BLUESIGHT™

2025 Breach Barometer®

Introduction

At Bluesight, we are dedicated to empowering healthcare organizations with intelligence to simplify inventory management, procurement, and compliance. Our patient privacy monitoring solution leverages machine learning to accurately and efficiently safeguard protected health information (PHI), ensuring healthcare organizations can focus on delivering exceptional care while maintaining adherence to strict compliance regulations. Bluesight offers a comprehensive solution to safeguard patient data, maintain regulatory compliance, and mitigate both reputational and financial risks.

Since 2016, the Breach Barometer report has tracked data breaches affecting U.S. patient and health data, leveraging a broader dataset than HHS's public breach tool. The 2025 report builds on these methods and includes analyses from Bluesight and DataBreaches.net.

In 2024, 1,160 breach reports were compiled, with 1,043 being new incidents. A staggering 305,527,355 patient records were breached—a sharp increase driven by a single catastrophic event. The healthcare industry continues to grapple with increasing cyber threats as well as delayed notifications and transparency issues. Explore the full report to uncover the key trends and lessons from this challenging year.

Contents

Key Themes

Trend 1: **Records Breached are at an All-Time High**

More than 300 million patient records were breached, marking a 26% increase over 2023. This includes the largest healthcare breach ever recorded, affecting 1 in 2 Americans.

Trend 2: **Insider Threats and Hackers Drive Breach Impact**

Insider errors and hacking-related incidents were the dominant drivers of healthcare data breaches in 2024, causing significant disruptions to patient privacy and exposing sensitive medical information on a large scale.

Trend 3: **Lack of Transparency and Notifications**

Many entities failed to disclose breaches or notify patients within required timeframes. Notifications took an average of 205 days after an incident, a significant delay compared to previous years.

Trend 4: **Rising Cost of a Healthcare Data Breach**

Healthcare data breaches in 2024 averaged $9.77M, with rising costs from ransomware, legal actions, and regulatory fines, placing immense strain on healthcare organizations.

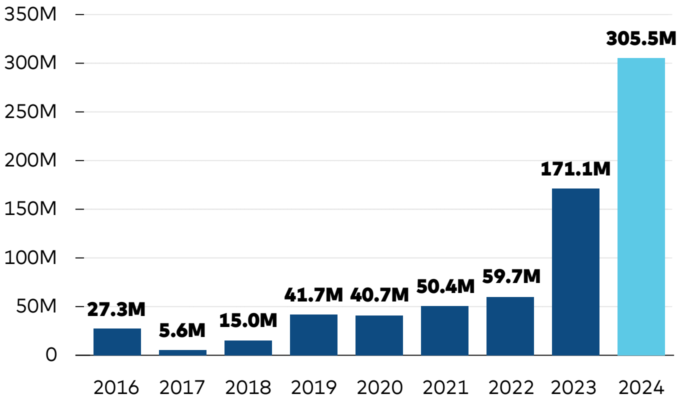
Trend 1: **Records Breached are at an All-Time High**

2024 Breached Records Overview

A Year of Unprecedented Challenges

In 2024, the healthcare industry experienced a concerning surge in data breaches, with over 300 million patient records compromised — a 26% increase from 2023. The Breach Barometer reported 1,160 incidents, including 1,043 new breaches, with 816 providing data on the number of records affected. A single catastrophic breach accounted for 190 million records, the largest breach ever recorded, contributing to a staggering total of 305,527,355 patient records compromised. This alarming trend highlights the urgent need for stronger cybersecurity measures to protect sensitive patient data and maintain trust in the healthcare industry.

Figure 1. Number of Breached Records for All Reports Compiled by Breach Barometer Per Year



It is important to note that many of these breaches actually occurred in 2023 but were only disclosed or reported in 2024, which demonstrates one of the hurdles in delayed breach notification practices.

Annual reports for the U.S. healthcare sector often highlight the most significant data breaches as recorded on HHS's public breach tool. Table 1 shows the top five largest breaches reported to HHS in 2024, along with the type of each incident. It is important to note that many of these breaches actually occurred in 2023 but were only disclosed or reported in 2024, which demonstrates one of the hurdles in delayed breach notification practices.

