Whitepaper

From Vulnerable Application Estates to Resilient Healthcare Operations

Why AI-Enabled Application Lifecycle Modernization Is Now a Must

Author

Sharath Dudala

Executive Summary

Today, healthcare providers do not simply face a technology upgrade problem; they also face portfolio risk. Healthcare institutions experience years of growth, acquisitions, and regulatory changes while operating on piecemeal solutions. On top of that, aging infrastructure, unsupported software versions, brittle systems integration, decentralized app management, and increasing cyber risks make operations much more complex. In this environment, most providers manage between 400 and 1,000 applications, with larger institutions handling even more[1]. Simultaneously, hospitals continue to allocate substantial budgets to technology support, with the average IT spend around $9.2 million, serving approximately 4,660 facilities[2]. Yet much of this spending sustains complexity rather than reducing it.

In healthcare, the stakes extend well beyond IT. A single application failure has a ripple effect on patient access, referrals, scheduling, laboratories, radiology, clinical charting, claims management, billing, procurement, supply chain, and reporting. Recent cyberattacks on Change Healthcare highlight these criticalities and underscore IT's impact on the care continuum. At the same time, healthcare remains the sector with the highest average cost of a data breach, reaching nearly $9.77 million in 2024[3]. These realities demand a fundamentally different approach.

This whitepaper details how a systematic and AI-driven modernization approach can mitigate cyber risks, streamline their application portfolios, and safeguard continuity of care while steering clients toward a more resilient future.

Table of Contents

Estate Risk Management:
The Real Problem with Software in Healthcare

The crux of the matter: not many organizations lack solutions that require significant upgrades. On the contrary, institutions lack a comprehensive strategy to manage their entire application lifecycle. In practice, healthcare systems build up over time across multiple domains, such as inpatient, outpatient, specialist, diagnostic, and administrative.

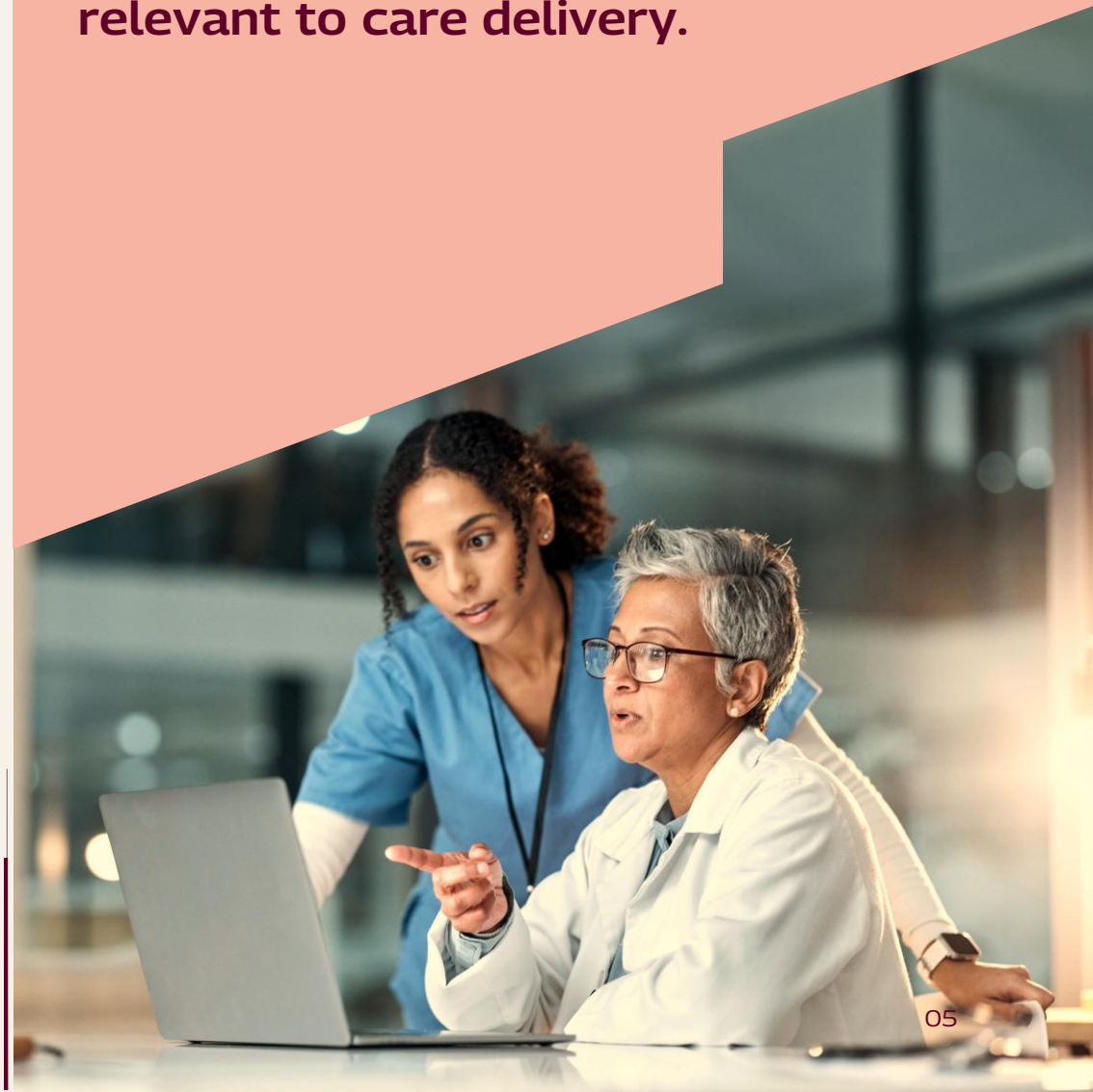
Typically, a single organization ends up with separate applications for each function, such as patient access, bed management, operating room bookings, lab procedures, radiology image storage, pharmacy management, quality assurance, insurance claims processing, contract management, workforce management, remote patient monitoring, and analytics. Most of these applications integrate through interfaces, batch jobs, shared infrastructure, identity management, and reporting. However, the real issue is that some of these applications age differently from others.

