity infrastructure as a major academic medical center.

5.2 Health Care Cybersecurity and Resilience Act of 2025

Reintroduced by bipartisan Senators Cassidy, Warner, Hassan, and Cornyn, this bill (S. 1851) sought to codify the partnership between HHS and the Cybersecurity and Infrastructure Security Agency (CISA).[6]

- **Grants vs. Fines:** Unlike the punitive nature of the HIPAA update, this Act focused on support. It authorized **grants** specifically for rural health clinics and hospitals to fund cybersecurity upgrades, acknowledging the "resource gap" identified by CHIME.[28]

- **Incident Response:** It required HHS to develop a sector-specific incident response plan and mandated the public reporting of the *number* of individuals affected by breaches, increasing transparency.[29]
- **Status:** As of late 2025, the bill was advancing, seen as the legislative "carrot" to the regulatory "stick".[30]

---

6. Operational Resilience: The "Clinical Continuity" Paradigm

A critical intellectual shift occurred in 2025 regarding how hospitals plan for disasters. The industry moved from IT-centric "Business Continuity" to patient-centric "Clinical Continuity."

6.1 The 30-Day Downtime Standard

The American Hospital Association (AHA) and other bodies began advocating for downtime procedures that account for a loss of mission-critical services for **30 days or longer**.[7]

- **The Reality Gap:** Previous plans often assumed outages of 24-72 hours. Ransomware incidents in 2024-2025 (like Ascension) proved that full recovery often takes 3-4 weeks.
- **Clinical vs. Business Continuity:** Hospital leadership realized that "Business Continuity" plans often focused on revenue cycle and email restoration. "Clinical Continuity" asks harder questions: *How do we diagnose a stroke without a PACS system? How do we verify drug interactions without an e-prescribing database? How do we deliver radiation therapy when linear accelerators are offline?*.[7]

6.2 The "Blast Radius" Defense

Hospitals began to map their "ransomware blast radius"—identifying which clinical functions would fail if a specific third-party vendor went dark.

- **Dependency Mapping:** Best practices in 2025 involved rigorous data mapping to understand dependencies on network-connected medical devices and external SaaS platforms.
- **Paper Charting Proficiency:** Paradoxically, the most advanced defense in 2025 was the re-training of clinical staff on manual, paper-based workflows. Hospitals conducted drills where staff had to run codes and manage admissions using physical paper for extended periods, ensuring muscle memory for analog care.[31]

6.3 Best Practices for Continuity Exercises

Based on 2025 tabletop exercise guidelines [32], effective clinical continuity planning now requires:

1. **Specific Scenarios:** Testing not just "outage," but specific scenarios like "Ransomware encryption of the PACS server" or "Cloud EMR unavailability."
2. **Cross-Functional Teams:** Exercises must include Chief Medical Officers and nursing leadership, not just IT.
3. **Communication Failover:** Testing alternative communication channels (e.g., runner systems, encrypted messaging apps) when VoIP and email are down.

---

7. Financial Dimensions of Healthcare Cybersecurity

The economics of healthcare cybersecurity in 2025 reflected a sector under siege but adapting to the pressure through financial instruments and shifting insurance dynamics.

7.1 Cost of a Data Breach

According to the **2025 Cost of a Data Breach Report** by IBM, the average cost of a healthcare breach in the U.S. was **$7.42 million**.[9]

- **Trend:** This represented a decrease of $2.35 million from 2024 highs. However, healthcare remained the **costliest industry** for data breaches for the 14th consecutive year.[9]
- **Why so expensive?:** Healthcare breaches took the longest to identify and contain—an average of **279 days** (compared to a global average of 241 days).[9] This extensive "dwell time" allows attackers to harvest more data and necessitates deeper, more expensive forensic cleanups.
- **Consumer Impact:** Nearly half of breached organizations reported raising prices to cover these costs, suggesting that cyber insecurity is directly contributing to medical inflation.[9]

7.2 Cyber Insurance Market Stabilization

Contrary to the skyrocketing premiums of 2021-2023, the cyber insurance market in 2025 showed signs of stabilization and "softening."

- **Premiums:** Rates remained relatively flat or saw slight decreases (0.2% to 1.6% in the U.S.).[36]
- **Decoupling:** Insurers began decoupling encryption coverage from extortion coverage. Since backups have improved, companies often don't need to pay ransoms for decryption. However, they heavily need coverage for the legal fallout of data theft (class action lawsuits, regulatory fines).
- **Prerequisites:** Obtaining insurance in 2025 required rigorous proof of hygiene. **MFA, EDR (Endpoint Detection and Response), and immutable backups** became non-negotiable prerequisites. Organizations without these controls were effectively uninsurable.[37]

8. Emerging Technology Risks: IoMT and AI

As hospitals digitized further, the attack surface expanded through the Internet of Medical Things (IoMT) and AI integration.

8.1 Internet of Medical Things (IoMT) Vulnerabilities

By 2025, the proliferation of connected devices (infusion pumps, pacemakers, diagnostic equipment) became a critical risk vector. It is predicted that by 2026, smart hospitals will deploy over 7 million IoMT devices.[39]

- **The Patching Problem:** Many of these devices run on legacy operating systems that cannot be easily patched without regulatory recertification.
- **Impact:** Vulnerabilities in these devices (like those found in infusion pumps) were flagged as major risks for patient safety.
- **Defense:** Mature organizations accelerated the adoption of **Zero Trust architectures** and network segmentation, isolating IoMT devices in "green zones" to prevent lateral movement to the main EHR.[40]

8.2 AI: The Double-Edged Sword

- **AI as a Threat:** As noted, AI facilitated highly effective phishing and deepfake social engineering.
- **AI as a Defense:** Conversely, defenders increasingly relied on AI-driven SOC (Security Operations Center) tools. Organizations using AI and automation in cybersecurity detected and contained incidents **98 days faster** than those that did not.[41] This "AI vs. AI" dynamic is defining the modern SOC.

9. Strategic Outlook: 2026 and Beyond

Looking toward 2026, the trajectory suggests a "Year of the Defender" characterized by the forced maturation of cybersecurity practices and the automation of defense.

9.1 Predictions for 2026

- **Autonomous Defense:** We anticipate a shift toward "autonomous AI agents" in defense. The ratio of machine-to-human identity management (82:1) will necessitate automated governance that can act at machine speed.[42]
- **Liability Shifts:** 2026 may see the first major lawsuits holding executives personally liable for rogue AI actions or gross negligence in cybersecurity governance. The "New Gavel"

will elevate cyber risk to a board-level liability issue.[42]

- **Quantum Preparation:** With "harvest now, decrypt later" threats looming, 2026 will likely mark the beginning of serious investment in **post-quantum cryptography (PQC)** for long-retention health data. Data stolen today could be decrypted by quantum computers in the near future, making crypto-agility a new requirement.[42]

9.2 Strategic Recommendations for 2026

Based on the lessons of 2025, healthcare organizations must prioritize the following:

1. **Clinical Continuity Drills:** Move beyond IT tabletop exercises. Conduct full-scale drills with clinical staff simulating a 30-day EHR outage.
2. **Third-Party Risk Rigor:** Implement continuous monitoring of third-party vendors. The "Salesloft" incident proved that static annual questionnaires are insufficient.
3. **Identity Hardening:** With the rise of OAuth abuse, organizations must rigorously audit non-human identities (API keys, tokens) and enforce least-privilege principles for SaaS integrations.
4. **Cyber Performance Goals:** Align internal security frameworks with the forthcoming mandatory standards from HHS to avoid regulatory penalties and ensure insurability.

Conclusion

The year 2025 was defined by the realization that healthcare cybersecurity is no longer solely a technical challenge but a patient safety imperative and a national security concern. The stabilization of breach volumes masks a more dangerous reality: attacks are becoming targeted, extortion-based, and systemic via the supply chain.

The friction between necessary regulatory mandates and the economic fragility of healthcare providers defined the political landscape of the year. However, the emerging consensus is clear: the cost of insecurity—measured in diverted ambulances, delayed cancer treatments, and exposed private histories—far exceeds the cost of defense. As the industry moves into 2026, the focus must remain resolutely on **resilience**: the ability to deliver care even when the digital lights go out.

Works cited

1. 2025 Cybersecurity Year in Review, Part One: Breaches and ..., accessed December 16, 2025, https://www.aha.org/news/aha-cyber-intel/2025-10-07-2025-cybersecurity-year-review-part-one-breaches-and-defensive-measures
2. Healthcare cybersecurity so far in 2025: 5 notes - Becker's Hospital Review, accessed December 16, 2025, https://www.beckershospitalreview.com/healthcare-information-technology/ehrs/healthcare-cybersecurity-so-far-in-2025-5-notes/

3. How Healthcare Ransomware Attacks Shifted In 2025 - J&R Report, accessed December 16, 2025, https://jrreport.wordandbrown.com/2025/12/02/how-healthcare-ransomware-attacks-shifted-in-2025/
4. HHS Proposes Major 2025 Update to HIPAA Security Rule - Morgan Lewis, accessed December 16, 2025, https://www.morganlewis.com/pubs/2025/01/hhs-proposes-major-2025-update-to-hipaa-security-rule
5. Hospitals Pushback on Proposed HIPAA Security Rule Updates, accessed December 16, 2025, https://compliancy-group.com/pushback-on-proposed-hipaa-security-rule-updates/
6. Bill Reintroduced to Strengthen Healthcare Cybersecurity - The HIPAA Journal, accessed December 16, 2025, https://www.hipaajournal.com/health-care-cybersecurity-resiliency-act-2025/
7. 2025 Cybersecurity Year in Review, Part Two: Mitigating Third-Party ..., accessed December 16, 2025, https://www.aha.org/news/aha-cyber-intel/2025-10-21-2025-cybersecurity-year-review-part-two-mitigating-third-party-risk-ensuring-clinical
8. August 2025 Healthcare Data Breach Report - The HIPAA Journal, accessed December 16, 2025, https://www.hipaajournal.com/august-2025-healthcare-data-breach-report/
9. Average Cost of a Healthcare Data Breach Falls to $7.42 Million, accessed December 16, 2025, https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-2025/
10. Healthcare Cybersecurity Statistics 2025 - Total Assure Blog, accessed December 16, 2025, https://www.totalassure.com/blog/healthcare-cybersecurity-statistics-2025
11. 2025 Healthcare Cybersecurity Review: Breaches & Defense - SecureTrust ZTX Platform, accessed December 16, 2025, https://blog.securetrust.io/2025-healthcare-cybersecurity-review-breaches-defense/
12. Salesloft Drift Breach: What Happened and How Does It Affect Me? | UpGuard, accessed December 16, 2025, https://www.upguard.com/blog/salesloft-drift-breach
13. The impact of the Salesloft Drift breach on Cloudflare and our customers, accessed December 16, 2025, https://blog.cloudflare.com/response-to-salesloft-drift-incident/
14. Cybersecurity Alert – Salesloft Drift AI Supply Chain Attack | FINRA.org, accessed December 16, 2025, https://www.finra.org/rules-guidance/guidance/salesloft-drift-AI-supply-chain-attack
15. The Salesloft–Drift Breach: An Attack Path Case Study - SpecterOps, accessed December 16, 2025, https://specterops.io/blog/2025/09/24/the-salesloft-drift-breach-an-attack-path-case-study/
16. The Salesloft Drift breach: A cross-vendor attack | Silverfort, accessed December 16, 2025, https://www.silverfort.com/blog/the-salesloft-drift-breach-a-cross-vendor-lateral-movement-attack-that-requires-a-new-shared-security-model/

17. Salesloft Drift Supply Chain Incident: Key Details and Zscaler's Response, accessed December 16, 2025, https://www.zscaler.com/blogs/company-news/salesloft-drift-supply-chain-incident-key-details-and-zscaler-s-response
18. Top 10 Data Breaches of 2025 | Guardz.com, accessed December 16, 2025, https://guardz.com/blog/top-recent-data-breaches/
19. 60+ Healthcare Data Breach Statistics (Oct - 2025) - Bright Defense, accessed December 16, 2025, https://www.brightdefense.com/resources/healthcare-data-breach-statistics/
20. How healthcare ransomware attacks are shifting in 2025, accessed December 16, 2025, https://www.fiercehealthcare.com/health-tech/how-healthcare-ransomware-attacks-are-shifting-2025
21. 50+ Ransomware Statistics for 2025 - Spacelift, accessed December 16, 2025, https://spacelift.io/blog/ransomware-statistics
22. Healthcare Data Breaches 2025 Statistics: $10.22M Cost - DeepStrike, accessed December 16, 2025, https://deepstrike.io/blog/healthcare-data-breaches-2025-statistics
23. How Healthcare Ransomware Attacks Shifted in 2025 - HLTH, accessed December 16, 2025, https://hlth.com/insights/news/how-healthcare-ransomware-attacks-shifted-in-2025-2025-11-28
24. AI is making phishing smarter and healthcare systems more vulnerable - Paubox, accessed December 16, 2025, https://www.paubox.com/blog/ai-is-making-phishing-smarter-and-healthcare-systems-more-vulnerable
25. New AI-Powered Physical Threats to Healthcare—and How to Prepare, accessed December 16, 2025, https://optimumhit.com/insights/blog/digital-transformation/new-ai%E2%80%91powered-physical-threats-to-healthcare-and-how-to-prepare/
26. Unmasking the AI-powered, remote IT worker scams threatening businesses worldwide, accessed December 16, 2025, https://www.weforum.org/stories/2025/12/unmasking-ai-powered-remote-it-worker-scams-threatening-businesses-worldwide/
27. HHS Proposed Rule Would Increase Cybersecurity Requirements for Electronic Health Data, accessed December 16, 2025, https://ogletree.com/insights-resources/blog-posts/hhs-proposed-rule-would-increase-cybersecurity-requirements-for-electronic-health-data/
28. Healthcare cybersecurity bill promises increased guidance, grants for industry, accessed December 16, 2025, https://www.fiercehealthcare.com/digital-health/cassidy-introduces-healthcare-cybersecurity-bill-increased-guidance-grants-security
29. Health Care Cybersecurity and Resiliency Act of 2025 SECTION, accessed December 16, 2025, https://www.help.senate.gov/imo/media/doc/health_care_cybersecurity_and_resiliency_act_of_2025_section-by-section.pdf
30. Lawmakers advance Health Care Cybersecurity and Resilience Act 2025,

accessed December 16, 2025, https://hipaatimes.com/lawmakers-advance-health-care-cybersecurity-and-resilience-act-2025

31. Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field, accessed December 16, 2025, https://www.aha.org/system/files/media/file/2025/02/Change-Healthcare-Cyberattack-Underscores-Urgent-Need-to-Strengthen-Cyber-Preparedness.pdf
32. 9 Business Continuity Plan Testing Scenarios & Tabletop Exercises - Invenio IT, accessed December 16, 2025, https://invenioit.com/continuity/continuity-plan-testing-scenarios/
33. 15 Tabletop Exercise Examples to Prepare for Emergency – Most Common Scenarios, accessed December 16, 2025, https://www.alert-software.com/blog/tabletop-exercise-examples-for-emergency-preparedness
34. 60+ Key Data Breach Statistics for 2025 - Spacelift, accessed December 16, 2025, https://spacelift.io/blog/data-breach-statistics
35. 110+ of the Latest Data Breach Statistics to Know for 2026 & Beyond - Secureframe, accessed December 16, 2025, https://secureframe.com/blog/data-breach-statistics
36. Cyber Insurance Statistics 2025: Market, Threats, and Claims Data - DeepStrike, accessed December 16, 2025, https://deepstrike.io/blog/cyber-insurance-statistics-2025
37. The 2025 Cyber Insurance Trends Report - Huntress, accessed December 16, 2025, https://www.huntress.com/blog/cyber-insurance-trends
38. The State of Cyber Liability Insurance in 2025 | Omega Systems, accessed December 16, 2025, https://omegasystemscorp.com/insights/blog/the-state-of-cyber-insurance-trends-challenges-best-practices/
39. 2026 Healthcare Cybersecurity Trends: What IT Leaders Should Expect Next Year, accessed December 16, 2025, https://meriplex.com/2026-healthcare-cybersecurity-trends-what-it-leaders-should-expect-next-year/
40. Cybersecurity statistics 2025: trends, costs & insights - NordLayer, accessed December 16, 2025, https://nordlayer.com/blog/cybersecurity-statistics-of-2025/
41. 120+ Latest Healthcare Cybersecurity Statistics for 2025 - Dialog Health, accessed December 16, 2025, https://www.dialoghealth.com/post/healthcare-cybersecurity-statistics
42. Palo Alto Networks makes 2026 cyber predictions - APDR - Asia Pacific Defence Reporter, accessed December 16, 2025, https://asiapacificdefencereporter.com/palo-alto-networks-makes-2026-cyber-predictions/
43. Palo Alto Networks Forecasts 6 Predictions on Securing the New AI Economy for 2026, accessed December 16, 2025, https://investors.paloaltonetworks.com/news-releases/news-release-details/palo-alto-networks-forecasts-6-predictions-securing-new-ai/

44. Top cybersecurity companies to watch in 2026 - Nomios Germany, accessed December 16, 2025, https://www.nomios.de/en/news-blog/top-cybersecurity-companies-2026/