

As medical imaging data explodes and risk intensifies, healthcare leaders are turning to cloud-first infrastructure to safeguard patient data, contain costs, and automate compliance across mission-critical diagnostic and operational workflows.

Data Under Pressure: Navigating Medical Imaging Growth, Cyber-Risk, and Compliance Through Smarter Infrastructure

May 2025

Written by: Mutaz Shegawi, Senior Research Director, Worldwide Healthcare Provider Platforms and Technologies

Introduction

The healthcare IT landscape is transforming rapidly, with medical imaging and radiology becoming pivotal data domains at the heart of this evolution. From high-resolution diagnostic scans to AI-enhanced imaging workflows, these areas generate some of healthcare's largest and most complex data sets. This swift data proliferation poses not only a technical challenge but also a strategic pressure point that directly intersects with three organizational imperatives: safeguarding patient data, managing infrastructure costs, and ensuring regulatory compliance.

Healthcare provider organizations recognize that data is no longer a passive byproduct of care; it has become a vital asset that underpins everything from clinical decision-making and patient engagement to operations and revenue cycle optimization. The ability to manage and derive value from large volumes of imaging data is quickly becoming a competitive differentiator, particularly as clinical workflows evolve toward precision diagnostics, real-time collaboration, and AI-assisted interpretations. As imaging moves from a departmental function to an enterprisewide service, the underlying infrastructure must change, enabling unified access, intelligent archiving, and seamless scalability.

This shift in thinking is driving providers to realign their business and IT strategies toward more resilient, scalable, and intelligent data infrastructure. According to IDC's *U.S. Healthcare Provider IT Survey*, over one-third of providers (36.5%) cite adopting AI as a top business priority, and nearly half (49.2%) are modernizing their IT infrastructure in 2025. Furthermore, 32.6% expect to increase their investments in cloud computing by 2025 (see Figure 1).

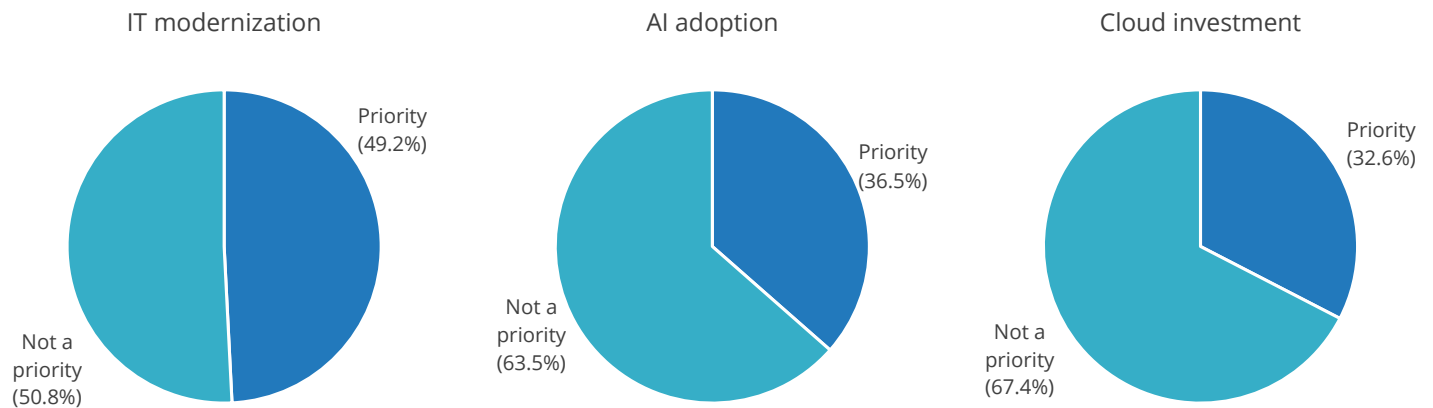
AT A GLANCE

KEY STATS

- » 49.2% of U.S. healthcare providers are modernizing IT infrastructure in 2025.
- » 35.5% of increased IT spending is on privacy, security, and data protection.

KEY TAKEAWAYS

- » Cybersecurity, cost control, and compliance are converging imperatives.
- » Cloud-based storage platforms offer a high-value pathway to modernize infrastructure while supporting imaging scalability, AI adoption, and disaster recovery needs.

