SEALD HEALTHCARE

Compliance vs. Security in Healthcare

Why HIPAA Compliance Is Not Enough and Why Data-Layer Security Is Required

White Paper | 2026 Edition

Seald Healthcare, Inc.
www.sealdhealthcare.com | charlie@sealdhealthcare.com

Table of Contents

Executive Summary

1. The Numbers Are Getting Worse, Not Better
- 1.1 The Headline Breaches
- 1.2 The Cumulative Toll
- 1.3 The Financial Reality

2. Why Compliance Has Not Stopped the Bleeding
- 2.1 What HIPAA Requires and What It Does Not
- 2.2 The Expanding Attack Surface

3. Why Cloud Adoption Has Not Solved the Problem

4. Why Traditional Encryption Falls Short

5. What Data-Layer Security Actually Means

6. How Seald Healthcare Works
- 6.1 End-to-End Encryption for Healthcare
- 6.2 Persistent Access Policies
- 6.3 AI-Powered Policy Management
- 6.4 Tamper-Evident Audit Trails
- 6.5 SDK-First Integration
- 6.6 Automatic Key Management
- 6.7 Group and Role-Based Access

7. What This Looks Like in Practice
- 7.1 Vendor Breach
- 7.2 Insider Threat
- 7.3 Ransomware Attack
- 7.4 Tracking Technology Exposure

8. Why This Cannot Wait
- 8.1 Third-Party Risk is Accelerating
- 8.2 AI Adoption is Expanding the Attack Surface
- 8.3 Regulatory Enforcement is Tightening
- 8.4 Cyber Insurance is Demanding More
- 8.5 Post-Quantum Cryptography is Coming

9. Getting Started

10. Conclusion

References

Executive Summary

Healthcare does not have a compliance problem. It has a data security problem. Between 2009 and 2024, more than 846 million patient records were exposed or impermissibly disclosed in reported healthcare data breaches, according to the HHS Office for Civil Rights breach portal (HIPAA Journal, 2026). In 2024 alone, roughly 276 million records were compromised, a 64% increase over the previous year's already record-breaking total (HIPAA Journal, 2024 Healthcare Data Breach Report). The single largest incident, a ransomware attack on Change Healthcare, affected an estimated 192.7 million individuals, nearly two-thirds of the U.S. population (HHS OCR, 2025).

Healthcare has led all industries in data breach costs for 14 consecutive years. The IBM/Ponemon Cost of a Data Breach Report for 2024 placed the average healthcare breach cost at $9.77 million, more than double the global cross-industry average of $4.88 million (IBM, 2024). That figure dropped to $7.42 million in the 2025 report, still the highest of any industry by a wide margin (IBM/HIPAA Journal, 2025).

None of this happened because healthcare organizations failed to pursue compliance. Most breached organizations held HIPAA compliance certifications, had adopted cloud platforms from AWS or Azure, and employed dedicated security teams. They were compliant. They were not secure.

The problem is structural. HIPAA and related frameworks protect systems. They do not protect data once it leaves the perimeter, crosses organizational boundaries, or sits inside an application in plaintext. And in modern healthcare, PHI moves constantly: between providers, billing systems, clearinghouses, payers, analytics platforms, AI tools, and dozens of third-party vendors.

This paper examines why compliance does not equal security, walks through the breach data that proves it, explains why traditional encryption models fail in healthcare workflows, and describes how Seald Healthcare addresses this gap by encrypting PHI at the source with persistent, policy-driven controls that travel with the data wherever it goes.

1. The Numbers Are Getting Worse, Not Better

The healthcare breach landscape is not improving. Despite growing awareness, increasing investment in cybersecurity tools, and tightening regulatory enforcement, the data tells a clear story: breaches are getting bigger, more frequent, and more damaging.

1.1 The Headline Breaches

Some breaches deserve to be examined individually because they illustrate how deeply the current approach to healthcare security has failed.

Change Healthcare (2024): In February 2024, a BlackCat/ALPHV ransomware affiliate accessed the Change Healthcare network through a Citrix remote access portal that lacked multi-factor authentication. Over nine days, the attackers exfiltrated data before deploying ransomware. UnitedHealth Group paid a $22 million ransom, which the attackers pocketed in an exit scam without restoring data. The final count: 192.7 million individuals affected, making it the largest healthcare data breach in history. Change Healthcare processed roughly 15 billion healthcare transactions annually. The outage that followed disrupted claims processing, payment systems, and pharmacy transactions across the entire country for weeks (HIPAA Journal; HHS OCR; UnitedHealth Group testimony, 2024).

Anthem Inc. (2015): For nearly a decade, the Anthem breach held the record at 78.8 million individuals. Anthem paid $16 million to HHS to settle potential HIPAA violations, which was the largest HIPAA settlement ever at the time (HIPAA Journal).

MOVEit Mass Exploitation (2023): The Clop ransomware group exploited a zero-day vulnerability in the MOVEit file transfer tool, compromising more than 2,500 organizations worldwide. Hundreds of healthcare entities were affected, and the total number of stolen healthcare records likely runs into the tens of millions. The attack demonstrated how a single vendor vulnerability can cascade across an entire industry in days (HIPAA Journal, 2024 Report).

Kaiser Foundation Health Plan (2024): Kaiser exposed data belonging to 13.4 million members not through hacking, but through tracking technologies embedded in its websites and applications that transmitted patient data to third-party vendors including Meta, Google, and Microsoft. This breach was entirely preventable and entirely legal under many current compliance frameworks (HIPAA Journal).

1.2 The Cumulative Toll

The individual headlines are alarming. The cumulative picture is worse.

According to the HIPAA Journal's analysis of OCR data, 6,759 large healthcare data breaches (affecting 500 or more individuals) were reported between 2009 and 2024. Those breaches exposed the records of 846,962,011 individuals. That is not a typo. More than 846 million records in an industry serving roughly 330 million Americans (HIPAA Journal, Healthcare Data Breach Statistics, updated February 2026).

In 2024 specifically, 742 large data breaches were reported to OCR. Across those breaches, 276,775,457 records were compromised, approximately 81% of the U.S. population. At least 36 of those breaches each affected 500,000 or more individuals. Fourteen breaches each affected more than one million people (HIPAA Journal, 2024 Report).

This was not an anomaly year. It was the third consecutive year with more than 700 large breaches reported. Hacking-related breaches jumped 239% between 2018 and 2023, and ransomware incidents surged 278% over the same period (HIPAA Journal).

In 2025, the numbers have improved somewhat: approximately 697 large breaches affecting around 61 million individuals, a substantial reduction from 2024, though that comparison is skewed by the massive Change Healthcare outlier. The underlying trend line, when you remove the single largest incidents, continues upward (HIPAA Journal, December 2025 Report).

1.3 The Financial Reality

Breaches do not just harm patients. They impose enormous financial costs on organizations.

IBM's 2024 Cost of a Data Breach Report found that healthcare breaches cost an average of $9.77 million, down from $10.93 million in 2023 but still nearly double the next most expensive industry (financial services at $6.08 million). The 2025 IBM report shows a further decline to $7.42 million per breach, but healthcare has remained the most expensive sector for 14 consecutive years (IBM/Ponemon Institute, 2024 and 2025 Reports).

Beyond direct costs, organizations face regulatory penalties from HHS OCR, state attorneys general, and international regulators. OCR closed 22 HIPAA investigations with financial penalties in 2024, and 2025 is on pace to be a record year for HIPAA enforcement, driven by OCR's new risk analysis enforcement initiative (HIPAA Journal). Class-action lawsuits are increasingly common. Nebraska's attorney general filed suit against UnitedHealth Group over the Change Healthcare breach, and that case survived a motion to dismiss in 2025. Nearly half of breached healthcare organizations raise prices to cover breach costs (IBM, 2024).

UnitedHealth Group alone spent $3.1 billion responding to the Change Healthcare attack in 2024 (Cybersecurity Dive). That number captures just one organization responding to one breach.

2. Why Compliance Has Not Stopped the Bleeding

Healthcare organizations that suffer major breaches are rarely non-compliant. Most have completed HIPAA risk assessments, signed Business Associate Agreements, implemented access controls, and adopted cloud platforms with security certifications. The breaches happen anyway and they happen at scale; they are rarely limited in their scale.

Compliance provides essential organizational discipline. But compliance was designed to answer one question: have the required safeguards been implemented? Security must answer a different question: can sensitive data be accessed, copied, or misused during real workflows, even when systems are compromised?

2.1 What HIPAA Requires and What It Does Not

HIPAA's Security Rule requires covered entities and business associates to implement reasonable safeguards for electronic PHI. The rule is intentionally flexible, allowing organizations to choose measures appropriate to their size and risk profile. That flexibility creates gaps (HHS, 45 CFR Part 164):

- HIPAA does not mandate end-to-end encryption. Encryption is classified as an "addressable" specification, meaning organizations can satisfy it by documenting why they chose not to encrypt and implementing an alternative measure.
- HIPAA allows broad administrative and service-account access to PHI. There is no requirement that access be cryptographically enforced or that decryption keys be separated from infrastructure credentials.
- HIPAA does not restrict decryption inside applications. Once data reaches an authorized system, it can exist in plaintext across memory, logs, caches, and temporary storage.
- HIPAA does not protect PHI after sharing beyond requiring a Business Associate Agreement, which is a contractual control, not a technical one. A BAA cannot prevent a third party from storing or mishandling plaintext data.
- HIPAA does not require tamper-evident, cryptographic audit trails. Organizations may rely on system logs that can be altered, deleted, or incomplete.

The result: an organization can pass a HIPAA audit and still have PHI sitting in plaintext across dozens of systems, vendor environments, and shared workflows. This is not a theoretical risk. It is how every major breach described in Section 1 occurred.

2.2 The Expanding Attack Surface

A modern healthcare organization may share PHI with EHR vendors, billing and coding platforms, clearinghouses, insurance payers, telehealth systems, analytics tools, AI platforms, cloud providers, Health Information Exchanges, and numerous consultants, auditors, and service providers. Each connection is a point where PHI may be decrypted, cached, logged, or exposed. The average hospital works with more than 1,300 vendors (Ponemon Institute).

HIPAA's framework of BAAs and organizational policies was not designed to enforce technical protections across this kind of sprawl. And it does not.

3. Why Cloud Adoption Has Not Solved the Problem

Cloud platforms like AWS, Azure, and Google Cloud provide strong infrastructure security: physical data centers, hardware isolation, availability, and baseline compliance certifications. But cloud security operates under a shared responsibility model. The provider secures the infrastructure. The customer is responsible for securing the data, applications, and access controls running on that infrastructure (AWS Shared Responsibility Model; Azure Shared Responsibility).

This distinction is frequently misunderstood. Migrating to AWS does not mean PHI is encrypted end-to-end, that administrators cannot access plaintext data, or that policies travel with data after sharing. Cloud encryption at rest and in transit protect data while stored on disk and while moving over a network. Both protections end the moment an application processes the data. At that point, PHI is plaintext.

Healthcare breaches most often result from credential compromise, misconfiguration, third-party attacks, insider threats, and ransomware (Verizon DBIR, 2024). In every one of these scenarios, the cloud infrastructure performs exactly as designed. The breach occurs because PHI exists in plaintext at the application layer, accessible to anyone with sufficient credentials or access.

4. Why Traditional Encryption Falls Short

Encryption at rest protects data on disk but is transparent to applications. Data is automatically decrypted when accessed by any authorized service or user. It does not prevent a compromised administrator from querying the database and reading every record in plaintext. It protects against one threat: physical theft of storage media, a risk largely mitigated by cloud data center security.

Encryption in transit (TLS/SSL) protects the communication channel. Data is decrypted at each endpoint, including every server, load balancer, API gateway, and application that processes it. TLS protects the pipe. It does not protect what flows through it.

Consumer end-to-end encryption, the model used by Signal and WhatsApp, protects messages between sender and recipient. But healthcare requires multi-party access across physicians, specialists, billing teams, payers, and labs. Access requirements change over time and must be revocable. Consumer E2EE does not support revocation after delivery, centralized audit trails, or policy-based access controls for time, device, role, or geography.

Healthcare needs an encryption model that provides genuine end-to-end protection while supporting the complex, multi-party, policy-driven workflows the industry requires.

5. What Data-Layer Security Actually Means

> ***Traditional security asks: "Is this system secure?" Data-layer security asks: "Is this data secure, regardless of what system it is on?"***

Data-layer security is a fundamentally different architecture. Instead of building walls around data (perimeter security) or locking the rooms where data is stored (encryption at rest), data-layer security locks the data itself. The protection travels with the data. It does not matter if the system is compromised, the administrator is malicious, or the vendor is breached. Without correct cryptographic authorization, the data is unreadable.

Effective data-layer security for healthcare must encrypt data at the source before it touches any network or third-party system; maintain encryption across storage, transit, processing, and sharing; prevent intermediary access to plaintext without explicit cryptographic authorization; enforce access policies that travel with the data across organizations; support revocable, dynamic access control even after sharing; provide tamper-evident audit trails with cryptographic integrity; integrate into existing workflows without requiring operational changes; and scale across providers, vendors, payers, and analytics platforms.

6. How Seald Healthcare Works

Seald Healthcare provides an encrypted data layer purpose-built for healthcare. PHI is encrypted at the source and protection is maintained across every system, vendor, and workflow the data touches. Here is what that looks like in practice.

6.1 End-to-End Encryption for Healthcare

PHI is encrypted at the source and only decrypted by authorized recipients. No intermediary, including Seald Healthcare itself, can access plaintext data. This is not the transparent encryption of cloud storage or the channel encryption of TLS. This is persistent, data-layer encryption where the cryptographic keys are independent of the infrastructure.

Unlike consumer end-to-end encryption, Seald Healthcare's model was designed from the ground up for healthcare's multi-party access requirements. A single patient record can be accessible to the treating physician, consulting specialists, the billing team, and the insurance payer, each with different permission levels, all enforced cryptographically.

6.2 Persistent Access Policies

Access policies travel with the data itself. Healthcare organizations can define exactly who can access data, from which devices, during which time windows, under which conditions (geographic, network, or MFA requirements), and for how long.

The key difference from traditional access controls: these policies are cryptographically enforced at the point of decryption, not at the network perimeter. And they can be modified or revoked at any time, even after data has been shared. When a vendor's contract expires, access is revoked. When a staff member changes roles, permissions update automatically. When a security incident is detected, access can be suspended across the entire ecosystem in real time.

6.3 AI-Powered Policy Management

Seald Healthcare's AI Studio allows administrators to define access policies in plain English. Instead of configuring complex rule engines or writing security policies in technical syntax, an administrator can write:

> ***"Only allow our clinical staff to decrypt patient records during office hours from managed devices."***

The AI Studio translates natural language into enforceable cryptographic policies. This dramatically reduces the complexity of policy management while eliminating the misconfiguration risk that causes so many breaches in the first place.

6.4 Tamper-Evident Audit Trails

Every access event, whether it is a successful decryption, a denied access attempt, a policy change, a key rotation, or a permission modification, is logged with cryptographic integrity. These logs cannot be altered without detection. They record who accessed data, when, from where, and from which device. They provide evidence-grade records for compliance audits, breach investigations, regulatory inquiries, and legal proceedings. And they are maintained independently of the systems storing or processing PHI.

6.5 SDK-First Integration

Seald Healthcare integrates into existing healthcare workflows through an SDK-first approach. The Seald Healthcare SDK can be embedded into EHR systems, patient portals, telehealth platforms, secure messaging applications, file-sharing systems, and custom internal tools. Integration does not require changes to existing clinical or administrative workflows. Staff continue to use the same systems they use today. The encryption and policy enforcement

happen transparently at the data layer, complementing existing cloud environments including AWS, Google Cloud, and Azure.

6.6 Automatic Key Management

Managing encryption keys is one of the most complex challenges in applied cryptography. Seald Healthcare handles it automatically. Keys are issued, rotated, rewrapped, and revoked without manual intervention. Key management is separated from infrastructure access, meaning cloud administrators cannot access decryption keys. No cryptography expertise is required from the healthcare organization's IT team. The key lifecycle follows NIST best practices and is designed for quantum-safe cryptographic migration as post-quantum standards (FIPS 203/204/205) are adopted across the industry (NIST, 2024).

6.7 Group and Role-Based Access

Healthcare is organized around teams, departments, and roles, not individual users. Seald Healthcare supports this structure natively. Permissions can be assigned to care teams, departments, or roles rather than individuals. Access updates automatically as group membership changes. When a physician joins a department, they gain access to that department's encrypted data without manual provisioning. When a nurse transfers to another unit, permissions adjust accordingly. The system supports the complex access patterns healthcare demands: primary care teams, consulting specialists, and administrative staff can each hold different permission levels on the same data.

7. What This Looks Like in Practice

Abstract security concepts become concrete when you consider the scenarios healthcare organizations actually face.

7.1 Vendor Breach

Without Seald Healthcare: A revenue cycle management vendor is breached. The vendor has access to plaintext PHI for millions of patients across dozens of healthcare clients. All patient data is exposed. The healthcare organization learns of the breach weeks later and has no ability to limit the damage. This is exactly what happened with Change Healthcare.

With Seald Healthcare: The same vendor is breached, but all PHI passing through or stored by the vendor is encrypted with Seald Healthcare. The attacker obtains ciphertext, which is unreadable without cryptographic authorization they do not have. The healthcare organization revokes the vendor's decryption permissions in real time. The audit trail shows exactly what data the vendor accessed before the revocation. Patient data remains secure.

7.2 Insider Threat

Without Seald Healthcare: A database administrator with broad system access exfiltrates patient records. Traditional access controls cannot prevent someone with legitimate administrative credentials from querying the database. The organization discovers the theft months later through an unrelated investigation. In 2024, a former employee at Nuance Communications (a Geisinger contractor) accessed records of 1,276,026 patients two days after being terminated because credentials were not revoked (HIPAA Journal).

With Seald Healthcare: The administrator can access the database but cannot decrypt PHI because decryption keys are managed independently of infrastructure credentials. The data in the database is ciphertext. Access attempts are logged in the tamper-evident audit trail, triggering real-time alerts.

7.3 Ransomware Attack

Without Seald Healthcare: Attackers exfiltrate PHI before deploying ransomware. Even if the organization recovers from the ransomware, the exfiltrated data is permanently compromised. The organization faces regulatory penalties, class-action lawsuits, and reputational damage. UnitedHealth Group spent $3.1 billion responding to a single ransomware incident.

With Seald Healthcare: Attackers exfiltrate encrypted data. Without Seald Healthcare's decryption keys, the data is useless. The organization can demonstrate to regulators and patients that PHI was never exposed in plaintext. Under HIPAA's encryption safe harbor provision, the breach notification obligation may be eliminated entirely, because encrypted data that is breached is not considered "unsecured PHI" under the Breach Notification Rule.

7.4 Tracking Technology Exposure

Without Seald Healthcare: Website tracking pixels from Google, Meta, or other advertising platforms inadvertently capture and transmit patient data to third parties. Kaiser Foundation Health Plan exposed 13.4 million member records this way in 2024. The data was sent to advertising companies in plaintext (HIPAA Journal).

With Seald Healthcare: Even if tracking technologies capture data fields, the underlying PHI is encrypted. What gets transmitted is ciphertext. The advertising platform cannot read it. The exposure is neutralized.

8. Why This Cannot Wait

Several forces are converging that make data-layer security not just advisable but unavoidable for healthcare organizations. The urgency for healthcare organizations to adopt data-layer security is accelerating. It is no longer a matter of best practice, but an existential requirement driven by the convergence of several major, intensifying forces. These pressures (from rapidly escalating vendor-related compromises and a massive expansion of the attack surface due to AI adoption, to tightening regulatory enforcement and the hard demands of the cyber insurance market) are rendering traditional, perimeter-focused security models obsolete. Furthermore, the industry must now begin planning for a fundamental shift in cryptographic standards with the advent of post-quantum computing. For these reasons, data-layer security has become not just advisable, but an unavoidable imperative.

8.1 Third-Party Risk Is Accelerating

The Change Healthcare and MOVEit breaches demonstrated that vendor compromises cascade across entire industries. The average hospital works with more than 1,300 vendors (Ponemon Institute). In 2024, business associate breaches accounted for a disproportionate share of compromised records (HIPAA Journal). This trend will intensify as healthcare continues to outsource functions to specialized technology providers.

8.2 AI Adoption Is Expanding the Attack Surface

Clinical decision support, population health analytics, predictive modeling, and administrative automation all require access to patient data. Every AI model, every analytics pipeline, and every data-sharing arrangement expands the attack surface. Without data-layer encryption, AI adoption in healthcare means PHI exposure at scale.

8.3 Regulatory Enforcement Is Tightening

In December 2024, HHS published a proposed update to the HIPAA Security Rule that would, if enacted, require healthcare organizations to implement multifactor authentication, encryption for data at rest and in transit, network segmentation, cybersecurity testing, and other measures currently treated as optional (HIPAA Journal; HHS NPRM, 2024). OCR's new risk analysis enforcement initiative has already resulted in multiple penalties in 2025, with the year on track to set a record for HIPAA enforcement actions (HIPAA Journal). State attorneys general are also increasing enforcement.

8.4 Cyber Insurance Is Demanding More

Cyber insurers are shifting from compliance checklists to demonstrated technical controls as conditions of coverage. Organizations that cannot show data-layer protections will face higher premiums, narrower coverage, and exclusions that leave them exposed when breaches occur.

8.5 Post-Quantum Cryptography Is Coming

NIST has finalized its first post-quantum cryptographic standards (FIPS 203, 204, and 205). Organizations across industries are beginning migration planning. Healthcare organizations that have not modernized their cryptographic architecture will face expensive, disruptive upgrades. Seald Healthcare's architecture is designed for quantum-safe cryptographic migration, providing protection today and a clear path forward as standards evolve (NIST, 2024).

9. Getting Started

Adopting data-layer security does not require ripping out existing infrastructure. Seald Healthcare is designed to layer on top of current systems, complementing existing security investments while closing the gaps that perimeter-based approaches leave open.

There are three integration paths: SDK integration embeds the Seald Healthcare SDK directly into existing applications, handling encryption, decryption, key management, and policy enforcement transparently. Gateway deployment encrypts data as it enters or exits environments that cannot be modified at the application level. API-based integration enables custom workflows for specialized analytics pipelines, interoperability requirements, or novel use cases.

Seald Healthcare integrates in minutes, not months. Organizations can begin encrypting PHI in their highest-risk workflows immediately and expand coverage incrementally. There is no requirement to encrypt everything at once.

And data-layer security does not replace existing security infrastructure. Firewalls, identity providers, SIEM systems, and endpoint protection all remain in place. Seald Healthcare adds a layer of cryptographic protection that these systems cannot provide. Even if every perimeter control fails, data encrypted with Seald Healthcare remains unreadable without explicit cryptographic authorization.

10. Conclusion

Healthcare does not have a compliance problem. It has a data security problem.

The numbers are unambiguous. More than 846 million patient records compromised since 2009. Nearly 277 million in 2024 alone. A single breach affecting 192.7 million people. Average breach costs that have exceeded every other industry for 14 straight years. Record enforcement penalties. Mounting litigation. Accelerating third-party risk.

Compliance frameworks and cloud platforms remain necessary. They provide essential baseline protections, organizational discipline, and regulatory alignment. But they were never designed to protect PHI as it moves across the modern healthcare ecosystem, an ecosystem of hundreds of vendors, thousands of integration points, and millions of daily data transactions.

The gap is structural. Perimeter-based security protects systems. Data-layer security protects data. Healthcare needs both.

Seald Healthcare provides the encrypted data layer that compliance frameworks were never built to deliver. By encrypting PHI at the source, enforcing access policies cryptographically, maintaining tamper-evident audit trails, and integrating seamlessly into existing workflows, Seald Healthcare ensures that patient data remains secure and unreadable, even when systems are compromised, vendors are breached, and credentials are stolen.

Are you ready to be secure, not just compliant?

Learn more at www.sealdhealthcare.com or contact charlie@sealdhealthcare.com to see Seald Healthcare in action.

References

1. HIPAA Journal, "Healthcare Data Breach Statistics," updated February 4, 2026. Based on data from the HHS Office for Civil Rights breach portal through January 31, 2026. https://www.hipaajournal.com/healthcare-data-breach-statistics/

2. HIPAA Journal, "2024 Healthcare Data Breach Report," January 2025. https://www.hipaajournal.com/2024-healthcare-data-breach-report/

3. HIPAA Journal, "The Biggest Healthcare Data Breaches of 2024," March 2025. https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/

4. HIPAA Journal, "Largest Healthcare Data Breaches of 2025," December 2025. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2025/

5. HIPAA Journal, "December 2025 Healthcare Data Breach Report," February 2026. https://www.hipaajournal.com/december-2025-healthcare-data-breach-report/

6. HIPAA Journal, "Average Cost of a Healthcare Data Breach Falls to $7.42 Million," July 2025. https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-2025/

7. IBM Security / Ponemon Institute, "Cost of a Data Breach Report 2024." Healthcare industry average: $9.77 million. Global average: $4.88 million. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

8. IBM Security / Ponemon Institute, "Cost of a Data Breach Report 2025." Healthcare industry average: $7.42 million. U.S. average: $10.22 million. https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry

9. HHS Office for Civil Rights, "Change Healthcare Cybersecurity Incident FAQs," updated July 2025. Confirmed 192.7 million affected individuals. https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/

10. UnitedHealth Group, Change Healthcare consumer support page. Confirmed breach details, notification timeline, and affected data types. https://www.unitedhealthgroup.com/ns/health-data-breach.html

11. Cybersecurity Dive, "UnitedHealth hikes number of Change cyberattack breach victims to 190M," January 2025. Reported $3.1 billion in response costs. https://www.cybersecuritydive.com/news/change-healthcare-attack-affects-190-million/738369/

12. U.S. Department of Health and Human Services, HIPAA Security Rule, 45 CFR Part 164.

13. HHS Office for Civil Rights, HIPAA Security Rule Notice of Proposed Rulemaking (NPRM), December 2024.

14. Amazon Web Services, "Shared Responsibility Model." https://aws.amazon.com/compliance/shared-responsibility-model/

15. Microsoft Azure, "Shared Responsibility in the Cloud." https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

16. Verizon, "Data Breach Investigations Report (Healthcare Sector)," 2024.

17. Ponemon Institute, "Third-Party Risk in Healthcare," 2024.

18. National Institute of Standards and Technology, Post-Quantum Cryptography Standardization Program, FIPS 203/204/205, 2024. https://csrc.nist.gov/projects/post-quantum-cryptography