SEALD HEALTHCARE

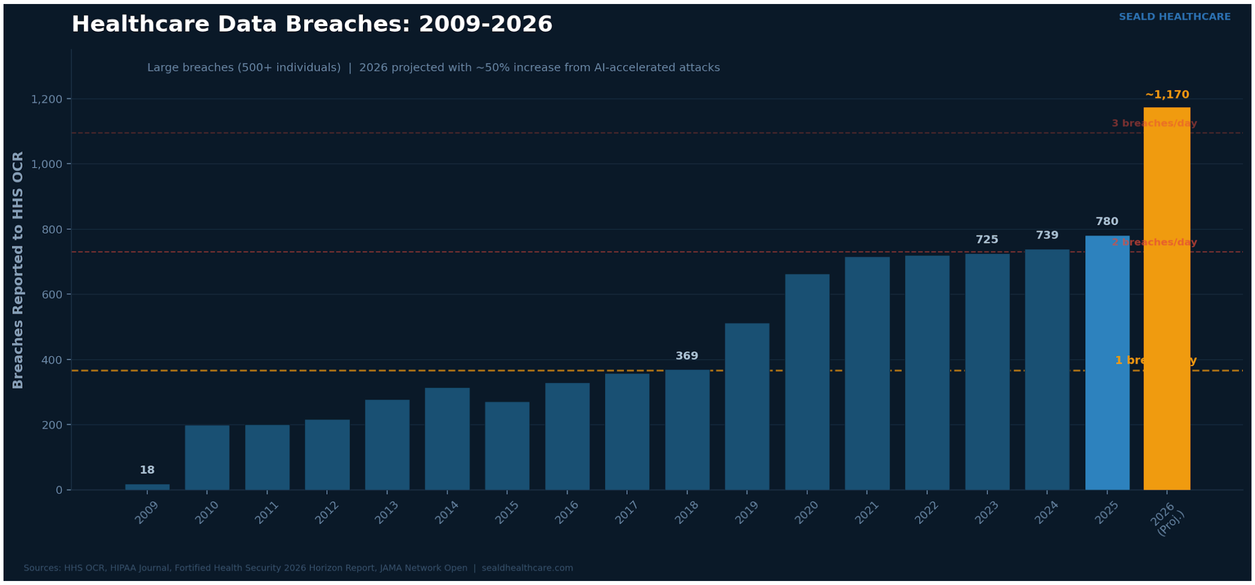
42 Breaches in 45 Days. AI Is Accelerating Healthcare Cyberattacks. Here’s What Has to Change.

February 2026

We are seven weeks into 2026 and the U.S. Department of Health and Human Services has already logged 42 healthcare data breaches classified as affecting 500 or more individuals in each breach, with some breaches exceeding 700,000. Forty-two organizations. Millions of patients. Forty-five days.

That number should alarm you, but it should not surprise you. This is the continuation of a trajectory that has been building for years. In 2025, healthcare breach frequency more than doubled compared to the prior year according to Fortified Health Security's 2026 Horizon Report. Cyberattacks on healthcare are not slowing down, they are accelerating, and the single biggest reason is artificial intelligence.

The Numbers



Sources: HHS OCR, HIPAA Journal, Fortified Health Security 2026 Horizon Report, JAMA Network Open | sealdhealthcare.com

Figure 1: Healthcare data breaches reported to HHS OCR, 2009–2026 (projected)

The HHS Office for Civil Rights Breach Portal, often called the "Wall of Shame," tells a clear story. Between 2009 and 2024, over 6,700 large healthcare breaches were reported. Those breaches exposed the protected health information of more than 846 million individuals. In 2024 alone, roughly 275 million records were compromised. The Change Healthcare ransomware attack accounted for an estimated 190 million of those.

Then 2025 happened. Total reported breaches surged by more than 112 percent year over year. Email-based breaches more than doubled. Hacking and IT incidents dominated the breach reports. The average size of individual breaches trended smaller, which signals that some containment measures are working. But the volume of attacks created what Fortified Health Security's CEO Dan Dodson called "relentless pressure."

Now look at the first weeks of 2026. Forty-two breaches already reported. The OCR portal shows the same patterns repeating. Network server compromises. Email intrusions. Unauthorized access to electronic medical records. And a growing number of incidents involving business associates, the third-party vendors that healthcare organizations depend on every day.

AI Changed the Game for Attackers

What makes this moment different is not just the volume of attacks. It is the sophistication, speed, and scalability behind them, and AI is the reason.

Health-ISAC's 2026 Global Health Sector Threat Landscape report identifies AI-enabled attacks as a top concern for the year ahead. Industry telemetry shows AI-generated phishing emails have surged by more than 1,000 percent year over year since large language models became widely available. Attackers are using AI to craft phishing emails nearly indistinguishable from legitimate hospital communications. They are generating voice deepfakes that mimic executives. They are discovering network misconfigurations at machine speed and producing malware variants faster than signature-based defenses can catalog them.

This is not theoretical. It is happening now.

Healthcare IT Today reported that by 2026, the speed of AI-enhanced cyberattacks is expected to outpace traditional cybersecurity defenses and human-led detection. Manual security processes and legacy detection tools are not keeping up. AI has also lowered the barrier to entry for cybercrime across the board. Inexperienced attackers can now use AI-powered toolkits to identify vulnerable organizations, automate phishing campaigns, and deploy ransomware with minimal technical expertise.

Healthcare is especially attractive because of its high-value data, legacy systems, 24/7 operational requirements, and heavy vendor dependencies. Threat actors know this and that’s why they are hyper-focused on this vertical.

Perimeter Security Is Not Enough

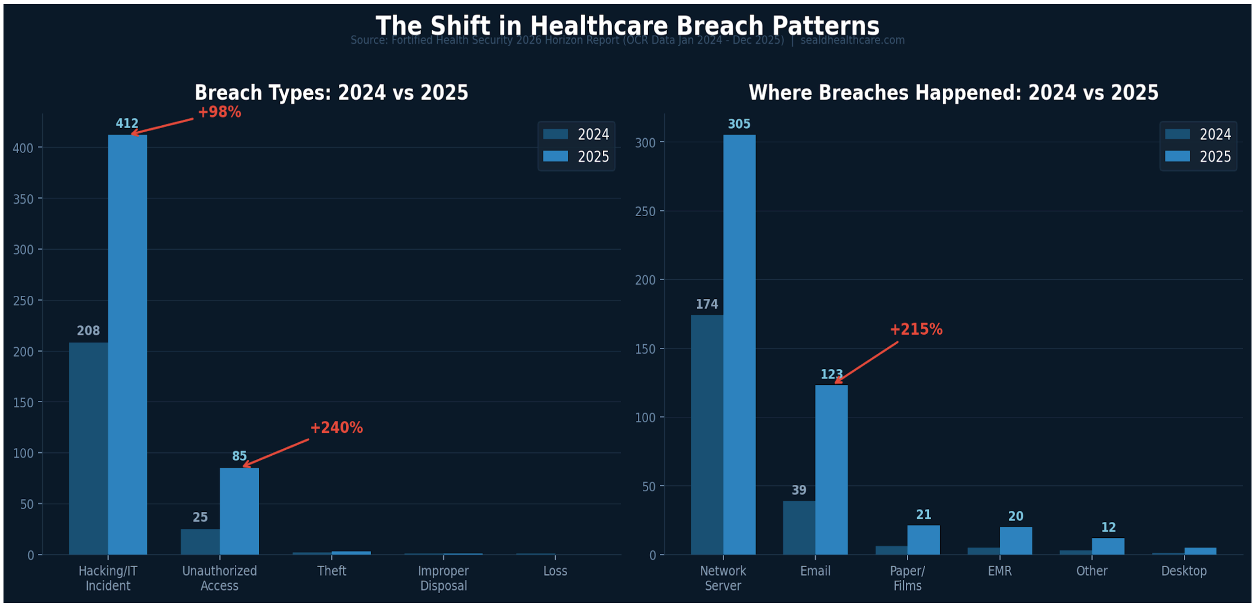


Figure 3: Shift in healthcare breach types and locations, 2024 vs 2025 (Fortified/OCR data)

For decades, the healthcare cybersecurity strategy has been built around the perimeter. Firewalls. Intrusion detection. Endpoint protection. Access controls. These tools still matter. But the 2025 and 2026 breach data tells us something every healthcare leader needs to internalize.

The perimeter will be breached. It is not a matter of if. It is when.

Look at the recent OCR breach reports. VITAS Hospice Services reported a hacking incident affecting over 319,000 individuals. Fieldtex Products, a business associate, reported multiple breaches across several covered entities totaling hundreds of thousands of affected records. Richmond Behavioral Health Authority saw over 113,000 records compromised. Delta Dental of Virginia reported nearly 127,000 individuals affected through email. Tri Century Eye Care reported 200,000 individuals impacted.

In every one of those cases, the attackers got in. Firewalls did not stop them. Endpoint protection did not stop them.

The question that matters now is different. Once attackers are inside, what protects the data itself?

That is the paradigm shift. Cybersecurity can no longer be just about keeping attackers out. It has to be about making sure that when they get in, the data they find is useless.

Protect the Data, Not Just the Perimeter

This is where the conversation needs to shift from perimeter defense to data-layer security. Not encryption as a checkbox. Encryption at the record level, with governance that follows the data wherever it goes.

HIPAA's Security Rule requires covered entities and business associates to implement technical security measures that guard against unauthorized access to electronic protected health information. Encryption is classified as an "addressable" specification. But the regulatory reality is clear. In today's threat environment, leaving ePHI in plaintext is an indefensible position.

Here is the part that matters most. Under the HIPAA Breach Notification Rule, if encrypted data is compromised but rendered unreadable through encryption that meets NIST standards, the incident is not considered a reportable breach.

Properly encrypted data, even when stolen, does not trigger breach notification obligations.

That is not a loophole. It is recognition that encryption fundamentally changes the risk equation, but here is what most people miss. Traditional encryption approaches, like TLS in transit or full disk encryption at rest, still leave plaintext PHI sitting exposed inside your applications, databases, and vendor systems. If someone breaches a server and that data is in plaintext, it is visible and stolen.

The only secure approach is encrypting data at the record level, at the source, before it ever leaves the device or application. That means the data itself is protected.

At Seald Healthcare, we encrypt PHI at the record level via SDKs and APIs. The encryption happens at the source, on the user's device, before it enters your system. Access policies travel with the data, not with the network. That means you can control who accesses it, from what device, during what time window, and revoke that access at any time, even after the data has been shared.

We also built an AI policy engine that lets teams write access policies in plain English and enforce them automatically at the point of decryption. Every access event, every denial, every policy change is logged in tamper-evident audit trails. You get a full chain of custody over every piece of PHI, across every recipient and every workflow.

No intermediary can access the plaintext data. Not your cloud provider. Not your vendor. Not even us.

The Third-Party Problem

One of the most striking trends in recent breach data is the role of business associates. Security experts describe a shift from opportunistic attacks to coordinated operations that treat healthcare like a high-value supply chain. Attackers know that breaching one widely deployed vendor platform can open the door to dozens or hundreds of healthcare organizations at once.

The OCR portal confirms this. Fieldtex Products alone appears in multiple breach entries affecting different covered entities. Business associates like Persante Health Care, Davies McFarland & Carroll, and Personic Management Company all reported significant hacking incidents in late 2025. The Fortified Health Security report found that third-party weakness was a primary driver of the breach surge.

Record-level encryption with persistent access policies directly addresses this vulnerability. When data is encrypted before it reaches a third-party system, the compromise of that system does not compromise the data. The business associate cannot decrypt what they were never authorized to read. And if a relationship ends or access needs to change, you revoke it, in real time.

This is not about trusting your vendors less. It is about making sure that trust is not the only security control you have.

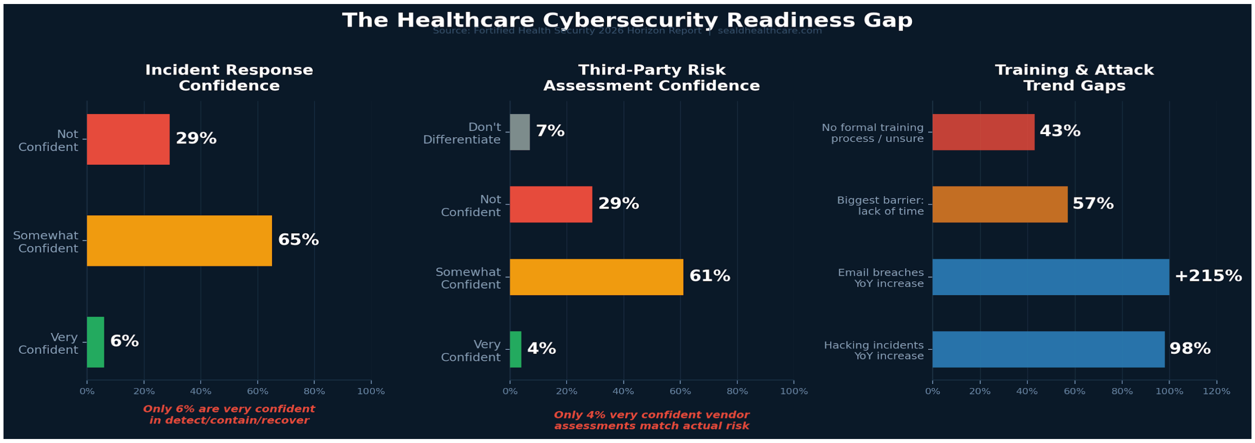
From Compliance to Resilience

The defining challenge in healthcare cybersecurity is no longer just prevention. It is resilience. The ability to keep operating, protect patient care, and limit damage even when a breach occurs.

ECRI's Top 10 Health Technology Hazards for 2026 placed risks from AI in healthcare at the top of the list. The Health Sector Coordinating Council is rolling out new 2026 guidance on managing AI cybersecurity risks. Proposed updates to the HIPAA Security Rule are expected to tighten requirements around encryption, incident response, and vendor oversight.

The regulatory environment is heading toward a future where encryption is not optional. Organizations that move now to encrypt PHI at the data layer are not just ahead of the compliance curve,they are building real resilience into how they operate. They are ensuring that when an attacker gets through the perimeter, the most sensitive data patients entrust to them stays protected. Not because of where it is stored, but because of how it is secured.

The Readiness Gap Is Alarming


The Healthcare Cybersecurity Readiness Gap

Source: Fortified Health Security 2026 Horizon Report | sealdhealthcare.com

Incident Response Confidence

Third-Party Risk Assessment Confidence

Training & Attack Trend Gaps

Only 6% are very confident in detect/contain/recover

Only 4% very confident vendor assessments match actual risk

Figure 2: Healthcare cybersecurity readiness gaps (Fortified Health Security 2026 survey)

The Fortified Health Security 2026 Horizon Report includes survey data from healthcare leaders across the country. The findings should concern everyone in the industry.

Only 6 percent of healthcare organizations report being very confident in their ability to detect, contain, and recover from a cyber incident. Six percent. That means 94 percent of healthcare organizations are not fully confident they can handle what is already happening at a rate of nearly one breach per day.

Third-party risk management is arguably worse. Just 4 percent of surveyed leaders expressed strong confidence that their vendor risk assessments align with actual risk. Twenty-nine percent said they are not confident at all. Another 7 percent admitted they do not currently differentiate risk levels among vendors. This is happening while business associate breaches are driving a significant share of the breach surge.

Then there is Shadow AI. Fortified's report identifies the unsanctioned use of AI tools by clinicians and staff as one of the most immediate and underestimated threats facing healthcare today. Clinicians are using consumer-grade tools like ChatGPT and transcription apps to work more efficiently. That is understandable, but when those tools are used without organizational vetting or HIPAA compliance, every upload and every query may be sending sensitive data into external environments that cannot be monitored or controlled. As Fortified's VP of Threat Services put it, Shadow AI does not look like an attack. It looks like productivity, that is what makes it so dangerous.

Forty-three percent of healthcare organizations either have no formal cybersecurity training process or are not sure if one exists. Fifty-seven percent of leaders cite lack of time as the biggest barrier to effective training. Meanwhile, email-based breaches jumped 215 percent year over year and hacking incidents nearly doubled.

These gaps are not theoretical. They are the reason breaches keep happening. And they point to a fundamental problem. Most healthcare organizations are still trying to defend data they cannot actually control once it leaves their systems.

Record-level encryption with persistent access policies closes that gap. When data is encrypted at the source, with policies that travel with it and audit trails that log every access event, Shadow AI tools cannot expose plaintext PHI. Compromised vendors cannot read what they were never authorized to decrypt. And the 94 percent of organizations that are not fully confident in their detection and response capabilities gain a layer of protection that works even when everything else fails.

What Healthcare Leaders Should Do Now

Forty-two breaches in forty-five days is not a statistic to file away. It is a signal to act. Here is what healthcare executives, CISOs, and technology leaders should be prioritizing based on the current threat landscape.

Accept the breach assumption. Stop building your security strategy around the hope that your perimeter will hold. It will not hold against AI-powered attacks operating at machine speed. Ask this question. When our perimeter fails, what protects the data? If the answer is nothing, you have work to do.

Encrypt at the data layer. TLS protects data in transit but does nothing once it reaches a server. Full disk encryption protects against physical theft but not a network compromise. Record-level encryption applied at the source, where access policies travel with the data and are enforced at decryption, is what actually changes the outcome.

Audit your third-party exposure. The supply chain attack vector is expanding fast. Evaluate every business associate that touches ePHI. Ask not just whether they are HIPAA-compliant, but whether the data they handle is encrypted in a way that limits your exposure if their systems are compromised.

Prepare for AI-driven threats. Invest in AI-augmented defense, but do not rely on detection alone. AI-generated phishing, deepfake social engineering, and automated vulnerability exploitation are going to intensify. Security awareness training has to evolve and so do your defenses.

Use encryption as your breach notification safe harbor. Under HIPAA, encrypted data that is breached does not require notification if the encryption meets NIST standards. That is not a technicality. It is a strategic advantage that protects your organization, your patients, and your reputation.

Final Word

Healthcare in 2026 is at a defining moment. AI is the most promising tool for improving patient care and the most dangerous weapon being aimed at the industry's defenses at the same time. The organizations that will come through this are the ones that recognize something fundamental. You cannot firewall your way out of an AI-powered threat landscape, but you can protect the data itself. When PHI is encrypted at the record level, when access policies travel with it, when every access event is logged and auditable, when you can revoke access even after sharing, the breach that was inevitable becomes the breach that does not matter. The attacker gets in and finds nothing but ciphertext. No patient names. No Social Security numbers. No medical records. Nothing.

Organizations should build their cybersecurity programs around their adversaries, not assumptions. Threat actors are hyper-focused on healthcare. Your defenses should be built with that same focus. The conversation has to move beyond perimeter security and into data-layer protection. That is where healthcare is headed.

Forty-two breaches in forty-five days. The question is not whether this pace will continue. The question is what you are going to do about it.

About Seald Healthcare — Seald Healthcare secures PHI at the data layer. Our SDKs and APIs encrypt data at the record level with persistent access policies and an AI policy engine that lets teams write governance rules in plain English. Every access event is logged in tamper-evident audit trails. No intermediary, including Seald Healthcare, can access the plaintext data. Works with EHRs, patient portals, telehealth, messaging, file sharing, and custom applications. Complements AWS, Google Cloud, and Azure environments. Learn more at sealdhealthcare.com.

Sources

U.S. Department of Health and Human Services, Office for Civil Rights Breach Portal (ocrportal.hhs.gov)

Fortified Health Security, 2026 Horizon Report (January 2026)

Health-ISAC, 2026 Global Health Sector Threat Landscape Report (January 2026)

HIPAA Journal, Healthcare Data Breach Statistics (hipaajournal.com)

Healthcare IT Today, Healthcare Cybersecurity – 2026 Health IT Predictions (December 2025)

ECRI, Top 10 Health Technology Hazards for 2026

Forbes, 10 Cybersecurity Predictions That Will Define 2026 (December 2025)

Healthcare Dive, How the Generative AI Boom Changes Healthcare Cybersecurity (February 2026)

HIPAA Vault, AI in Healthcare: Good AI vs Bad AI in the New Cybersecurity War (February 2026)