What the Last Decade of OCR Breach Data Reveals

Jericho Simmons
Shield and Seed LLC
1/2026

Executive Summary

Over the past decade, healthcare cybersecurity has undergone a fundamental shift. While breach reporting volumes have stabilized in recent years, the scale, reach, and consequence of breaches have grown dramatically. Data from OCR between 2015 and 2025 shows that modern healthcare breaches are no longer defined by how often they occur, but by how much damage a single incident can cause.

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

~~The most important change is not frequency. It is concentration. Patient data is now centralized in network servers, cloud platforms, and email systems that create unprecedented blast radius when controls fail. In 2024 alone, hundreds of millions of patient records were exposed through server-based incidents. Once exposure reaches that scale, traditional incident response assumptions break down. Communication, governance, and leadership decision-making become the determining factors in outcomes.~~

~~This data also confirms a shift in attacker behavior. Hacking and IT-related incidents now dominate healthcare breaches, driven by the high value of patient data and the relatively low cost of exploiting under-secured environments. Compliance-driven security programs and checkbox certifications have not kept pace with this reality. Organizations that rely on compliance as a proxy for security consistently underestimate both their exposure and their response readiness.~~

~~The most damaging failures do not begin with technology. They begin with misalignment at the leadership level. Boards receive metrics that do not support decisions. Executives lack clarity on escalation thresholds, communication authority, and vendor accountability. Risk assessments are performed reactively or inconsistently, leaving leaders unaware of gaps until an incident forces them into the open.~~

~~This article examines a decade of healthcare breach data through the lens of real-world breach response experience. It highlights where risk has accumulated, why traditional approaches fail at scale, and how leadership decisions before an incident largely determine outcomes after one occurs.~~

~~The central warning is clear. Healthcare organizations cannot eliminate breaches entirely, but they can decide whether they will face them with clarity or confusion. The difference lies in understanding where data lives, aligning leadership around risk ownership, and investing deliberately before pressure makes those decisions unavoidable.~~

Introduction

In 2015, the role of the CISO was still maturing across healthcare. Many organizations recognized the need for a security leader, but that role rarely had a seat in the executive room. Security was often grouped under IT and viewed as a technical function rather than an organizational risk. When a breach occurred, the security leader frequently became the scapegoat, expected to explain failures without having been empowered to influence decisions.

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

That mindset has shifted over the past decade. Increased regulation, public breach reporting, and the tangible business impact of cyber incidents have forced leadership teams to acknowledge that cybersecurity is not just an IT issue. It is an enterprise risk. While that evolution has been necessary, it has not resolved every misconception.

One of the most persistent misunderstandings is the belief that the CISO should have all the answers. In reality, the strength of a CISO is not omniscience. It is judgment. A capable CISO knows which questions to ask and how to connect the right people to arrive at the right answers. Without sufficient resources, authority, and operational support, even the strongest strategy remains theoretical. Documentation alone does not reduce risk. Action does.

Early in my career, before I led my first security team, I witnessed a ransomware attack that encrypted a file server. What stood out was not just the technical failure, but the leadership confusion that followed. Executives struggled to understand when the attack began, what was affected, and where the exposure truly lived. That moment clarified something for me early on. Security programs span many domains, but effective leadership depends on three foundational questions. First, can we prevent the attack from occurring? If not, can we respond quickly? And if response fails, can we reduce the scope of impact?

Those questions still guide how I evaluate controls today.

If there is one warning I would give to any board reading this article, it is this. A degree in the art of security provides definitions, but real strength comes from advisors who have carried the weight of decisions and outcomes. Experience, not theory, is what protects organizations when it matters most.

Over the last decade, OCR breach data has quietly documented this shift. From 2015 through 2025, the number of reported incidents has grown, but more importantly, the size, reach, and impact of those breaches have changed dramatically. The data tells a story of increasing concentration, growing dependency on centralized systems, and a widening gap between traditional security models and modern healthcare operations. What follows is not just a review of breach statistics. It is an interpretation of what those numbers reveal about how healthcare risk has evolved, and why our approach to security must evolve with it.

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Breach Volume and Patient Impact: When Stability Is the Most Dangerous Moment

~~When leaders see breach counts leveling off, there is a natural temptation to exhale. Stability can feel like progress. In reality, it is often the most dangerous moment.~~

~~Leveling breach counts are not a signal to celebrate. They are a signal to ask what storm may be forming next. This period should be treated as a pause between waves, not calm seas. It is a moment to reflect on lessons learned, examine where innovation has outpaced understanding, identify emerging threat actors, and address environments that have quietly accumulated risk. This is not a time to step away. It is a time to prepare the ground before the next rainfall begins, which requires strategic investment and engaged leadership.~~

~~Patient impact complicates this picture further. In healthcare, patient harm is never merely inconvenient. It becomes unmanageable when organizations try to force every risk into the same category and pursue perfection instead of prioritization. Not every threat demands the same level of response. Allowing minor, well-understood risks to exist within the ecosystem can prevent distraction from what truly matters. The danger begins when patient data is treated as just another asset. In reality, it represents someone's life. When patient impact is framed as a business nuisance, leadership intent should be reexamined.~~

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

~~The difference between breaches affecting thousands of records versus millions is profound. Financial models often dominate executive thinking, particularly when per-record cost estimates and insurance coverage are introduced. In some cases, cyber insurance or self-insured models soften the immediate financial impact. What they cannot absorb is the human consequence. Insurance fraud, identity misuse, and delayed care transform abstract risk into real harm. At that scale, breaches stop being theoretical and become deeply personal.~~

~~What organizations consistently fail to plan for once breaches cross this threshold is leadership execution under scrutiny. Incident response is not only a technical exercise. Communication quickly becomes the weakest link. Escalation paths are unclear. Authority to speak is undefined. Help desks are overwhelmed without scripts or guidance. Public-facing responses become inconsistent, and trust erodes in real time. These are not exceptional failures. They are predictable outcomes when breach response planning does not account for scale.~~

~~One of the first decisions leadership regrets after a large-scale incident is how long it took to involve the right people. I have worked with executives who preferred not to be informed until public notification was unavoidable, and others who wanted immediate awareness once an incident was confirmed, even before patient data exposure was established. These positions sit at opposite ends of the spectrum, yet both reveal the same gap. Organizations often lack a shared understanding of when escalation should occur, who has decision authority, and what information leaders need at each stage. A CISO does not decide when public reporting occurs, but they must know who does. Just as importantly, they must ensure communication protocols are defined long before an incident forces those decisions into the open.~~

~~The OCR data makes this clear. As breaches have grown in scale over the past decade, the cost of delayed or misaligned leadership communication has increased alongside them.~~

Breach Type Trends: Why Hacking Dominates and Why That Matters

Breach Type	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Hacking/IT Incident	56	114	149	165	314	457	546	570	608	609	457
Unauthorized Access/Disclosure	103	130	127	140	138	139	130	115	117	111	103
Loss	24	16	16	13	15	13	10	11	4	5	1
Improper Disposal	6	7	11	10	6	15	5	4	5	4	1
Theft	81	61	55	41	38	39	24	19	12	13	8

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Over the past decade, hacking and IT incidents have come to dominate healthcare breach reporting. This shift is not accidental, and it is not surprising.

Healthcare has been an attractive target for far longer than many leaders are willing to admit. The reason is simple. The return for attackers is high, and the investment required to succeed is often low. When a malicious actor can compromise a healthcare organization, extract millions of patient records, and sell that data for a relatively small amount per record, the scale makes the effort worthwhile. When entry-level tools costing a few hundred dollars can be used to breach an organization that has not operationalized security, the economics heavily favor the attacker. High-value data combined with weak execution creates an irresistible target.

Many organizations still rely on assumptions that were already fragile in 2015 and are now outright dangerous. One of the most persistent is checkbox compliance thinking. Certifications, annual assessments, and external attestations are often treated as proof of security rather than indicators of where work remains. A SOC 2 report or similar certification does not make an organization immune. The real question leaders must ask is why they are pursuing these checkboxes in the first place. If the goal is to reassure regulators or customers without improving real protections, the effort loses its value. A strong leader understands that while not every control in a report is critical, the report itself is not a checkbox exercise. It is an opportunity to protect both the organization and the people it serves.

When it comes to investment, the issue is not always that healthcare organizations are spending heavily in the wrong places. More often, they are not investing at all unless forced to do so by regulation or after suffering an incident. Regulatory pressure has improved baseline attention to security, but compliance-driven investment alone does not keep pace with evolving threats. Reactive spending tends to follow yesterday's attacks, not tomorrow's.

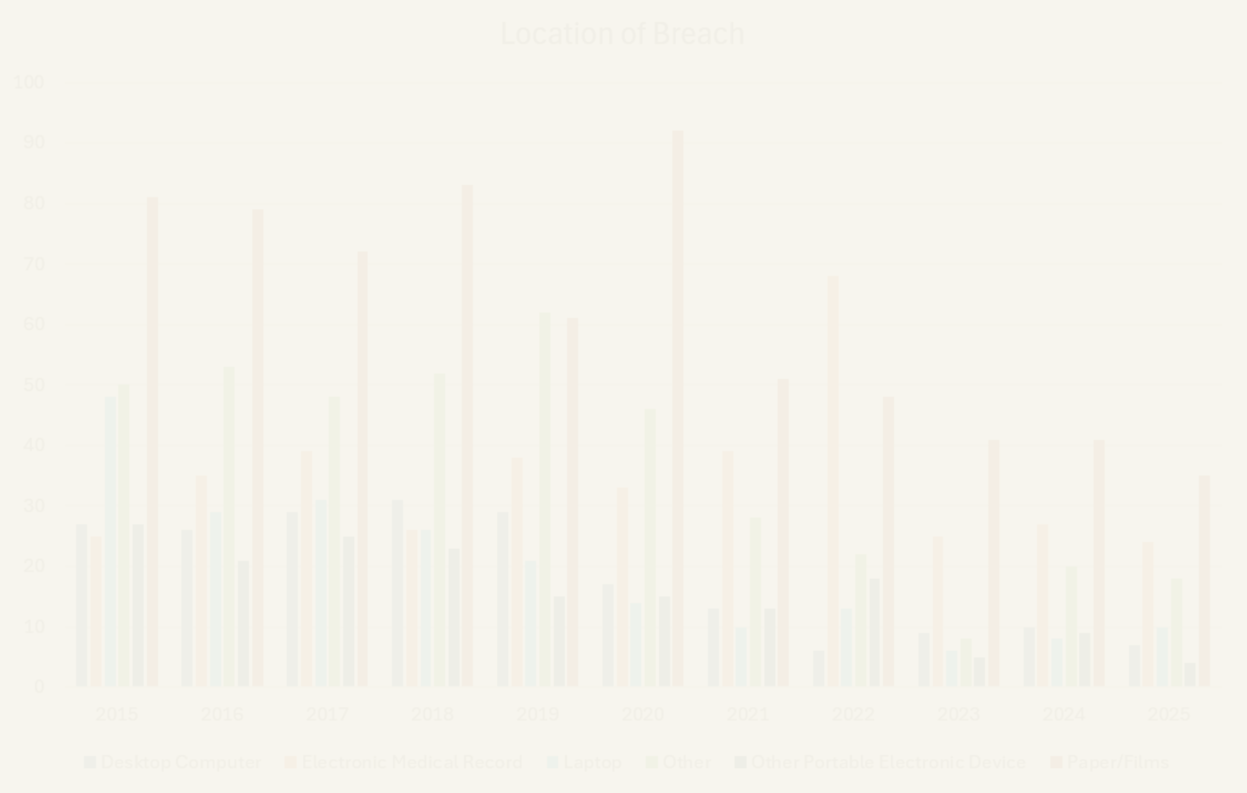
The dominance of hacking and IT incidents also reveals how attacker intent has changed. These attacks are both deliberate and opportunistic. Some actors view their actions as exposing negligence and expect reward or recognition in return. Others, including nation-state–backed groups, are focused on disruption, economic damage, and erosion of trust in healthcare infrastructure. Compounding this challenge is the rapid advancement of artificial intelligence. AI has crossed a threshold where it now enables faster, more persistent, and more adaptive attacks. This places enormous pressure on security operations centers, which are expected to respond more quickly while facing increasingly sophisticated threats.

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

~~One of the most common failures revealed during breach response is impact identification. Leaders often believe this capability is far stronger than it actually is. There is an assumption that once an attack is contained, understanding what was accessed or exfiltrated should be quick and definitive. In reality, forensic investigators are constrained by what has been instrumented in advance and by the practical limits of analysis. Containing an attack can happen quickly. Determining the full impact on data assets often takes far longer. This gap is why data identification and classification are so critical. When organizations understand where meaningful data resides, response efforts can focus on what truly matters instead of trying to analyze everything at once.~~

~~The OCR data reflects this reality. As hacking and IT incidents have increased, so has the complexity of understanding their consequences. Organizations that mistake detection for understanding find themselves unprepared for what comes next.~~

Breach Vectors: How Centralization Amplifies Impact



~~Over the last decade, network servers and email systems have emerged as the most common and consequential breach vectors in healthcare. This trend closely mirrors the industry's shift toward cloud adoption and centralized infrastructure. While these~~

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

changes have delivered operational efficiency and scalability, they have also dramatically expanded the blast radius of failures.

Cloud adoption has fundamentally altered how breaches unfold. Some security responsibilities can be transferred to cloud providers, but accountability does not disappear. Healthcare organizations remain responsible for how those environments are configured, monitored, and secured. When a foundational component fails, the consequences can cascade quickly. Recent history has shown how a single failure in shared infrastructure can disrupt services across the country. At the same time, cloud environments offer real advantages. The ability to scale computing power rapidly can accelerate response and recovery during an incident. This benefit should be factored into risk analysis. However, it comes with tradeoffs. Organizations lose direct control over foundational infrastructure security and become dependent on provider configurations or third-party tools to close gaps. In many ways, this mirrors running an on-premises data center, except the flexibility and complexity both increase.

Email presents a different, but equally underestimated, form of risk. Many leaders still view email primarily as a communication tool. In practice, it has become the organization's filing cabinet. Employees work directly from their inboxes, store sensitive information in email threads, and treat it as the central hub for daily operations. While this may improve productivity, it significantly complicates breach response. During forensic investigations, searching through thousands of mailboxes to identify exposed data, communications, or attachments becomes an enormous challenge. Email platforms have improved header detail and investigative tooling, but they still fall short of providing the level of forensic clarity needed to materially reduce response effort. Continuing to use email as a de facto file server increases exposure during business email compromise events. Archiving and deletion practices are often neglected, leaving environments unnecessarily large and difficult to analyze when breaches occur.

When incidents happen, leaders frequently discover that segmentation, access control, and visibility are not as mature as assumed. Many executives believe that security teams have comprehensive visibility into everything that is accessed and every action that occurs. In reality, access controls across most organizations remain uneven. Some mature organizations have invested in protecting a handful of high-risk areas, but enterprise-wide segmentation is far less common. Security teams cannot see everything on their own. Effective visibility requires participation across the organization, not just technology.

Convenience further compounds this problem. Healthcare organizations regularly trade user-impacting controls for a smoother user experience. When security measures affect login frequency, password behavior, or after-hours activity monitoring, leadership often

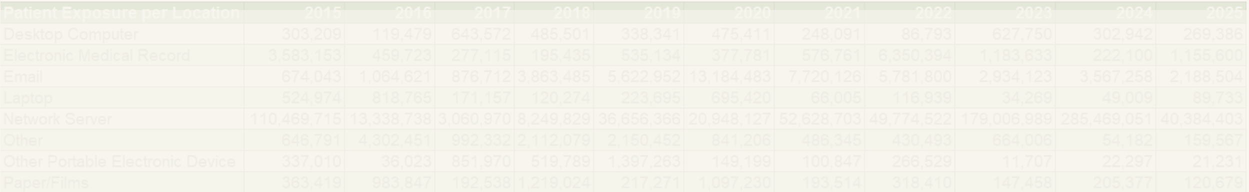
Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

~~demands immediate justification. The return on investment is questioned in traditional financial terms. What is often missed is the concept of risk reduction return on investment. Many security controls do not generate revenue, but they prevent losses that are otherwise inevitable. Experienced security leaders understand this balance, but they cannot enforce it alone. Protecting the organization requires visible support from other executives who are willing to accept measured friction in exchange for reduced risk.~~

~~One architectural area has had an outsized impact on breach severity over the past decade: identity and access management. Strong IAM practices, including stricter authorization, geographic restrictions, and behavioral monitoring, have materially reduced the scope of major breaches. These controls do more than limit access. They generate valuable signals that enable security operations teams to detect anomalies, investigate suspicious behavior, and trigger additional authentication when risk increases. While IAM was initially adopted to control access, its true value has been in the intelligence it provides. That intelligence has become essential as attacks grow more persistent and adaptive.~~

~~The OCR data reflects these realities. As breaches have increasingly originated from servers and email systems, organizations that underestimated the risk concentrated in these platforms have faced the most severe consequences. Centralization without discipline has proven to be one of the costliest decisions of the past decade.~~

Patient Exposure by Location: Where the Risk Actually Lives



Patient Exposure per Location	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Desktop Computer	303,209	119,479	643,572	485,501	338,341	475,411	248,091	86,793	627,750	302,942	269,386
Electronic Medical Record	3,583,153	459,723	277,115	195,435	535,134	377,781	576,761	6,350,394	1,183,633	222,100	1,155,600
Email	674,043	1,064,621	876,712	3,863,485	5,622,952	13,184,483	7,720,126	5,781,800	2,934,123	3,567,258	2,188,504
Laptop	524,974	818,765	171,157	120,274	223,695	695,420	66,005	116,939	34,269	49,009	89,733
Network Server	110,469,715	13,338,738	3,060,970	8,249,829	36,656,366	20,948,127	52,628,703	49,774,522	179,006,989	285,469,051	40,384,403
Other	646,791	4,302,451	992,332	2,112,079	2,150,452	841,206	486,345	430,493	664,006	54,182	159,567
Other Portable Electronic Device	337,010	36,023	851,970	519,789	1,397,263	149,199	100,847	266,529	11,707	22,297	21,231
Paper/Films	363,419	983,847	192,538	1,219,024	217,271	1,097,230	193,514	318,410	147,458	205,377	120,679

~~When it comes to breach impact, how an incident occurs is often less important than where the data resides. Understanding breach methods matters, but impact is determined by exposure. That exposure is defined by the location of the organization's most critical data assets.~~

~~Every healthcare organization has crown jewels and black swan scenarios. Identifying them establishes the maximum credible impact of a breach. Only after that ceiling is understood can leaders meaningfully reduce risk. In healthcare, these black swan events generally fall within the familiar framework of confidentiality, integrity, and availability. Applying this framework in practice, rather than in theory, forces difficult prioritization~~

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

decisions. Hospitals must ensure availability so patient care can continue even when technology is impaired. Medical records must preserve integrity to support accurate billing and future treatment. Confidentiality must be protected to prevent fraudulent use and downstream patient harm. Knowing where data lives allow organizations to align controls to these priorities, enabling operations to continue and patients to receive care without the cascading consequences of insurance abuse or malpractice exposure.

Executives are often surprised to learn where patient data is actually exposed after an incident. Some of the most impactful breaches do not originate from sophisticated attacks but from data left in publicly accessible locations. SharePoint repositories, SFTP sites, and source code repositories have all been used to store sensitive information or credentials that were never meant to be exposed. These are not exotic failures. They are basic lapses in data governance that become catastrophic when discovered by the wrong audience.

Data concentration magnifies these consequences. Centralized repositories such as data lakes offer significant operational value when properly secured, but they also represent a single, high-impact point of failure. The regulatory, legal, and reputational consequences of a breach grow dramatically when all sensitive data resides in one location. The analogy is familiar. Pirates never kept all their treasure on a single ship because they understood that when it was lost, it would be lost entirely. Healthcare organizations must apply the same discipline. Data that no longer serves an active business purpose should not remain in operational environments. Moving it to cold storage, separate cloud providers, or certified offline facilities reduces exposure without sacrificing retention requirements.

Data sprawl further compounds the problem. In breach response, one investigative path often leads to many others, consuming time and resources that organizations cannot afford. Without clear boundaries, forensic investigations can expand unnecessarily. Business email compromise illustrates this challenge well. Logs may show hundreds of emails being opened, but forensic analysis can often distinguish between automated activity and actual data access by examining timing and header attributes. Understanding these nuances allows investigators to narrow scope intelligently instead of assuming worst-case exposure. Organizations that lack this expertise allow data sprawl to dictate responses, extending investigations and increasing costs. Having certified forensic expertise in place before an incident enables faster resolution, better coordination with insurers and law enforcement, and more defensible outcomes.

If there is one mindset shift leaders must make, it is this. Not all data is good data. Retaining information without a clear purpose increases risk without delivering value. Holding onto data "just in case" mirrors the habit of keeping obsolete equipment that no longer fits current needs. Over time, it becomes clutter. In healthcare, that clutter carries

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

consequences. Understanding why data exists, where it lives, and when it should be retired is one of the most effective ways to reduce breach impact across the organization.

The OCR data reflects this truth. Over the past decade, the largest patient exposures have consistently occurred where data was most concentrated and least governed. Location, not method, has defined the damage.

Why I Recommend What I Do: From Patterns to Practice

Over the past decade, cybersecurity has slowly made its way into the boardroom. That visibility is an important step forward, but visibility alone is not enough. The most common failure I see before a breach is not a lack of reporting. It is reporting that does not support decision-making.

Board-level dashboards often focus on metrics that make security teams appear successful instead of metrics that help leaders decide where to invest. Effective reporting should not communicate inevitability or fear. It should communicate humility and clarity. No organization is perfect. The role of security leadership is to explain where risk exists, why it matters to the business, and where expert judgment recommends investment. That includes vendor contracting risk, environment cleanup and segmentation, and the preparedness of relational response playbooks. Boards do not need to be trained as practitioners, but they do need to understand, from trusted advisors, where risk is concentrated and what action is required.

After an incident, the most common statement I hear from leadership is, "I wish we had done a risk assessment sooner." Breach reviews frequently surface technology and process gaps leaders never fully understood as business risks. These gaps may have been mentioned before, but without a comprehensive, prioritized view, they were not actionable. Leaders do not respond well to piecemeal gap analysis delivered in isolation. That approach creates fatigue and undermines credibility. A structured, enterprise risk assessment conducted by an unbiased external party allows leaders to see all gaps together, understand relative priority, and approve remediation intentionally. Once that baseline is set, progress can be tracked and accountability becomes clear. This continuous cycle of planning, execution, review, and adjustment allows organizations to mature without panic-driven decision-making.

Vendor-related breaches introduce a different set of emotional and operational challenges. As healthcare increasingly relies on cloud providers and third parties, the

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

operational impact of vendor incidents has grown significantly. Emotionally, vendor breaches are often met with resignation. Leaders may frame them as outside their control and defer responsibility to legal teams. Internally caused incidents, by contrast, trigger deeper scrutiny and discomfort. Decisions about accepted risk, delayed investment, or incomplete reporting come under pressure. These moments demand calm leadership that is deliberate, attentive, and disciplined. Without clear playbooks, patience can be misread as inaction. Well-designed response processes allow incidents to progress effectively without unnecessary escalation or confusion.

Resistance to board-level visibility remains common. I recall a board member once stating that they did not need to understand cyber risk and only wanted to know when something went wrong. That perspective was not unique, and it reflected how security was viewed as an insurance policy rather than an operational dependency. Progress did not come from confrontation. It came incrementally. By partnering with compliance and legal leaders, securing small opportunities to speak, and bringing forward the collective voice of business risk owners, the conversation slowly shifted. Over time, boards began asking better questions. Engagement grew. Cyber risk was no longer an abstract cost center but a recognized factor in operational resilience.

At the core of my advisory approach is this principle. Always be ready to speak, be prepared to speak at every level of the organization, and remain quick to listen and deliberate in response. Experience has shown me that the most effective security leaders are not the loudest voices in the room. They are the ones whose judgment earns trust before an incident ever occurs.

Closing Thought

A decade of healthcare breach data does not point to a failure of intent. It points to a failure of alignment. Over the past ten years, organizations have invested in tools, compliance efforts, and response capabilities, yet breaches have continued to grow in scale and consequence. The data makes one thing clear. Risk in healthcare is no longer defined by how often incidents occur, but by how unprepared leadership is for their impact.

Every exposed record represents a patient who trusted the healthcare system with something deeply personal. That trust is not protected by certifications, dashboards, or contracts alone. It is protected by leaders who understand where risk lives, who make deliberate decisions before an incident occurs, and who are willing to act on uncomfortable truths.

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

The organizations that will navigate the next decade successfully are not those that believe breaches can be eliminated entirely. They are the ones that recognize inevitability without surrendering to it. They invest during periods of calm, define accountability before pressure mounts, and prepare their people to respond with clarity instead of confusion.

Cybersecurity in healthcare is no longer about preventing embarrassment or regulatory scrutiny. It is about safeguarding care, continuity, and dignity. The data has already delivered its warning. What matters now is how leadership chooses to respond.

About the Author

Jericho Simmons is a healthcare cybersecurity executive with more

than a decade of experience leading security strategy, operations, and risk programs across complex healthcare environments. His leadership approach is grounded in clarity, stewardship, and a deep commitment to protecting what sustains patient care and organizational mission.

Jericho specializes in aligning cybersecurity with clinical operations, revenue cycle performance, and executive decision-making. Through Shield and Seed, he partners with healthcare leaders to build purpose-driven, business-aligned security strategies that strengthen resilience, reduce risk, and support long-term organizational health.

Jericho Simmons

Technology Executive

Jericho.simmons@shieldandseed.net

www.shieldandseed.net

SHIELD & Seed LLC

SECURE THE PRESENT. SOW THE FUTURE.

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf