Analyst Connection, sponsored by:
Everpure

Modernizing Healthcare Data Infrastructure to Enable AI, Resilience, and Cloud Agility

Questions posed by:

Everpure

Answers by:

Mutaz Shegewi
Senior Research Director
Worldwide Healthcare AI, Platforms, and Technologies

Published:
July 2026

Healthcare organizations must modernize data infrastructure now to support AI at scale, withstand evolving cyberthreats, and operate coherently across hybrid cloud environments, without disrupting 24 x 7 clinical operations.

Q. Why is healthcare data infrastructure modernization an urgent priority right now?

EHR platforms have become the operational backbone of care delivery across every care setting. Performance, availability, and data continuity are no longer purely IT concerns; they are clinical requirements. As health systems expand across ambulatory, specialty, and post-acute environments, the scale and distribution of EHR data have grown far beyond what legacy storage architectures were designed to handle.

The workload profile of healthcare data infrastructure is fundamentally changing. Clinical AI applications, including ambient documentation, clinical decision support, real-time imaging analytics, and agentic workflow automation, impose continuous, high-throughput data demands on the same infrastructure that must also support transactional EHR operations. Legacy architectures optimized for sequential, batch-oriented workloads cannot handle this concurrency without performance degradation.

IDC's *U.S. Healthcare Provider IT Survey* confirms the investment signal is strong and forward-looking: nearly half of respondents ranked modernizing IT infrastructure among their most important IT goals in 2026, close to three in five respondents reported active investment in infrastructure modernization, and an equally large share plan to sustain that investment. Among organizations expecting their IT budgets to grow, IT operations and data infrastructure ranked as the single spending category most frequently targeted for increased investment. Merger and acquisition activity, multisite growth, and regulatory mandates on data availability and protection are further amplifying the urgency. Organizations that delay infrastructure modernization are not simply deferring a capital decision. They are constraining their capacity to adopt AI tools, meet evolving compliance requirements, and maintain competitive care delivery at scale.

Q. What measurable business and clinical value does a modern data infrastructure foundation deliver?

The business case for infrastructure modernization is not one argument; it is four converging pressures: operational efficiency, clinical performance, financial predictability, and risk reduction. Organizations that make the case along a single dimension typically lose; those that secure budget make the argument across all four, showing how a single architecture decision moves the needle on each.

On the clinical operations side, EHR application performance directly determines clinician productivity. System latency increases documentation time and disrupts workflow adoption, adding to the administrative burden that clinicians consistently cite as a driver of burnout. Health systems that move to high-performance, low-latency storage architectures can expect improvements in EHR response times, reduced maintenance windows, and fewer unplanned outages that interrupt care delivery.

Traditional procurement comparisons are structurally incomplete. Organizations cycling through forklift upgrades absorb costs that never appear in an RFP response: migration planning hours, clinical team downtime, and AI initiatives that get deprioritized. Architectures that support continuous, nondisruptive upgrades do not simply reduce that overhead; they reclaim the organizational capacity that would otherwise be spent servicing infrastructure debt.

Infrastructure modernization also enables the execution of AI programs. Health systems building clinical AI capabilities on aging storage foundations consistently encounter architectural bottlenecks when scaling inference workloads. Proactive modernization creates the data layer AI applications require without downstream redesign cycles. IDC's *U.S. Healthcare Provider IT Survey* confirms the scale: More than half of healthcare provider organizations expect generative AI and agentic AI investment to increase in 2026, demanding infrastructure capable of supporting concurrent inference at clinical speed and scale.

Q. How are healthcare organizations approaching hybrid cloud strategy for EHR and clinical workloads?

Hybrid cloud is no longer a direction of travel; it is the installed reality. IDC's *Industry AI and Cloud Path Survey* found that more than 60% of healthcare organizations are already deploying hybrid cloud across one or more business units. The prevailing pattern places latency-sensitive, regulated clinical workloads, including production EHR databases and real-time clinical decision support, on premises while leveraging public cloud for analytics pipelines, disaster recovery, and secondary data processing.

This model reflects a practical constraint: EHR platforms impose performance and configuration requirements that public cloud environments cannot consistently satisfy at the latency thresholds clinical operations demand. Health systems that have attempted a full cloud migration of production EHR workloads frequently encounter performance variability and data residency issues that require architectural remediation.

The imperative is unified management across both environments. Separate toolsets with distinct governance models and policy frameworks create more than operational overhead; in healthcare, fragmented infrastructure is a compliance liability. HIPAA audit obligations, chain-of-custody requirements, and incident reporting mandates apply wherever patient data resides.

Health systems that cannot demonstrate consistent policy enforcement across their hybrid environment face a compliance surface that regulators are increasingly equipped to scrutinize.

