BLUESIGHT™

2026 Privacy Trends

THE STATE OF HEALTHCARE PRIVACY OPERATIONS

2026 Privacy Trends

Introduction

The 2026 Privacy Trends Report marks a transition from Bluesight's annual Breach Barometer reports, focused on retrospective breach reporting, to a more comprehensive set of privacy insights about the industry at large.

This report analyzes data throughout 2025, and where applicable, includes trends dating back to 2023. While 2024 was defined by a single catastrophic event that drove breached records to an all-time high of over 305 million, 2025 revealed a more insidious trend: the weaponization of internal access and the exploitation of privacy data vulnerabilities.

This report leverages three distinct data sources:

1. **Publicly Available Breach Data**

   Federal and state-level incident tracking, industry-reported data points, and historical context from previous Breach Barometer reports.

2. **Bluesight PrivacyPro Platform Data**

   Real-world metrics from over 1,400 healthcare sites using patient privacy monitoring powered by machine learning.

3. **2026 Healthcare Privacy Survey**

   Insights from 43 healthcare privacy and compliance professionals on current priorities and risks, conducted by Bluesight in March 2026.

Table of Contents

Key Trends

Trend 1

The Transparency Gap of True Scale vs. Reported Data

Federal Department of Health and Human Services (HHS), Office for Civil Rights (OCR) data often fails to reflect the immediate reality of a breach due to placeholder reporting and extended forensic timelines.

Trend 2

Insider Threats Remain High

Insider threats continue to be the most persistent and expensive vulnerability for healthcare organizations

Trend 3

Healthcare Breach Costs Remain Highest for 12th Consecutive Year

Despite a decrease from 2024's record highs, healthcare breaches in the United States averaged $7.42 million per incident in 2025, 67% higher than the global average.

Trend 4

Early Detection Saves Millions

Compared to two years prior, healthcare organizations in 2025 reviewed nearly 50% more cases and identified nearly 70% more violations, indicating greater precision in detecting high-risk access.

Trend 1
The Transparency Gap of True Scale vs Reported Data

Federal reporting from the US Department of Health and Human Services Office for Civil Rights (HHS OCR) often misses the full scope of each breach due to the 500-record threshold for public disclosure.

In 2025, approximately 710 large healthcare data breaches were reported to HHS OCR, affecting at least 61.6 million individuals (HIPAA Journal). One of the most significant incidents that year was the Conduent breach in October 2025. This business associate initially reported 42,616 individuals impacted to the OCR. However, state filings in Texas and Oregon later confirmed that over 25 million individuals were affected nationwide, making it the largest healthcare-related breach of 2025.

61.6M individuals affected by large healthcare data breaches in 2025

2025 Major Breach Incidents

In 2025, attackers shifted focus toward high-value targets, such as business associates and large insurers. The four largest breaches reported to HHS in 2025 include:

Conduent Business Services *October 2025*	Over 25 million individuals affected via claims processing systems.
Aflac *August 2025*	13.9 million individuals affected by a Scattered Spider group cyberattack.
Yale New Haven Health *March 2025*	5.56 million patients affected; $18 million settlement.
Episource *February 2025*	5.42 million patients impacted by a ransomware attack on a medical coding vendor.

Source: HIPAA Journal

Trend 2
Insider Threats Remain High

Insider threats, tied to staff activity, remain an ongoing and expensive vulnerability for healthcare organizations, occurring year after year despite security measure improvements. These threats fall into two categories: insider error and insider wrongdoing, the latter referring to intentional misbehavior.

While insider threats remain the second highest category of data breaches reported to HHS OCR, behind hacking and IT incidents, **the financial and reputational impact of insider-related breaches remains disproportionately high**. This persistent pattern reinforces that the insider threat is not a secondary concern but a consistent and significant source of organizational risk

Insider Threats in 2025

Insider breaches remained a persistent threat to healthcare organizations in 2025, with both accidental and malicious insider incidents continuing to compromise patient data. Notable 2025 insider breach incidents include:

61,104 patient records

Texas HHSC: Seven employees were fired and referred for prosecution after unauthorized access to 61,104 records.

5,357 patient records

Harris Health: One employee terminated after accessing 5,357 patient records over a ten-year span.

2,599 patient records

Jackson Health System: One employee accessed 2,599 patient records over five years without authorization.