The overwhelming scale of these incidents, particularly the Change Healthcare breach, underscores the evolving threat landscape in healthcare data security. It is clear that addressing these challenges requires a proactive, collaborative approach to strengthen data security and protect sensitive healthcare information.

Table 1. Five Largest Breaches Reported to HHS in 2024

Name	Role	Records Breached	Incident Type
Change Healthcare	Business Associate	**190,000,000**	Ransomware attack
Kaiser Foundation Health	Health Plan	**13,400,000**	Pixel tracking error
Ascension Health	Healthcare Provider	**5,599,699**	Ransomware attack
HealthEquity, Inc.	Business Associate	**4,300,000**	Credential compromise
Concentra Health Services	Healthcare Provider	**3,998,163**	Hacked medical transcription

Trend 1: **Records Breached are at an All-Time High**

Type of Entity

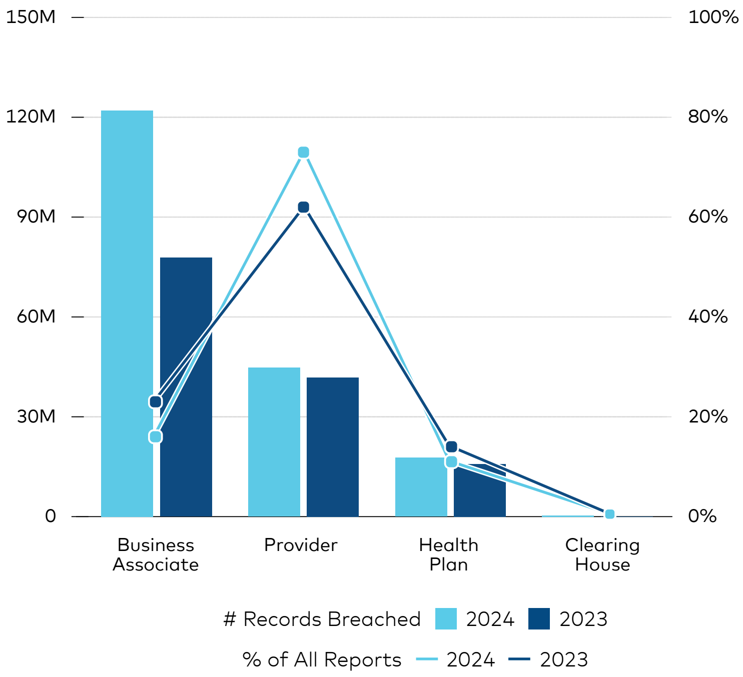
Business Associates were Responsible for 66% of All Breached Records

HHS's breach data provides valuable insights into how different types of entities contribute to healthcare data breaches. The primary entity types include healthcare providers, business associates, health plans, and clearinghouses. Each plays a distinct role in the healthcare ecosystem, and their involvement in breaches varies significantly. Providers were responsible for the majority of reports submitted to HHS in 2024, accounting for 73% of all reports. However, they represented only 24% of all breached records, highlighting a disparity between the volume of breaches and their overall impact. Conversely, while business associates submitted only 16% of reports, they represented a staggering 66% of all breached records—a clear indication of the significant risks posed by third-party entities.

Analyzing the data from 2023 and 2024 underscores consistent trends in how entity types contribute to breaches. Across both years, business associates are found to be the leading source of breached records, with their share growing in 2024. Furthermore, breaches involving business associates (regardless of the reporting entity) accounted for 66% of breached records in HHS's 2024 dataset. This trend was mirrored in the Breach Barometer data, which revealed that 77% of all breached records were linked to incidents involving business associates.

These findings serve as a critical reminder for healthcare entities to strengthen risk management and oversight when engaging with business associates to mitigate potential vulnerabilities.

Figure 2. Entity Types by # Records Breached, and % of All Reports Between 2023 and 2024



Insider Threats

Insider Errors Resulted in Nearly 16 million Breached Records — A Sharp Increase from Previous Years

Insider breaches, whether accidental or deliberate, continue to pose a significant threat to data security. In 2024, insider errors, such as email mistakes or misconfigured cloud storage, resulted in nearly 16 million breached records—almost quadruple last year's number of breached records for insider-error incidents. Leveraging automated machine learning in cybersecurity can be an effective solution for addressing human vulnerabilities.

While less common, insider-wrongdoing caused substantial damage, with over 1.3 million records compromised in 2024 due to malicious actions like terminated employees exploiting access for financial gain. To mitigate insider threats, organizations must adopt proactive measures, including advanced monitoring tools, strict access controls, and regular audits. By fostering a culture of accountability and vigilance, companies can reduce risks and better protect sensitive data.

Hacking and Ransomware

Hacking-Related Incidents Accounted for 82% of Breaches Reported in 2024

Analysis of breaches in 2024 continued to highlight the dominance of hacking-related incidents in the cybersecurity landscape. According to HHS's public data set, 586 out of the 720 reports (81%) were coded as "Hacking/IT Incidents" and accounted for 91% of all breached records. Similarly, the Breach Barometer recorded 852 hacking-related incidents out of 1,043 new reports, representing 82% of reported breaches and 94% of compromised records. While these percentages align closely with those reported by HHS, differences in methodologies and reporting details underscore the complexity involved in accurately capturing data. Notably, Breach Barometer documented 267 more hacking incidents than HHS, further emphasizing variations in data collection and reporting processes. These hacking-related incidents not only compromise sensitive information but are often associated with significant financial costs, including ransoms, legal fees, regulatory fines, and reputational damage.

A major challenge in analyzing hacking incidents is distinguishing between different types of cyberattacks, particularly ransomware, which often blurs the lines between encryption, data theft, and extortion. This ambiguity makes it difficult to differentiate between ransomware attacks (involving encryption and ransom demands) and hacking incidents involving data theft and extortion, leading to underreporting and underestimations in breach analyses. Further complicating matters, many incidents go unreported or include placeholder data for breached records. For instance, over 200 incidents in the 2024 dataset lacked breach counts, with most tied to ransomware or extortion events that entities failed to disclose to regulators.

Trend 3: **Lack of Transparency and Notifications**

Gaps in Discovery and Notification

Breaches in 2024 Took an Average of 102 Days to be Identified — Up from 79 Days in 2023

In 2024, the time between when a breach occurs, is discovered, and is reported to those affected increased significantly, highlighting critical issues in breach identification and management protocols. On average, it took organizations 102 days to identify a breach, a sharp increase from 79 days in 2023. This longer exposure period significantly heightens the risk of sensitive information being misused or stolen. Furthermore, once a breach was discovered, the average notification time stretched to 205 days, compared to 177 days in the previous year. These delays left affected individuals unaware of the risks to their personal data, delaying crucial protective actions like changing passwords, freezing credit, or monitoring for fraudulent activity.

Delays left affected individuals unaware of the risks to their personal data, delaying crucial protective actions.

These widening gaps in discovery and notification not only put individuals at greater risk of harm but also reflect poorly on organizational readiness to detect and respond to breaches. Such delays can lead to regulatory penalties and legal consequences, as timely breach reporting is often a requirement under data protection laws. Addressing these gaps must become a priority for organizations to protect both their stakeholders and their compliance standing.

Table 2. Number of Days from Breach to Discovery

	Mean	Median
2021	140.3	21.8
2022	95.5	14
2023	79.2	10
2024	101.8	8

Table 3. Number of Days from Discovery to Notification

	Mean	Median
2021	117.4	64
2022	117.4	79.5
2023	112.6	60
2024	127.7	87

Table 4. Number of Days from Breach to Notification

	Mean	Median
2021	227.8	133.5
2022	229.6	154
2023	176.9	83
2024	205.4	116

Trend 4: **Rising Cost of a Healthcare Data Breach**

Cost of a Healthcare Data Breach in 2024

The Financial Toll of Healthcare Data Breaches

The financial impact of data breaches in the healthcare sector reached alarming levels in 2024. According to IBM's **Cost of a Data Breach 2024** report, the global average cost of healthcare breaches averaged $9.77 million, making it the most expensive sector for data breaches despite a 10.6% decrease from the previous year. This decline was reported early in 2024, but subsequent incidents likely drove the annual average higher. Two major breaches dominated headlines: UnitedHealth Group faced over $2.5 billion in costs after the Change Healthcare breach, and Cencora paid an astounding $75 million ransom, excluding additional costs for incident response and forensics. Beyond ransoms, expenses extended to regulator investigations, mitigation services, and potential class-action lawsuits.

Ransomware attacks are a major financial burden for healthcare organizations, as cybercriminals exploit vulnerabilities in critical infrastructure and demand higher ransoms. These breaches not only increase costs but also disrupt operations, forcing hospitals to divert resources, delay patient care, and undergo lengthy recoveries. To address these challenges, healthcare organizations must adopt holistic cybersecurity frameworks to reduce financial exposure, safeguard patient data, and minimize operational disruptions in an increasingly threat-filled digital landscape.

Beyond Financial Costs

The True Costs of Healthcare Data Breaches

While the monetary repercussions of healthcare breaches were staggering in 2024, the true cost often exceeded financial damage:

- **Patient Safety Risks:** Ransomware attacks and data breaches frequently disrupted essential hospital operations. For instance, a ransomware attack on Synnovis in the United Kingdom severely impacted services provided by the NHS, causing months of delays, appointment cancellations, and documented harm to patients.
- **Erosion of Patient Trust:** Breaches undermined confidence in healthcare providers, particularly when insider threats, such as data snooping or improper sharing, were involved. Restoring trust after such events proves challenging and often requires significant reputational recovery efforts.
- **Patient Churn:** Breaches can lead to increased patient turnover, with some individuals switching to alternative providers where available. This exacerbated challenges to patient loyalty and retention for already-burdened healthcare institutions.
- **Higher Cyberinsurance Costs:** Entities that experience breaches can face steep hikes in cyberinsurance premiums, and some reported difficulty obtaining coverage altogether due to heightened risks. This development added an extra layer of strain for organizations already grappling with the effects of a breach.

The escalating cost, complexity, and consequences of healthcare data breaches in 2024 serve as a stark reminder of the critical importance of robust cybersecurity strategies, proactive risk management, and ongoing investments in patient data protection. Without these measures, healthcare organizations risk not only their financial stability but also the trust and safety of the patients they serve.

Key Takeaways from the 2025 Breach Barometer Report

- **Over 300 Million Records Breached:** An all-time high of 305,527,355 patient records were reported breached in 2024, representing a staggering increase in the severity of healthcare data exposure.
- **Business Associate Breaches Dominate:** Breaches involving business associates accounted for the majority of breached records (77%) in the 2024 Breach Barometer dataset, highlighting continued vulnerabilities in third-party relationships.
- **Delayed Disclosure Remains an Issue:** Hundreds of entities failed to disclose breaches or notify patients in a timely manner, leaving individuals exposed to prolonged risk and raising compliance concerns.
- **Rising Threat of Ransomware and Extortion:** The proliferation of threat actor groups and diversification of attack methods, including ransomware and data exfiltration with extortion demands, reinforced the critical need for robust cybersecurity measures across healthcare organizations.
- **Soaring Financial Costs of Breaches:** Healthcare data breaches in 2024 incurred an average cost of $9.77 million, emphasizing the urgent need for stronger prevention and response strategies.

The 2025 Breach Barometer Report highlights the critical challenges and escalating risks faced by the healthcare sector in securing patient data. With a record-breaking 305 million patient records breached in 2024, largely driven by the largest healthcare breach in history, the report underscores the urgent need for comprehensive cybersecurity measures. Key findings reveal business associates remain a significant vulnerability, responsible for the majority of breached records, while insider threats and sophisticated hacking methods, including ransomware, continue to proliferate. Additionally, gaps in breach discovery and notification have further exposed individuals to risks, eroding trust and amplifying financial strain. Amid these challenges, the report serves as a clarion call for healthcare organizations to prioritize robust data protection strategies, improve transparency, and foster a culture of accountability to mitigate risks and safeguard both patient data and trust. By taking a proactive action, healthcare organizations can work toward a more secure and resilient future.