To illustrate further, an organization may have mission-critical applications with no documentation, core operational applications that no longer function in the current technical environment, applications with overlapping features, and applications that remain functional due to tight integration with departments' processes. These irregularities in the application estate hinder collective modernization efforts.

This problem of aging IT infrastructure is well known in healthcare, where the cybersecurity team is concerned about out-of-support products; the infrastructure team tries to maintain legacy systems; the application development team depends on third-party software vendors, while the business owner refuses to disrupt critical workflows, and upgrades are made only when risks are high.

AI can significantly help in this stage. Leveraging it to review configuration records, architecture diagrams, support tickets, vulnerability assessments, and integration artifacts enables teams to address emerging risks. This AI intervention provides a stronger foundation for modernization and makes the process less reactive.

The healthcare industry needs to evolve from its vulnerable, inefficient, and costly application environment to one that is far more secure, rationalized, resilient, and relevant to care delivery.



Why Healthcare Demands a Unique Approach to Application Modernization

Unlike other industries, application modernization in healthcare requires special attention, especially because any application issues can translate into critical service provisioning problems. For instance, a patient access solution may be viewed as an administrative tool, but the application outage will inevitably delay patient registration, authorization, and scheduling. Similarly, a laboratory or radiology solution might be considered a department-specific tool, but a failure in its application will lead to interruptions in order processing, results delivery, and physician decision-making. Finally, even though a revenue cycle management solution might not be used directly in patient care, an outage in the application will impact cash flow, claim submission, and patient eligibility verification.

AI significantly strengthens application modernization efforts. By analyzing interface logs, API traffic, change records, support tickets, and configuration data, it uncovers hidden interdependencies far earlier than manual reviews. This gained insight proves especially valuable when organizations lack a current, complete map of their applications' dependencies.

In healthcare, an everyday infrastructure or application update impacts patient flow, diagnostic capabilities, payment processes, and operational stability all at the same time.

A Vision of Future State:
Secure, Rationalized, and Resilient Operations

For healthcare executives, the goal is not limited to upgrading applications. What they truly seek is an IT environment where every application is fully supported, cyber risks are minimized, legacy systems are eliminated, and modernization never disrupts patient care.

This envisioned future state portfolio is secure, with applications upgraded to supported, defensible versions that meet the healthcare industry's growing cybersecurity demands. It is rationalized by classifying each application as an upgrade, retention, consolidation, replacement, or retirement. It is resilient, with interdependencies established, rollback strategies defined, and changes scheduled in alignment with operations. It's defensible, with better ownership, testing, documentation, and handoffs. And more importantly, it's smart, with AI serving as an ongoing assessment and prioritization tool for testing and stabilization, rather than just an add-on.

A Better Modernization Model:
Each Upgrade as a Strategic Decision

Every upgrade should begin with a single, fundamental question: Should this application even exist in the future-state portfolio?

This shift in perspective creates an opportunity for risk mitigation, supportability improvements, licensing optimization, and overall portfolio consolidation. For healthcare institutions, it simplifies retiring duplicate applications across multiple facilities; decommissioning legacy department-level applications while considering enterprise functionality; and eliminating older platforms where the cost-to-support ratio is no longer reasonable.

AI intelligently transforms this decisioning process by categorizing applications based on technical viability, business importance, incident frequency, supportability, vulnerability, usage, and integration complexity. Such a strategic AI-enabled approach ensures that only the right applications survive, setting the foundation for true modernization success.

The Modernization Leap: *A Four-motion Approach*

A successful application modernization initiative in healthcare follows a disciplined, four-motion framework that connects discovery to lasting value.

Motion	Purpose
Portfolio diagnosis	Validates what applications exist, who owns them, what they support, what they depend on, and how exposed they are.
Disposition-led decisioning	Determines whether the right move is to upgrade, replace, consolidate, or retire.
Controlled execution	Coordinates architecture, infrastructure, security, interoperability, testing, deployment readiness, and support transition.
Value capture	Updates the portfolio to reduce technical debt, improve supportability, and lower long-term risk.

This structured approach benefits significantly from AI at every stage. AI accelerates discovery, maps complex dependencies, identifies probable points of failure, generates test cases, and supports hyper-care through intelligent incident clustering and root-cause recommendations.

The Final Note

Despite rising IT investments, many healthcare providers remain trapped in maintaining outdated, vulnerable applications that consume significant resources and expose them to serious cyber threats. Continuing to upgrade isolated legacy systems or applications only deepens this complexity. A far more effective path exists: the proposed strategic, portfolio-wide modernization approach, grounded in disciplined portfolio management and cybersecurity principles. Powered by AI, this method equips healthcare institutions to systematically modernize their entire application estate, reducing cyber risk, eliminating technical debt, lowering long-term costs, and strengthening operational resilience, all while safeguarding the continuity and quality of patient care.

For healthcare leaders today, application modernization is no longer optional; it is a strategic imperative.

End Notes

1. College of Healthcare Information Management Executives. (2026, March 5). Application rationalization in healthcare: Why CIOs can't afford to wait. CHIME Central. https://chimecentral.org/chime/resource-post/application-rationalization-in-healthcare-why-cios-cant-afford-to-wait

2. Definitive Healthcare. (2024, July 24). Top 10 hospitals with the highest IT expenses. https://www.definitivehc.com/resources/healthcare-insights/25-hospitals-highest-operating-budget

3. International Business Machines Corporation. (2024). Cost of a data breach report, 2024. https://www.ibm.com/reports/data-breach

Sharath
Dudala

Program Manager,
Healthcare Provider,
Tech Mahindra

About the Author

With nearly two decades of experience supporting healthcare providers, Sharath helps large health systems in the US by combining engineering excellence, delivery ownership, and talent management. He previously served as HLS Practice Head and Solutions Architect, leading large and complex engagements. Sharath has co-founded two tech startups in blockchain and medical IoT and holds a patent for improving key processes within the US healthcare system. He holds a Master's degree in Computer Science.

About **Tech Mahindra**

Tech Mahindra (NSE: TECHM) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 147,000+ professionals across 90+ countries helping 1100+ clients, Tech Mahindra provides a full spectrum of services including consulting, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognizes global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

*Figures as per Q4, FY 26.

www.techmahindra.com
www.linkedin.com/company/tech-mahindra
www.x.com/Tech_Mahindra