1,421 patient records

Berkshire Health Systems: An employee accessed 1,421 patient records without a valid work-related purpose.

Sources: Texas Health and Human Services, Texas Tribune, Harris Health, Jackson Health System, HHS OCR Breach Portal, HIPAA Journal

Trend 2
Insider Threats Remain High

Rising Costs

The financial burden of managing internal threats remains the highest for healthcare and pharmaceutical organizations. **The total annualized cost of insider security incidents averaged $28.8M per healthcare organization in 2025**, down slightly from $29.2M in 2024 (Ponemon Institute). These costs encompass the entire lifecycle of risk management and total annual financial burden per organization, including the immediate response, as well as ongoing expenses of monitoring, detection, and long-term forensic investigations. Globally across industries, negligent or mistaken employees are both the most frequent and most costly source of insider incidents, accounting for 53% of all incidents and $10.3M of the $19.5M global average annual cost per organization – more than twice the $4.7M attributed to malicious insiders.

Year-Over-Year Comparison

Compared to 2024, insider threats in 2025 shifted from massive, single-event exposures to a higher frequency of small-scale incidents. While unauthorized access incidents increased 17% in volume, the total number of individuals affected dropped dramatically – from around 16M in 2024 to just under 2M in 2025 (HIPAA Journal). This decrease in impact may be attributed to broader industry investment in both employee training and privacy monitoring technology. Bluesight's platform data supports this conjecture, showing a **35% increase in organizations using PrivacyPro between 2023 and 2025**.

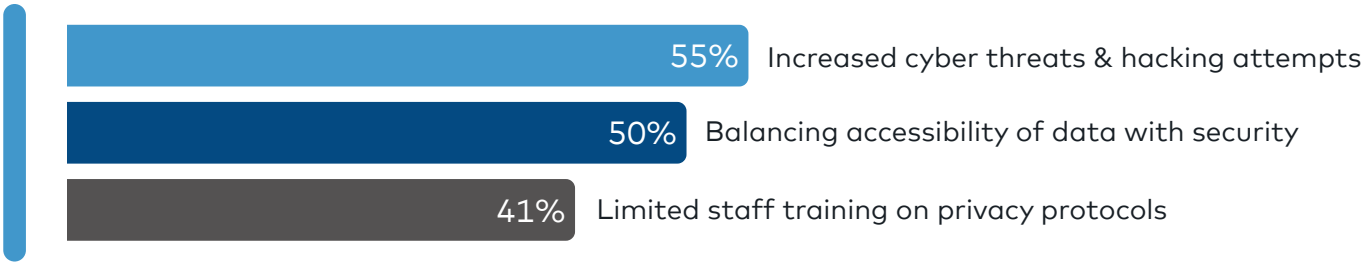
The Breach Reality: Causes and Frequency

The threat environment remains high, with 55% of surveyed organizations experiencing a patient data breach within the last 12 months. When identifying the root causes of their most significant breaches, two areas stood out:

1	**Third-Party Vulnerabilities**	**40%** of respondents identified third-party vendor compromise as the main cause of their most significant breach.
2	**The Insider Threat**	**25%** attributed their breaches to insider threats, whether intentional or accidental.

Trend 3
Healthcare Breach Costs Remain Highest for 12th Consecutive Year

Privacy and compliance professionals identified their top three challenges for maintaining and ensuring patient privacy in 2026:



When a privacy lapse occurs, the consequences extend well beyond the incident itself. **The most significant team-level impacts include time spent on damage control and reporting (83%)**, loss of trust from patients and stakeholders (76%), and increased administrative workload to address compliance gaps (64%). For healthcare teams, a data breach is not just a financial or legal event, but also a massive operational disruption.

The Financial Toll

In 2025, **the average cost of a healthcare data breach was $7.42M**, down from the record $9.77M in 2024 (IBM). Healthcare remains the most expensive of any industry for the 12th straight year, running **67% above the global all-industry average** of $4.44M. On average, the three largest costs across all industries are:

$1.47M **Detection and Escalation**	Forensic and investigative activities, assessment and audit services, and crisis management
$1.38M **Lost Business**	The "hidden" cost, including business downtime, the cost of acquiring new customers to replace those who left, and reputation loss
$1.2M **Post-Breach Response**	Help desk activities, inbound communications, legal fees, and regulatory fines

Beyond these costs are also a significant reallocation of staff time and resources across security, legal, and IT teams, where staff are pulled away from operations to manage technical discovery, business stabilization, and regulatory compliance.

Trend 3
Healthcare Breach Costs Remain Highest for 12th Consecutive Year

Why Healthcare Costs are Unique

Three factors consistently drive healthcare's outsized breach costs. First, dwell time: in 2025, healthcare breaches took an average of 279 days to identify and contain, which is five weeks longer than the global average (Deep Strike). The speed of response has a direct financial impact as well. Across all industries, organizations that identify and contain a breach in under 200 days save an average of $1.14 million compared to those with longer containment timelines (Total Assure).

279 average days to identify and contain a healthcare breach

Second, target value: medical records command up to $500 each on the dark web, making healthcare data disproportionately attractive to bad actors (Deep Strike).

Third, Shadow AI exposure: Despite HIPAA requirements for complete auditability of patient data access, only 35% of healthcare organizations have meaningful visibility into how staff are using third party AI tools, which may be producing unknown risk against PHI exposure (Kiteworks).

35% of healthcare organizations have visiblity into how staff are using 3rd party AI tools

Healthcare organizations are responding to this threat by standing up AI governance committees, and compliance leaders who have opted out of AI entirely cite data privacy concerns, accuracy limitations, and organizational policy as their primary reasons. Even so, the risk remains material: across all industries, organizations with high levels of unmonitored AI adoption face **an average of $670,000 in additional breach costs** (IBM).

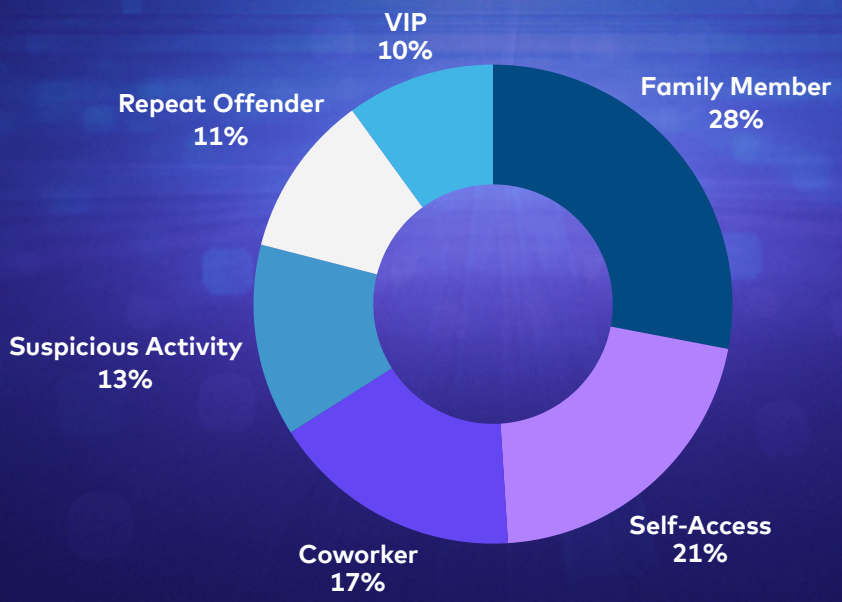
Trend 4
Early Detection Saves Millions

The shift toward proactive monitoring is reflected in the massive growth of case reviews. In 2025, PrivacyPro customers reviewed nearly 200,000 cases, representing a 46% increase since 2023. More notably, violation identification increased 69% over the same period, indicating that organizations are not just reviewing more cases, but becoming more accurate at distinguishing genuine privacy violations from routine access events. This improvement reflects a maturing approach to privacy monitoring that is consistent with more true signals.

↑69% increase in patient privacy violation identification from 2023 to 2025

2025 Top Access Categories and Clinical Context

The following categories represent the most frequently reviewed access scenarios across PrivacyPro customers in 2025. Together, they reveal where the boundaries between clinical workflow and privacy violation are most frequently tested.



The Proactive Monitoring Dividend

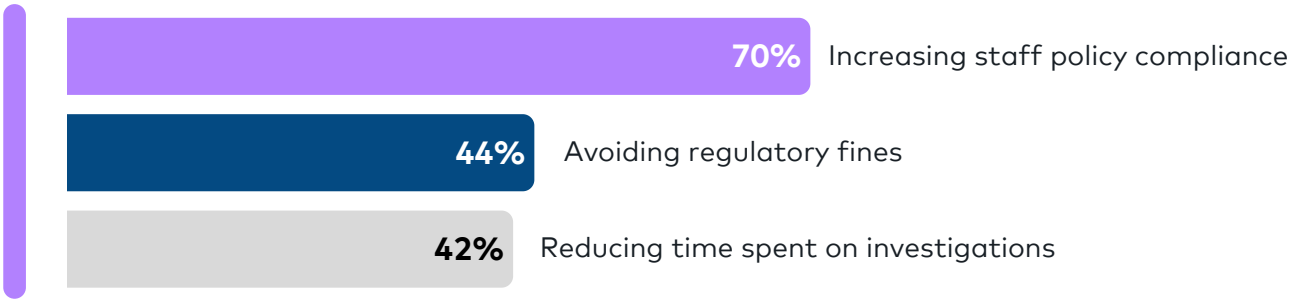
Family member access remains the most reviewed category at 28%. While these cases sometimes stem from benign intentions, such as an employee checking on a relative's care or acting on a patient's informal request, they still represent a policy violation. Self-access at 21% carries a similar dynamic, as employees often perceive accessing their own records as harmless, yet it bypasses the established clinical disclosure workflows that exist to protect all patients equally.

At the other end of the spectrum, repeat offenders (11%) and VIP access (10%) represent lower volume but disproportionately higher risk. Repeat offenders represent cases where a privacy violation has already occurred once and was not sufficiently deterred, making this category a direct indicator of where re-education efforts may be falling short. VIP access, which involves high-profile patients such as public figures or executives, remains a high-stakes area where a single lapse can lead to major reputational damage for healthcare organizations.

ROI of Privacy Monitoring Teams and Software

While quantifying ROI for patient privacy programs can be challenging, survey data shows that **70% of healthcare organizations identify increasing staff policy compliance as their primary measure of success**.

Risk mitigation and efficiency follow closely, with 44% prioritizing the avoidance of regulatory fines and 42% focused on reducing time spent investigating incidents. Other teams share more unique measures such as quicker identification of opportunities for improvement and an overall decrease in the number of alerts.



Trend 4
Early Detection Saves Millions

Privacy officers are increasingly moving away from reactive audits in favor of continuous, proactive monitoring – with **81% of surveyed healthcare privacy and compliance leaders now using a dedicated software tool** to do so. The data also reveals what healthcare organizations expect from their privacy monitoring technology:

Defining the Best Software

51% of professionals define an industry-leading privacy solution as one that provides proactive, around-the-clock monitoring and rapid breach response.

Vendor Expectations

86% of respondents cited better functionality and consistent innovation as the primary reasons they would consider switching privacy monitoring vendors.

Desired Features

The top capabilities organizations look for in a monitoring solution are a user-friendly interface (86%), easy integration with existing IT systems (84%), and advanced analytics via machine learning and AI (77%).

2026 Privacy Trends Key Takeaways

Breach Costs Show Signs of Stabilizing: After reaching a record $9.77M in 2024, the average healthcare breach cost declined to $7.42M in 2025 – though lengthy detection timelines, the high value of medical records on the dark web, and growing shadow AI exposure continue to keep risks elevated.

Insider Threats Dominate: Negligent employees remain the most frequent and costly source of insider incidents globally and the second leading cause of healthcare breaches – a risk compounded by the fact that only a third of healthcare organizations have visibility into how their staff are using third-party AI tools.

Adoption of Privacy Monitoring Technology: 81% of surveyed healthcare organizations report using a dedicated monitoring tool, and organizations that have invested in a machine-learning based tool are identifying 69% more genuine violations than they were just two years ago.

About Bluesight®

Bluesight powers hospital and pharmacy operations with intelligence that simplifies inventory management, procurement, and compliance. Through its suite of industry-leading solutions, Bluesight ensures that health systems protect every patient and optimize every dollar. Over 3,000 United States and Canadian hospitals rely on Bluesight every day to have efficient and safe operations.

Request a Demo

Bluesight.com | 1800 Duke St. Suite 108 | Alexandria, VA 22314 | Phone: 786.548.2432 | ©2026