For more insights, visit **Bluesight.com**

Privacy Monitoring Insights from Clearwater

Protecting Patient Privacy Through Expert — Tech-Enabled — Services

Clearwater
Healthcare – Secure, Compliant, Resilient

Rapid shifts in healthcare delivery, the adoption of new technologies, and the accompanying risks make protecting patient privacy and managing regulatory risks more important than ever. Healthcare organizations today are undergoing pressure to quickly detect and address suspicious activity surrounding health information—potential signs of inappropriate access, misuse of data, and even external threats.

At **Clearwater**, we've created a practical, in-depth approach to analyzing user behavior and access patterns using tools such as Bluesight (formerly Protenus for Patient Privacy). In this section, we'll explore the key factors involved in our analyses and share real-world examples that highlight how robust reporting and analysis can safeguard patient privacy and strengthen trust.

Critical Factors in User Activity Analysis

When assessing potential anomalies in user access patterns, Clearwater experts consider a number of factors to determine whether further investigation is necessary. One key consideration is whether the user's department and job title align with the actions performed in the patient's record, and if not, can we identify a rationale that might justify the access. Abnormal patterns in activity in the electronic health record usually signal inappropriate access.

Other considerations include the volume of information accessed, high frequencies of access within a specific timeframe, access of records by co-workers, and access to information about VIPs, such as celebrities and politicians. Generally, cases where a user's activity stands out starkly from their usual habits or peers may signal misuse. Additionally, we take into account client-specific policies, such as prohibitions on self- accessing records, ensuring the analysis aligns with compliance requirements.

Real-World Investigations and Outcomes

Accessing a record of a patient with the same address

An investigation found a doctor accessed the medical record of a patient living at the same address. While there could be legitimate reasons for this type of access, a review of access over a period of six days, including activity before and after the incident, showed behavior that didn't match typical care workflows. For example, during the six-day period, the provider accessed only two distinct records, including their own.

Additionally, the data reviewed in the patient's chart did not align with the typical responsibilities of the specific doctor's practice. The investigation included interviews with the doctor and medical director, and the organization ultimately decided to terminate the doctor's employment.

Unauthorized access to a coworker's record

Another analysis involved unusual access patterns when a nurse from a surgery department accessed a colleague's medical record. This event was particularly suspicious as the user had not accessed any other records for four hours beforehand, and the patient record was accessed after normal operating hours.

Another indication of suspicious activity: the nurse only accessed a sidebar report, showing information about diagnosis. This type of activity was unusual both for the nurse and well as their colleagues, since multiple reports and screens are typically used during patient chart reviews.

Even though the investigation revealed the user only accessed limited metrics during the review, the organization concluded the behavior constituted a HIPAA violation, leading to the employee's termination.

The Role of Data-Driven Insights in Preserving Privacy

These examples underscore Clearwater's commitment to leveraging advanced user activity analysis to protect patient privacy and bolster workplace accountability. Insights gained through deep analysis of data access play a crucial role in patient privacy monitoring by identifying unusual access patterns, detecting potential breaches, and ensuring compliance with privacy regulations without compromising the quality of care.

By leveraging Clearwater expertise along with Bluesight, healthcare organizations can proactively detect and respond to unauthorized access without placing undue burden on the workforce. An effective monitoring program not only strengthens privacy and security of the health information, it also builds trust among patients and the community, reassuring them their sensitive information is protected. Additionally, these insights help organizations continually refine policies, adjust their risk tolerance, improve workflow efficiency, and mature overall data governance, creating a safer and more transparent healthcare environment.

About Bluesight

Bluesight powers your hospital and pharmacy operations with intelligence that simplifies inventory management, procurement, and compliance – ensuring every patient is protected and every dollar is optimized. Over 2,400 hospitals trust Bluesight's solutions to connect disparate data, teams, and processes to reveal the story behind it all.

About DataBreaches.net

DataBreaches.net is a website devoted to reporting on data security breaches, their impact, and legislative developments relevant to protecting consumer and patient information. In addition to providing news aggregation from global sources, the site also features original investigative reporting and commentary by the site's owner, a healthcare professional and privacy advocate who has blogged pseudonymously as "Dissent Doe" since 2006.

BLUESIGHT™

www.bluesight.com