Consumption-based infrastructure models resolve a long-standing tension: on-premises preserved performance consistency, but at the cost of capital expenditure cycles and technology refresh risk. As-a-service infrastructure delivered on premises changes the economic model without the latency variability that has made full cloud migration impractical for production EHR environments. The trade-off shifts from capital expenditure cycles to contractual commitments, which organizations should model carefully in exchange for more predictable per-unit economics alongside the performance and governance characteristics that clinical operations require.

Q. What does a mature cyber-resilience posture look like for healthcare provider data infrastructure?

A health system that cannot access its EHR cannot deliver care safely. That dependency makes healthcare a persistently attractive ransomware target: Disruption is immediate, clinically consequential, and measurable in hours. The financial consequences compound long after the initial incident: clinical downtime, care diversion, regulatory scrutiny, and reputational damage that persists well beyond recovery. IDC's *U.S. Healthcare Provider IT Survey* confirms the investment posture reflects this urgency: More than 4 in 10 respondents expect security budgets to increase in 2026, with AI-powered threat detection and identity and access management among the areas receiving the largest incremental investment.

A mature cyber-resilience posture is distinct from a cybersecurity posture. Cybersecurity focuses on prevention and perimeter defense. Cyber-resilience assumes breaches will occur and builds capabilities to detect threats early, contain the blast radius, and restore operations rapidly with minimal data loss.

For data infrastructure specifically, maturity means immutable, air-gap-capable snapshot architectures; isolation capabilities that can quarantine affected systems; and recovery time objectives for EHR databases measured in minutes, not hours. The EHR is the highest-value target because it is operationally indispensable; recovery procedures must be tested under realistic conditions, not just documented.

A critical gap is the distance between a recovery plan on paper and one that executes under active incident conditions. Organizations should validate that their infrastructure supports automated anomaly detection, policy-driven quarantine, and operationally tested clean-restore workflows. Clinical operations leadership must be integrated into cyber-resilience planning, as recovery prioritization decisions carry direct patient-care implications.

Q. What criteria should healthcare IT leaders apply when evaluating enterprise data infrastructure partners?

The enterprise storage market has no shortage of vendors claiming healthcare expertise. The relevant question is which have built their architecture and professional services around clinical demands. The cost of getting this wrong rarely shows up in procurement, surfacing as performance remediation, unplanned upgrades, and rearchitecting when a clinical AI program hits an infrastructure ceiling.

EHR workload expertise is foundational. Organizations should distinguish vendors with general enterprise capability from those with documented, validated guidance for their specific EHR platform. For platforms with precise sizing and configuration requirements like Epic, this distinction is consequential. Epic operates under precise sizing and configuration requirements, and the gap between a validated vendor and one without shows directly in application performance and upgrade outcomes.

Nondisruptive upgrade architecture is nonnegotiable in a 24 x 7 clinical environment. Forklift upgrades pose a risk that most health systems cannot absorb. Evaluate whether the platform supports continuous, in-place modernization without downtime.

Hybrid cloud integration should be evaluated as a management architecture question, not a connectivity one: unified governance, data portability, and coherent policy enforcement across on premises and cloud. Cyber-resilience should extend beyond snapshots to detection, immutability enforcement, and tested healthcare-specific recovery runbooks. AI readiness, the capacity to support model training, inference, and analytics without architectural redesign, is increasingly core as clinical programs scale.

Domain depth, including a verified healthcare reference base and professional services with EHR expertise, is a differentiator that general enterprise credentials do not substitute for. IDC research confirms that healthcare organizations consistently rank data security, trust for mission-critical workloads, and industry-specific understanding among their top criteria when evaluating infrastructure providers.

About the IDC analyst

Mutaz Shegewi
Senior Research Director

Mutaz Shegewi leads the Worldwide Healthcare Provider Research Practice at IDC Health Insights, overseeing research on AI, platforms, cloud, infrastructure, services, and security for the industry vertical. He advises healthcare provider organizations and global technology suppliers on modernizing legacy environments, accelerating AI adoption, strengthening operational resilience, and accelerating the shift toward more digitally native, data-driven, and consumer-centric care models.

More about Mutaz Shegewi.

Message from the sponsor

Everpure provides an efficient, reliable, and secure data management and storage platform for the healthcare industry to accelerate clinical application performance and AI-initiative readiness and adoption at scale while safeguarding patient data. Our platform delivers cost savings for all of your data needs to improve care outcomes, maximize operational efficiency, and drive clinical innovation.

Learn how Everpure can help your organization scale at: https://www.everpuredata.com/solutions/industries/healthcare/providers.html.

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
One Beacon Street, Suite 33100, MA 02108, USA
T +1 508 872 8200

blogs.idc.com | LinkedIn @IDC | www.idc.com

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA