keena
Healthcare Technology

WHITE PAPER

Shrinking the Attack Surface: **Reducing Healthcare Cyber Risk by Retiring Legacy EHRs and Over-Retained Data**

keenahealth.com | 315.707.7843

WHITE PAPER

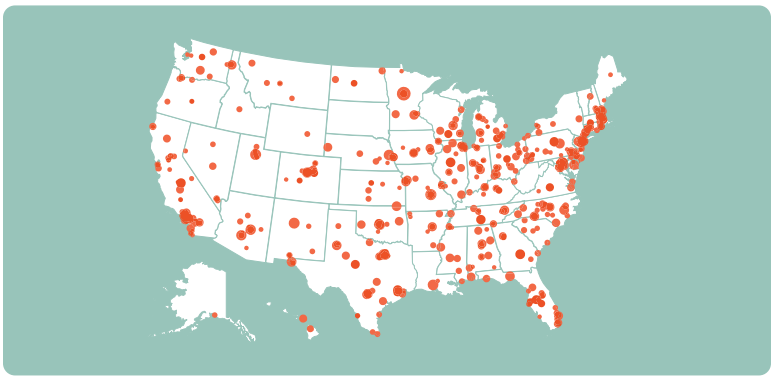
Shrinking the Attack Surface: **Reducing Healthcare Cyber Risk by Retiring Legacy EHRs and Over-Retained Data**

Introduction

Healthcare organizations face an escalating and costly cybersecurity crisis. In 2024, a record 289 million individuals had their protected health information (PHI) exposed or impermissibly disclosed—a figure that surpassed the entire U.S. population. Breaches are no longer isolated incidents; they are systemic failures rooted in predictable, addressable vulnerabilities.

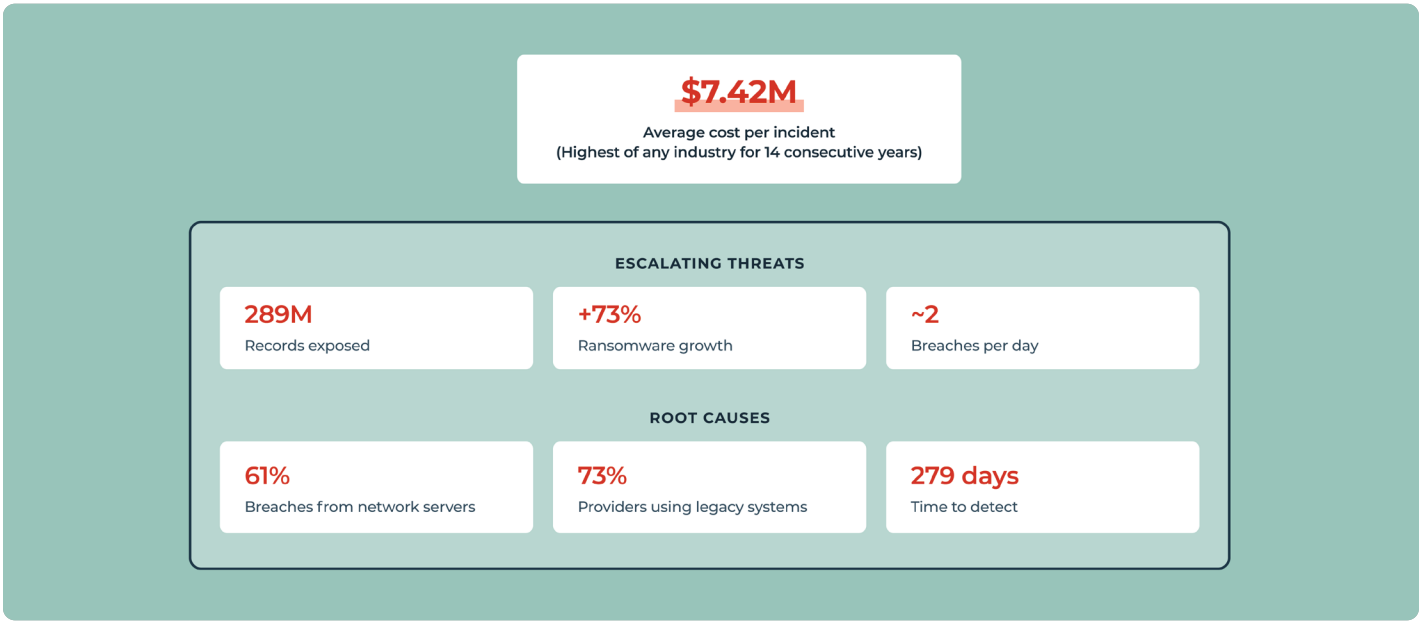
Chief among these vulnerabilities are legacy electronic health record (EHR) systems and the practice of retaining patient data far beyond legal requirements. Outdated platforms lack modern security controls, cannot be effectively patched, and are actively targeted by ransomware groups. Over-retained data magnifies breach impact: when attackers penetrate a legacy system, they can often access everything stored within it, including records that should have been destroyed years earlier.

