Healthcare Cybersecurity Trends 2026: Fewer Incidents, Greater Damage

2026 At A Glance: Key Signals from Q1

Data from the U.S. Department of Health and Human Services Office for Civil Rights (OCR) shows reported healthcare breaches in Q1 2026 are down 25% from last year. Simultaneously, the extent of this year's breaches has nearly tripled.

Two incidents alone accounted for more than 6.5 million of those records, and both traced directly to network servers compromised through hacking. Neither instance was, in retrospect, a surprise to anyone paying attention to where breach data has been pointing for the past decade.

When breach counts fall, organizations tend to exhale. Fewer reported incidents can feel like evidence that investments are finally working, that posture is improving, or that pressure might be lifting.

The question healthcare leaders must ask now is not "are breaches declining?"

The questions are "why is each breach reaching further?" and "is my organization built to limit that reach?"

86

BREACHES REPORTED

Down 24.6% vs Q1 2025

8.66M

INDIVIDUALS AFFECTED

Up 180.7% vs Q1 2025

91.9%

BREACHES FROM HACKING

Highest Q1 rate on record

What Actually Happened: The Incidents Behind the Numbers

To understand what the data from Q1 2026 suggests about emerging trends in IT, it helps to look closely at the two pivotal incidents. Together, the breaches that impacted TriZetto Provider Solutions and QualDerm Partners account for the overwhelming majority of individuals affected this quarter, and both illustrate patterns that have been emerging for years.

TriZetto Provider Solutions | 3.43M Individuals Impacted

February 2026 Network Server Breach

TriZetto, a Cognizant-owned healthcare revenue management and claims clearinghouse, processed more than four billion payment and eligibility transactions annually on behalf of hospitals, health systems, and physician practices. An unauthorized actor gained access to a web portal used by healthcare providers to access TriZetto systems as early as November 2024, and that access went undetected for nearly eleven months. By the time suspicious activity was identified in October 2025, the threat actor had been quietly accessing eligibility transaction reports containing names, Social Security numbers, insurance member numbers, and Medicare beneficiary identifiers for millions of patients. The covered entities affected had no direct contract with TriZetto. Their data only reached TriZetto through a chain of subcontractor relationships unknown to most patients. Patients who received breach notifications were confused about the source, with some questioning the legitimacy of the notification letters. This outcome reveals the startling distance between patients and the systems that guard their most sensitive data.

Sources: HIPAA Journal [3] | | Censinet [4] | Security Affairs [5]

QualDerm Partners | 3.12M Individuals Impacted

February 2026 Network Server Breach

QualDerm provides management services to 158 dermatology and skin care practices across 17 states, serving well over a million patients annually. Between December 23rd and 24th, 2025, an unauthorized actor gained access to systems within QualDerm's network and exfiltrated data. The actor removed treatment information, diagnosis records, insurance details, and in some cases, government-issued identification. The intrusion window was brief, suggesting a targeted operation with prior reconnaissance rather than opportunistic access. QualDerm began notifying affected individuals in late February 2026, roughly two months after the discovery. The company has confirmed that it is reviewing its security policies and procedures and has not yet publicly disclosed how initial access was achieved.

Sources: HIPAA Journal [6] | Cybernews [7] | HIPAA Guide [8] | Cory Watson Attorneys [9]

These two incidents are not outliers. They represent a concentrated version of a pattern the OCR archive has been documenting for years: centralized data stores, extended dwell times, third-party access chains with uneven visibility, and a widening gap between when access is gained and when it is finally detected. What IT leaders must take note of *now* is the rapid scale at which these patterns converged in a single quarter.

A Decade of Signals: Finally in Focus

Mapping the full OCR trajectory back to 2015 reveals that the threat is not simply growing louder; it is becoming more precise.

In 2015, hacking accounted for roughly 28% of all Q1 breaches. By 2022, that figure had crossed 85%, and in Q1 2026 it stands at 91.9%, the highest first-quarter hacking concentration in the dataset's history. Network server exposure follows the same arc, moving from 25% of breach locations in 2015 to 66.3% in Q1 2026.

Q1 Year	Breach Count	Individuals Affected	Hacking %	Network Server %
2015	67	92,143,061	28.4%	25.4%
2018	79	1,176,789	32.9%	19.0%
2021	158	12,372,113	69.0%	48.7%
2023	157	18,114,428	71.3%	62.4%
2024	230	21,165,904	80.9%	72.6%
2025	114	3,086,485	74.6%	55.3%
2026 (Q1, as of 4/16/2026)	**86**	**8,662,255**	**91.9%**	**66.3%**

These are not separate trends, but the same story told from two different angles. As healthcare centralized its data to gain operational efficiency, it also centralized its risk. Now that a single server-based incident can expose millions of records, the conversation about blast radius stops being a theoretical exercise and starts to become a leadership accountability question.

The business associate picture compounds this further. In Q1 2015, only two BA incidents appeared in the OCR data. By Q1 2023, that number had grown to 38. The TriZetto breach illustrates why this matters so clearly: the affected organization processed data at a scale that touched providers, subcontractors, and patients who, in many cases, were not aware that their information had passed through TriZetto's system.

When the chain of custody for PHI extends this far, the traditional perimeter model of healthcare security becomes conceptually irrelevant.

This is Not Just a Clearinghouse Problem

A common response to incidents like TriZetto's data breach is to draw a comparison perimeter around the conversation.

> *"The reasoning often goes, "we are not a clearinghouse, and we do not process four billion transactions, therefore this does not reflect our risk profile." It is a response I have heard in boardrooms, and I understand the instinct behind it, but the logic does not hold once you examine what the risk is actually measured against."*
>
> ***Jericho Simmons***
> *Chief Information Security Officer, Kalosys*

The relevant question is not whether your organization resembles TriZetto in scale or structure. Instead, the questions are "what is your organization's data worth?" and "what would a breach of that data actually cost?"

Most healthcare organizations today consolidate patient information into centralized data environments including data lakes, warehouses, or shared platforms, because these are where modern clinical and operational workflows live. The asset class is the same regardless of transaction volume.

If your organization serves 200,000 individuals in a month, IBM's Cost of a Data Breach report puts the base financial exposure at roughly $185 per unique record. This means a data breach would expose approximately $37 million *before* factoring in regulatory penalties, litigation, operational disruption, and reputational damage. It is not a worthwhile exercise to compare your organization's architecture to a clearinghouse's.

Instead, it is important to apply a realistic probability to your organization's exposure, determine what a 30% likelihood of a breach costs compared to a 20% likelihood, then decide whether this difference justifies the investment required to close it. This conversation is one most executives have not yet had, and the OCR data suggests the gap between having it and not having it is widening every year.

200,000 individuals (monthly) x $185 per record = $37M *base cost of a breach*

At 30% breach likelihood, that is $11.1M in expected loss.
At 20% breach likelihood, that is $7.4M in expected loss.

The decision for healthcare leaders is whether the cost of closing that gap is less than $3.7M. In most organizations, it is.

Compliance Investments Are Not Keeping Pace

One of the more concerning trends this data highlights is the positive correlation between compliance investment and breach severity over the last decade. HIPAA has been federal law since 1996, the HITECH Act added teeth in 2009, and HITRUST, SOC 2, and a growing library of frameworks have given organizations increasingly detailed roadmaps for what adequate security should look like. However, the data reveals that the scale of healthcare breaches increased rather than decreased as these frameworks matured and their adoption grew.

In short, increased investments into compliance have not produced fewer data breaches.

This trend does not suggest that these frameworks are without value. Rather, it suggests that these frameworks answer a backward-looking question about whether the required controls were in place at the time of the assessment. Meanwhile, the current threat landscape demands answers to forward-looking questions about what a motivated, well-resourced adversary will attempt next, and whether the detection and response capabilities of an organization are ready to meet that moment.

These are fundamentally different questions, and most compliance programs are designed only to answer the first one. The TriZetto intrusion sat undetected for nearly eleven months inside a system which presumably passed its most recent security review, but passing assessment did not translate into timely breach detection.

There is a related tension worth naming directly. Security leaders in many organizations understand this gap clearly and have documented it, escalated it, and in some cases presented the financial model above to the very executives who hold budget authority. When investment does not follow, it is not always because leadership does not understand the risk.

Sometimes, the risk has been formally acknowledged, accepted, and documented as a deliberate business decision. That is a legitimate governance outcome, and a security leader who has properly escalated, documented, and continued monitoring the accepted risk against other priorities has fulfilled their obligation. What is not legitimate, however, is informally accepting risk without documentation, then treating a breach as something that happened to the organization, rather than something the organization chose to absorb.

The difference between these two positions matters enormously when regulators, auditors, and legal counsel arrive.

AI Is Changing the Equation in Both Directions

Practitioners who work close to the technical reality will rightly point out that incidents like TriZetto do not require sophisticated AI-enabled attacks to explain. Eleven months of undetected access on a web portal points to foundational gaps in logging, behavioral monitoring, and access governance that have existed in healthcare environments for years. Framing this as an AI-problem risks misdirecting investment away from the basic visibility controls that would have caught it.

This critique is fair and worth taking seriously, because the foundational work still comes first. However, this does not address what is already happening at the edges of the threat landscape, or the direction that the landscape is moving. AI-powered threats are not an emerging future problem for healthcare security; they are already a reality.

Most organizations are not yet feeling their impacts because the adversaries deploying them are still targeting environments with the weakest foundations. These environments are absorbing the damage before more mature environments come into focus. Healthcare data has long attracted well-resourced threat actors because the return is high, and the cost of entry is low.

AI compresses both variables further by enabling faster reconnaissance, more adaptive persistence, and lateral movement that does not generate the behavioral signals that traditional detection was designed to catch. Organizations that have not yet resolved their foundational visibility gaps are not insulated from this dynamic; they are positioned at the front of it.

The more important point is that the same AI capabilities available to adversaries are equally available to defenders.

Continuous monitoring at scale, behavioral baselining across complex environments, and real-time signal correlation that would take human analysts days to complete are operational realities for organizations that have built the foundation to support them. The work of building that foundation is not glamorous and rarely generates the attention that a major incident does, but it is what separates organizations that detect anomalous access in days from ones that discover it after eleven months of uninterrupted dwell time.

AI does not change who wins the breach. It changes how fast the outcome is decided and how much damage accumulates before leadership has enough information to act.

Three Things Every Leader Should Take Away from This Data

A decade of OCR breach data points to a consistent pattern. Understanding it clearly is the first obligation for any leader responsible for an organization that holds patient data. The threat environment has shifted from opportunistic, low-scale incidents to targeted operations that exploit centralized infrastructure, third-party access chains, and the gap between what organizations believe they can see and what is happening inside their environments. This gap is not a technology problem alone; it is a visibility and governance problem. This gap only grows wider when leadership assumes that security functions have it covered without stress-testing that assumption against real incident scenarios.

Understanding the pattern is only meaningful if it connects to a clear sense of what is at stake for the organization. The TriZetto and QualDerm breaches did not affect IT systems in the abstract. They affected real patients; many of whom received confusing notifications about data they did not know had traveled through a particular vendor's infrastructure. Treatment histories, insurance details, Social Security numbers, and Medicare identifiers are the kind of information that, once exposed, create consequences for real people that credit monitoring services cannot fully undo. When leaders frame their security posture around regulatory exposure or insurance coverage alone, they are addressing the wrong stakes.

When risks are understood at this level, the path forward stops being about reacting to the last breach and starts being about deliberate preparation before the next one arrives.

Our work at Kalosys consistently surfaces the same finding: organizations that know where their risk lives, have leadership aligned around who owns it, and have tested their assumptions before pressure arrives, are the organizations that respond with clarity rather than confusion when an incident occurs. That preparation does not require waiting for a framework update or a regulatory mandate. It requires deciding, before an incident forces the question, whether the organization is built to face what the data has already told us is coming.

The Q1 2026 numbers are an early look at this year's story for healthcare organizations. As the OCR portal continues to be updated, the picture will sharpen further. However, the direction is already visible and consistent with everything that the last decade has signaled. The organizations that act on that signal now, during a period of relative calm, are the ones that will be positioned to protect the patients who are counting on them when the next wave arrives.

About the Author

Jericho Simmons

Chief Information Security Officer, Kalosys

Recognized as a Top 100 Global CISO, Jericho helps organizations translate cybersecurity into board-level strategy and decision-making, moving beyond compliance into true security maturity.

jericho.simmons@kalosys.net

Contributors

Steve Kay

Chief Resiliency Officer, Kalosys

Head of Security and Resilience solutions at Kalosys, Steve masterfully realizes the value of the Kalosys 3D Methodology for leaders across industries.

steve.kay@kalosys.net

Carlos Salazar, DBA

Chief AI Officer, Kalosys

Author of the Kalosys Co-Intelligence Advantage Framework and AIKA Methodology, Carlos leads all AI Strategy, Solutions, and Transformations at Kalosys.

carlos.salazar@kalosys.net

Sources

[1] HHS Office for Civil Rights Breach Portal. Data as of April 16, 2026.* https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf. **The OCR portal is a living database and figures are subject to revision as additional submissions are received.*

[2] IBM *Cost of a Data Breach Report*. 2024. https://www.ibm.com/reports/data-breach.

[3] The HIPAA Journal. *Trizetto Data Breach.* 2026. https://www.hipaajournal.com/trizetto-provider-solutions-data-breach/.

[4] Censinet. *TriZetto Provider Solutions Reports Data Breach Impacting Healthcare Clients.* 2026. https://censinet.com/perspectives/trizetto-provider-solutions-data-breach-healthcare-clients.

[5] Security Affairs. 2026. *Cognizant's TriZetto Provider Solutions data breach impacted over 3.4 million patients.* https://securityaffairs.com/189149/data-breach/cognizants-trizetto-provider-solutions-data-breach-impacted-over-3-4-million-patients.html.

[6] The HIPAA Journal. 2026. *QualDerm Partners Data Breach Affects More Than 3 Million Individuals.* https://www.hipaajournal.com/qualderm-partners-data-breach/.

[7] Cybernews. 2026. Dermatology services giant operating in 17 states exposes data of 3.1 million. https://cybernews.com/security/qualderm-data-breach-3-1-million-17-states/.

[8] The HIPAA Guide. 2026. *QualDerm Partners Data Breach Affects 3.1 Million Patients.* https://www.hipaaguide.net/qualderm-partners-data-breach.

[9] Cory Watson Attorneys. 2026. *QualDerm Partners Data Breach: What Patients Need to Know.* https://www.corywatson.com/blog/qualderm-partners-data-breach-what-patients-need-to-know/.