vorlon

WHITE PAPER

Why Third-Party API Risks are the #1 Healthcare Security Concern for 2025

Lessons Learned From the 2024 Breaches Impacting Healthcare Organizations

The state of healthcare cybersecurity

The healthcare industry is facing an unprecedented cybersecurity crisis. As hospitals, insurers, and medical technology companies increasingly adopt third-party applications and cloud-based services, the attack surface for cybercriminals has expanded dramatically. While innovations in electronic health records (EHRs), telehealth, and patient engagement platforms have improved operational efficiency, they have also introduced new risks—particularly through third-party API integrations.

The surge in healthcare data breaches

In 2024 healthcare faced over 1,220 data breaches, according to the latest Verizon Data Breach Investigations Report (DBIR), making it one of the most targeted industries. A significant portion of these incidents stemmed from third-party service providers and SaaS-based applications, where weak API security, excessive permissions, and poor credential hygiene allowed attackers to infiltrate sensitive systems.

Healthcare accounted for over 1,220 confirmed data breaches in 2024

1,220

Healthcare organizations have become a prime target for cybercriminals due to the high value of protected health information (PHI). Unlike financial data, which has a short lifespan for fraud, PHI contains persistent identifiers such as medical history, Social Security numbers, and insurance details—making it highly attractive for identity theft and black-market sales. The financial impact of a healthcare breach is also staggering, with the average cost of a breach reaching $10.93 million per incident in 2024, according to IBM's Cost of a Data Breach Report.

Third-party risk is now a top threat

One of the most alarming trends in healthcare security is the growing reliance on third-party vendors and cloud-based SaaS solutions, which often operate outside the direct control of security teams. Healthcare providers are increasingly dependent on external applications that interact with PHI.

Many healthcare providers have limited visibility into how data flows between applications, and security teams often lack the tools needed to monitor API access, misconfigurations, or unusual data-sharing behaviors. Attackers have recognized this weakness, leading to a sharp rise in API-based attacks, credential theft, and supply chain compromises. Reports show that 41.2% of all third-party breaches in 2024 impacted healthcare organizations, according to HIPAA Journal.

Why this matters for 2025

As the industry moves into 2025, third-party API security is a business-critical priority. With rising breach costs, increasing regulatory scrutiny, and sophisticated attack tactics, healthcare IT leaders must rethink how they detect, monitor, and respond to third-party risks in real time.

Why third-party APIs are healthcare's weakest security link

While APIs are critical to modern healthcare operations, they have also become a prime attack vector for cybercriminals. Poorly secured APIs, misconfigured third-party applications, and excessive data-sharing permissions create a hidden risk surface that many security teams struggle to monitor. According to a HIPAA Journal study, **79% of healthcare organizations experienced an API-related security incident in the past 12 months**, highlighting the growing urgency to secure API connections.

A separate report by Healthcare IT News found that **the healthcare industry led all sectors in third-party data breaches in 2024**, further reinforcing the critical need for improved third-party security strategies.

The growing attack surface in healthcare APIs

The healthcare sector is experiencing an explosion in API usage. Many organizations now operate hundreds or even thousands of APIs, each connecting different applications, vendors, and data sources. However, most security programs were built to protect traditional endpoints, networks, and user accounts, not third-party SaaS applications and APIs. This gap leaves organizations vulnerable to:

- **Excessive API permissions** – Many API connections have more access than they actually need, allowing third-party apps to read or modify sensitive PHI.
- **Hardcoded or exposed API keys** – If an API key or OAuth token is leaked, attackers can use it to extract data without triggering security alerts.
- **Lack of visibility into API data flows** – Security teams often cannot see which third-party vendors are accessing what data in real time.
- **SaaS misconfigurations** – Many APIs inherit overly permissive settings from SaaS applications, exposing PHI or other sensitive data.

As third-party integrations continue to grow, so do API-based security threats. A single over-permissive API token or unsecured vendor connection can lead to a massive breach before traditional security tools even detect the issue.

How attackers are exploiting third-party API weaknesses

Attackers have adapted their techniques to target third-party APIs and SaaS integrations, knowing that these connections often lack the same level of monitoring as traditional IT assets. The most common attack vectors include:

- **Credential theft and token hijacking** – Attackers steal OAuth tokens or API keys through phishing, malware, or exposed credentials on code repositories. These tokens allow them to bypass authentication and extract data directly from APIs.
- **Exploiting API misconfigurations** – APIs with weak authentication, excessive permissions, or open endpoints are vulnerable to unauthorized data access.
- **Session hijacking and token reuse** – Many healthcare APIs use long-lived tokens that are not properly rotated, allowing attackers to reuse stolen session data indefinitely.
- **Third-Party SaaS compromises** – If an EHR vendor, billing provider, or patient portal is breached, attackers can use that access to pivot into connected healthcare APIs.

In many cases, attackers do not need to breach the healthcare organization directly. They simply target a less secure vendor with API access to PHI. This is exactly what happened in several of 2024's largest breaches, where third-party vendors were the entry point for attackers.

The cost of ignoring API security in healthcare

The financial and regulatory consequences of an API-related breach can be severe. Since PHI is highly regulated under HIPAA, HITRUST, and other compliance frameworks, any exposure due to poor API security can result in:

- **HIPAA fines and regulatory penalties** for failing to protect patient data.
- **Lawsuits and financial damages** from affected patients.
- **Operational downtime and data loss**, disrupting patient care.
- **Brand and reputational damage**, leading to loss of trust.

As the number of third-party integrations in healthcare continues to grow, API security must become a top priority for IT and security teams. Organizations must take proactive steps to monitor API usage, detect credential misuse, and prevent excessive data exposure before a breach occurs.

2024's biggest healthcare data breaches — what went wrong?

The past year saw a surge in healthcare breaches, many of which stemmed from third-party vulnerabilities, API misconfigurations, and credential theft. Attackers increasingly exploited vendors and SaaS applications rather than targeting healthcare organizations directly. The following cases highlight some of the most significant breaches of 2024, demonstrating the risks posed by third-party integrations.

Change Healthcare (100M records exposed) – ransomware via third-party access

In February 2024, Change Healthcare, a major provider of billing and payment processing, was hit by one of the largest healthcare ransomware attacks to date. The BlackCat/ALPHV ransomware group exploited a compromised third-party API, allowing them to exfiltrate PHI before deploying ransomware. The breach disrupted medical billing across the country, leaving many hospitals and clinics unable to process payments. This attack highlights the risks of API credential theft and weak vendor security controls.

CHANGE HEALTHCARE

100 million
records exposed

Kaiser Foundation Health Plan (13.4M records exposed) – PHI leaked via tracking tools

Kaiser Foundation Health Plan reported a massive data exposure when unauthorized third-party tracking scripts embedded in their website collected and shared PHI with external companies. The breach occurred due to misconfigured SaaS tools, leading to the exposure of patient names, appointment details, and medical conditions.

KAISER PERMANENTE

13.4 million
records exposed

Ascension Health (5.6M records exposed) – API credential abuse

Ascension Health suffered a major breach when attackers exploited overprivileged API credentials from a third-party SaaS provider. The compromised credentials allowed unauthorized access to patient records, insurance details, and billing information. The breach went undetected for weeks due to a lack of API activity monitoring.

Ascension

5.6 million
records exposed

Perry Johnson & Associates (PJ&A) (14M records exposed) – vendor compromise

In May 2024, PJ&A, a Nevada-based medical transcription service provider, detected unauthorized activity within its IT systems. The investigation revealed that attackers had access to PJ&A's systems between March 27 and May 2, 2024, compromising the protected health information (PHI) of nearly 9 million individuals. Subsequent reports indicated that the breach affected additional clients, bringing the total number of impacted individuals to approximately 14 million. Exposed data included names, addresses, dates of birth, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, and clinical information from medical transcription files.

PJ&A

14 million
records exposed

HealthEquity (4.3M records exposed) – vendor account compromise

In March 2024, HealthEquity, a Draper, Utah-based financial technology and business services company specializing in health savings accounts (HSAs) and other consumer-directed benefits, identified suspicious activity involving a vendor's user accounts. These compromised accounts had access to an online data storage location (SharePoint), leading to unauthorized access to the personal identifying information (PII) of approximately 4.3 million individuals. The breached data primarily included sign-up information for accounts and benefits administered by HealthEquity, such as names, employee IDs, employer details, addresses, telephone numbers, Social Security numbers, general contact information of dependents, and payment card information (excluding payment card numbers/HealthEquity debit card information).

The compliance and regulatory landscape in 2025

Regulatory scrutiny on healthcare cybersecurity is increasing in response to the surge in third-party breaches and API security failures. The U.S. Department of Health and Human Services (HHS) is tightening cybersecurity requirements for healthcare organizations, with a focus on third-party vendor risk, API security, and real-time monitoring. Proposed updates to HIPAA and HITRUST frameworks emphasize multi-factor authentication (MFA), access controls, and continuous security audits.

The FTC and state regulators are also imposing stricter enforcement on data-sharing violations. In light of Kaiser's PHI exposure via third-party trackers, regulators are cracking down on unauthorized data flows, requiring healthcare providers to review SaaS configurations and third-party access (HIPAA Journal).

Why traditional security tools fail to secure the connected SaaS ecosystem

Most security tools are designed for endpoints, networks, or traditional IT systems—but they fail to detect threats in the connected SaaS ecosystem. SIEM and XDR solutions cannot see API-specific threats, and SSPM solutions only assess configuration and access risks, not real-time data flows. Without dedicated third-party application ecosystem security, healthcare organizations remain vulnerable to API-based attacks, vendor misconfigurations, and credential abuse.

To stay ahead of third-party threats, healthcare security teams must adopt solutions that provide real-time API security monitoring, automated risk detection, and direct integration with incident response workflows. By proactively monitoring third-party data flows and enforcing API governance, healthcare organizations can reduce breach risks and strengthen compliance with evolving regulatory standards.

Conclusion

Healthcare organizations are more connected than ever, but with increased reliance on third-party SaaS and APIs comes greater risk. Point-in-time vendor assessments and legacy security tools are not enough to prevent API-based threats. Healthcare security teams must implement real-time API monitoring, automated risk detection, and strict access governance to prevent data leaks, credential abuse, and supply chain compromises.

Organizations that take proactive steps now will not only reduce their risk of breaches but also stay ahead of evolving HIPAA, HITRUST, and HHS regulations. The time to act is now.

About Vorlon

Vorlon is the first easy way to detect and respond to third-party breaches. With Vorlon Third-Party Application Detection and Response (TADR), your vendor app ecosystem finally gets proactive security coverage like you have for your endpoints and cloud. After an agentless, proxy-free setup, you can monitor sensitive data flows, manage secrets, detect anomalies, and revoke access. Powered by patent-pending DataMatrix® technology, Vorlon creates an algorithmic model of your applications and connected services for faster, AI-driven remediation. Backed by Accel and SOC 2 Type 2 Certified, Vorlon is trusted by Fortune 500 companies and startups.

Learn more at vorlonsecurity.com.