This paper examines why minimizing the healthcare attack surface through disciplined data retirement and secure archival is now a foundational risk management requirement—and how KeenaArchive Perform enables organizations to achieve that goal.



Medical Data Breaches in the U.S., 2024
(Source: U.S. Department of Health and Human Services)

TABLE OF CONTENTS



The Threat Landscape: What The Data Shows

The scale of the healthcare cybersecurity problem is substantial and growing. Recent industry data paints a clear picture.

These figures are not anomalies. According to the HIPAA Journal's 2025 Healthcare Data Breach Report, healthcare has consistently led all sectors in both breach frequency and cost, with about two large breaches reported to OCR every day. Network servers—where legacy EHR data often resides—are involved in over 61% of annual breach incidents.

Healthcare IT News' cybersecurity roundup confirms the trend: over the past three years, average breach costs in healthcare have risen toward the $11 million threshold, driven by ransomware, regulatory penalties, and prolonged recovery timelines.

Archiving data into a purpose-built platform eliminates recurring legacy maintenance costs entirely, with most organizations achieving full ROI within 18–24 months.

Key Statistics (2024–2025)

- Healthcare breaches cost an average of $7.42 million per incident—the highest of any industry for 14 consecutive years (IBM Cost of a Data Breach Report, 2025)
- 289 million healthcare records were exposed in 2024, a new annual record (HIPAA Journal, 2025 Healthcare Data Breach Report)
- Healthcare breaches take an average of 279 days to identify and contain—five weeks longer than the cross-industry average (IBM, 2025)
- Ransomware attacks in healthcare increased 73% against United States facilities in recent years (KnowBe4 International Healthcare Report)
- 73% of healthcare providers continue to use medical devices or systems running legacy operating systems (Kaspersky, 2021)

Why Legacy Systems and Over-Retained Data Amplify Risk

Legacy EHRs Are Preferred Targets

Unsupported or end-of-life EHR platforms create significant structural vulnerabilities. Without vendor patching, known flaws remain open, and without modern monitoring and segmentation, attackers can persist and move laterally across networks.

The impact is well documented. Major health systems have experienced multi-hospital shutdowns tied to unpatched legacy environments. According to the HHS Office for Civil Rights, hacking and IT incidents now account for roughly 80% of reported healthcare breaches—up from 4% in 2010. Legacy infrastructure is a consistent driver of this trend.

Over-Retention Expands the Blast Radius

Storing patient data beyond required retention periods offers no clinical value and increases breach impact. When attackers access a legacy EHR, exposure is determined by what exists—not what is needed. Records that should have been destroyed become part of the breach.

HIPAA protections apply equally to deceased patient records, yet these are often overlooked. They accumulate in legacy systems, are rarely accessed (making anomalies harder to detect), and remain exploitable for identity fraud and record manipulation.

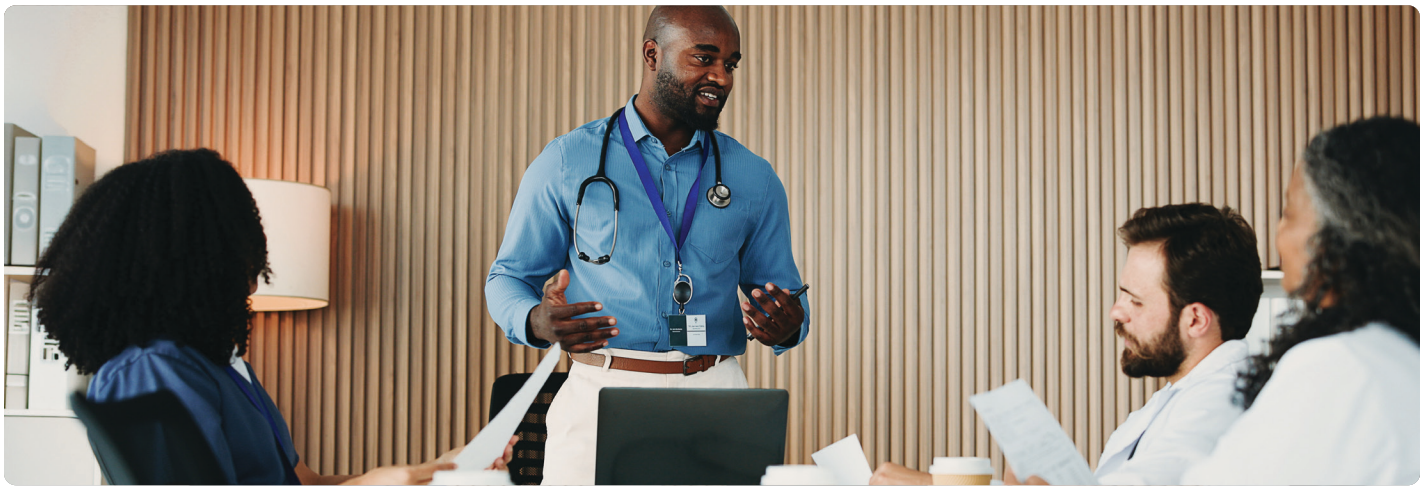
A disciplined retention strategy—enforcing destruction once legal requirements expire—directly reduces breach scope.

The Attack Surface Is Wider Than Most Organizations Realize

Healthcare organizations rely on nearly 1,000 applications on average. Each system storing or accessing PHI expands the attack surface.

Legacy EHRs maintained for occasional "view access" are common unmanaged risks: connected to the network, lightly monitored, and often excluded from rigorous security review.

Retiring these systems and migrating only legally required records into a secure archive reduces the number of PHI-containing systems—and the opportunities for exploitation.



The Compliance Dimension: Deceased Patient Records and Defensible Destruction

One of the most persistently overlooked risk categories in healthcare data governance is the deceased patient record. These records:

- Remain fully protected under HIPAA for a period after death (variable by state law, but commonly 50 years from the date of the record or 3 years after death—whichever is longer)
- Are rarely subject to proactive retention review in legacy EHR environments
- Are frequently targeted by identity theft schemes, as fraudsters exploit the time between death and notification to financial and insurance systems
- When breached, may go undetected longer due to lower access frequency, increasing the window of unauthorized exposure

Organizations with defensible destruction programs—those that can document when records were destroyed, under what authority, and in accordance with what retention schedule—are significantly better positioned in regulatory investigations and litigation.

The OCR's 2025 enforcement focus on HIPAA risk analysis compliance underscores that organizations without documented, systematic retention and destruction practices face elevated penalty exposure.

THE STRATEGIC PATH FORWARD: SECURE ARCHIVAL AS A RISK REDUCTION TOOL

Addressing legacy EHR risk does not require permanently losing access to historical patient data. Purpose-built clinical archives allow organizations to fully retire legacy platforms while preserving access to historical records in a secure, compliant environment.

Risk Reduction Through Archival: Key Outcomes

- Legacy "view-only" EHR systems are fully decommissioned, eliminating their attack surface
- Only legally required records are migrated—not the entire legacy dataset
- Deceased patient records and over-retained data are defensibly destroyed on a defined schedule
- Historical PHI remains accessible to authorized staff in a monitored, auditable environment
- The organization's overall threat footprint, measured in active systems containing PHI, decreases substantially

This approach aligns directly with the cybersecurity principle of minimizing attack surface: the fewer systems that store PHI, and the less data stored beyond its useful life, the less an attacker can access even in a worst-case breach scenario.

The Financial Case: Archiving Costs Less Than Keeping the Lights On

A common objection to retiring legacy EHR systems is cost—but the data consistently shows that the cost of inaction exceeds the cost of archiving. Legacy systems kept running in "read-only" or "view-only" mode continue to generate real, ongoing expenses across multiple categories.

These costs compound over time. State and federal medical record retention periods commonly run 7–25 years depending on record type and jurisdiction. An organization paying even $50,000 per year to maintain a single legacy platform across a 15-year retention window is spending $750,000—for read-only access to data that could be migrated to a secure archive at a fraction of that cost.

The financial calculus is straightforward: archiving eliminates vendor licensing fees, reduces hardware and IT overhead, shrinks the cybersecurity attack surface, and lowers breach liability—all simultaneously. The upfront cost of migration is a one-time investment. The cost of not migrating recurs every year.

Healthcare IT News' cybersecurity roundup confirms the trend: over the past three years, average breach costs in healthcare have risen toward the $11 million threshold, driven by ransomware, regulatory penalties, and prolonged recovery timelines.

THE TRUE COST OF A LEGACY EHR IN "VIEW-ONLY" MODE

Vendor maintenance fees: $4,000 to $8,000 per system per year in basic support alone, even with no active use (Healthcare IT Research, 2025)

Health-system scale: $1.5M–$3M annually for maintenance and support on major EHR platforms

Annual maintenance typically equals 15–20% of the original implementation cost—every year, indefinitely

Additional costs: hardware/server upkeep, IT staff time, security audits, and compliance monitoring

ROI on archiving: most organizations achieve full return on investment within 18–24 months of decommissioning

How KeenaArchive Perform Addresses These Risks

KeenaArchive Perform is purpose-built for EHR transitions and long-term healthcare data governance. It enables organizations to address legacy EHR cyber risk directly by providing:

- **Clinical Data Migration:** Standardized clinical data conversion that preserves the integrity and accessibility of historical patient records across all major EHR formats
- **Retention Governance:** Configurable retention rules aligned to applicable federal and state law, supporting systematic identification of records eligible for destruction
- **Defensible Destruction:** Documented, auditable destruction workflows that satisfy defensible destruction requirements under HIPAA and state regulations
- **Security Architecture:** Role-based access controls, encryption at rest and in transit, and comprehensive audit logging—security controls legacy EHR platforms typically cannot provide
- **Legacy Retirement:** Support for full legacy EHR decommissioning, eliminating ongoing licensing, maintenance, and security exposure from end-of-life platforms

The result is a materially smaller attack surface, lower operational and regulatory risk, and a data governance posture built for the current threat environment.

Conclusion

The cybersecurity data is unambiguous: healthcare is the most targeted and most expensive sector for data breaches, and legacy systems combined with over-retained data are consistently among the most exploited vulnerabilities. Continuing to maintain legacy EHR platforms for occasional access—while storing decades of patient records within them—is not a defensible risk management strategy in today's environment.

Reducing healthcare cyber risk requires deliberate action: retiring legacy systems, enforcing retention discipline, and migrating only what is legally required into a secure, purpose-built archive. KeenaArchive Perform exists to make that transition achievable—without sacrificing continuity of care or compliance standing.

For organizations ready to align their archival strategy with modern security and data governance requirements, Keena Healthcare is ready to help.

315.707.7843
sales@keenahealth.com

Sources & References
This white paper draws on the following third-party sources:

HIPAA Journal — Healthcare Data Breach Reports & Statistics (2025)

IBM — Cost of a Healthcare Data Breach Report (2025)

Healthcare IT News — Cybersecurity Roundup (U.S. Healthcare)

HHS Office for Civil Rights — Healthcare Data Breach Portal

KnowBe4 — International Healthcare Cybersecurity Report

Kaspersky / Healthcare Brew — Legacy OS Usage in Medical Devices Survey (2021)

Healthcare IT Research (TopFlight Apps, VozoHealth, Taction Software) — EHR Cost & Maintenance Guides (2025–2026)