FIGURE 1: **Comparison of Healthcare Provider IT Priorities**

Source: IDC's U.S. Healthcare Provider IT Survey, 2024

These investments underscore a systemic change in the role of IT from a traditional cost center focused on maintenance and uptime to a mission-critical function driving patient-centric innovation, enabling virtual care, and powering AI-augmented clinical workflows.

This trend toward modernization is particularly evident in medical imaging as cloud-based, AI-enhanced enterprise strategies become widespread. Healthcare organizations face growing pressure to manage a surge in imaging volume, resolution, and a variety of modalities while ensuring that data remains secure, accessible, and compliant with long-term retention requirements. Imaging data sets, typically stored in DICOM format and requiring high-fidelity preservation, pose challenges related to volume, complexity, and longevity. Traditional storage architectures characterized by siloed, on-premises systems struggle to meet these demands, leading to an increased risk of bottlenecks, performance degradation, and compliance gaps. Adding urgency to the situation is the rapidly evolving threat landscape. Healthcare remains a primary target for cybercriminals, with ransomware and data exfiltration attacks increasing in frequency and sophistication. Medical imaging systems and archives are becoming more vulnerable due to their high value, broad accessibility, and critical role in care delivery. IDC data indicates that 32.2% of healthcare providers are prioritizing IT security spending on identity and access management, while 29.6% are investing in data loss prevention technologies. In addition, 24.3% are allocating budgets toward HIPAA-specific compliance tools, underscoring the significance of security not only for data protection but also for operational continuity and avoiding costly penalties.

These cyberthreats often intersect with compliance obligations in complex ways. HIPAA, SOC-2, and other regulatory frameworks require not only data encryption and access controls but also evidence of immutable storage, audit trails, and the capacity to prove data integrity over time. As imaging data becomes central to both patient care and enterprise analytics, compliance readiness is no longer a function of policy alone; it must be architected into the infrastructure itself. This shift is driving organizations to adopt cloud storage solutions that offer native compliance features such as object lock, multifactor authentication, automated retention policies, and real-time monitoring. Financial considerations are equally critical. The long-term retention of imaging data, including pediatric records that must be stored for up to three decades, places significant strain on healthcare budgets. Providers increasingly seek storage platforms that offer flat-rate pricing models, eliminate egress fees, and reduce the operational overhead associated with archival data management.

According to IDC, 25.5% of healthcare providers plan to increase their spending on medical imaging and archiving in 2025, while 17.2% are allocating new funds specifically for modernizing storage infrastructure.

Beyond compliance and cost control, the future of imaging infrastructure is increasingly defined by its role in enabling innovation. Enterprise imaging strategies, driven by AI and advanced analytics, are creating new use cases in clinical decision support, workflow orchestration, and remote diagnostics. IDC survey data indicates that 63.9% of providers increasing imaging investment are prioritizing AI for diagnostics, while 50% are expanding enterprise imaging capabilities, and 44.4% are investing in digital pathology. These use cases require scalable computing resources and agile storage systems capable of high-throughput access, metadata tagging, and seamless integration with AI inference engines and third-party applications.

This broader shift also reflects the increasing consumerization of healthcare. Patients now expect their imaging data to be accessible across devices, locations, and points of care, mirroring their experiences with digital retail, banking, and media. As virtual care and tele-imaging become more mainstream, imaging infrastructure must support distributed access, data replication, and low-latency retrieval. Cloud-based storage platforms are equipped to meet these demands, offering geographic redundancy, automated failover, and seamless integration with telehealth platforms and mobile diagnostic tools.

All these trends converge around a common inflection point: the necessity for healthcare providers to adopt cloud-first, AI-ready architectures that can simultaneously support cybersecurity, compliance, cost efficiency, and clinical agility. This involves more than merely migrating data to the cloud; it requires embracing an infrastructure strategy that reflects the realities of modern healthcare delivery. Whether facilitating AI-powered diagnostics, reducing ransomware risk, or uncovering new efficiencies in imaging workflows, cloud-based storage is swiftly becoming a foundational element of digital transformation in healthcare. In this context, adopting cloud-first storage strategies is no longer optional or experimental but a strategic necessity. Intelligent data platforms provide a viable path forward for healthcare organizations facing the challenges of increasing imaging complexity, regulatory scrutiny, and financial constraints. The capability to scale storage on demand, enforce data governance policies, and enhance interoperability with medical imaging, EHRs, and other core clinical and operational systems will define the next generation of leadership in healthcare IT. As provider organizations strive to secure patient trust, improve care delivery, and cultivate operational resilience, infrastructure investments must be aligned with these priorities.

Benefits

Cloud-first infrastructure offers healthcare organizations a slew of benefits. These include:

- » **Strengthened cybersecurity posture:** Modern cloud platforms are designed with advanced security features such as object-level immutability, multifactor authentication (MFA), multiuser authentication (MUA), and continuous telemetry-based monitoring. These capabilities create layered defense architectures that reduce the risk of data tampering, credential compromise, and ransomware infiltration, which is particularly critical for medical imaging systems, EHRs, and hybrid cloud environments.
- » **Regulatory-ready architecture:** Built-in compliance frameworks aligned with HIPAA, SOC-2, GDPR, and key EU-specific mandates such as France's HDS, which are typically underpinned by ISO/IEC 27001 standards, provide a unified security baseline and ensure that healthcare providers meet regional and international regulatory obligations with reduced manual effort. Capabilities such as object lock, immutable audit logging, and compliance

mode offer cryptographic assurance of data integrity, streamline audit processes, and mitigate the risk of regulatory penalties.

- » **Predictable economics and cost modeling:** Flat-rate or consumption-based pricing models eliminate uncertainty from cloud storage budgeting, which is especially important for hospitals and medical imaging centers facing constrained financial planning cycles. Removing egress fees and API surcharges allows healthcare IT leaders to scale data operations without financial penalties, aligning expenditures with patient care delivery priorities.
- » **Data longevity, retention, and accessibility:** Medical imaging data, clinical records, and genomic data sets often require retention for decades. Cloud-native archives ensure long-term durability with object-level versioning, automated replication, and seamless retrieval via standard APIs or third-party integrations. Instant access to historical data sets enhances real-time diagnostic recall, legal inquiries, and AI model training.
- » **Operational efficiency through simplified management:** With user-friendly administrative interfaces and centralized control planes, cloud-based infrastructure and platforms simplify complexity. This enables small and midsize healthcare organizations with limited cloud-native skills to manage petabyte-scale data sets, set automated retention policies, and onboard new workloads without requiring extensive DevOps or storage engineering expertise.
- » **Support for virtual care and telehealth expansion:** Cloud accessibility and geographic replication guarantee low-latency data availability across distributed care environments, allowing radiologists, specialists, and care coordinators to access diagnostic imaging and patient records remotely. This supports telehealth, remote patient monitoring, and cross-provider data sharing with secure, always-on infrastructure.
- » **Resilience and recovery in the face of disruption:** Geo-redundant replication, snapshot-based recovery, and immutable backup copies ensure continuity of operations during cyberincidents, system failures, or physical disasters. For mission-critical functions like radiology, cardiology, and oncology, cloud-native disaster recovery minimizes downtime and safeguards against data loss.

Trends

Healthcare providers should be aware of the following trends as they move to adopt a cloud-first approach.

- » **Increased ransomware threats:** Healthcare remains among the most targeted sectors for ransomware, with attackers increasingly focusing on high-value assets such as EHRs, PACS, VNAs, and backup environments. This surge in attacks is accelerating the adoption of immutable, cloud-based storage architectures that support air-gapped protection, object lock enforcement, and automated recovery workflows, which are key components of a zero trust data resilience strategy.
- » **Healthcare consumerization:** Patients demand seamless, on-demand access to their health information, mirroring the user experiences they encounter in other industries. This shift pressures providers to modernize legacy infrastructure and adopt data platforms supporting omni-channel engagement, real-time imaging access, and personalized care journeys across virtual and in-person touch points.
- » **Platform-centric IT architectures:** Healthcare providers are moving beyond siloed systems and vendor-specific stacks toward platform-first strategies that support multicloud deployment, API-driven interoperability, and unified

data governance. This architectural evolution enables providers to integrate diverse data sources, including medical imaging, genomics, and Internet of Things telemetry into a centralized ecosystem supporting clinical and operational intelligence.

- » **AI-driven medical imaging:** The growing use of traditional, predictive, generative, and agentic AI for medical imaging–related use cases, such as diagnostic assistance, image classification, and workflow automation, places unprecedented demands on storage performance and capacity. Platforms increasingly serve as the backbone for training and deploying medical imaging algorithms, supporting elastic compute, parallel processing, and rapid retrieval of large imaging data sets.
- » **IT as cost center to revenue catalyst:** Forward-thinking healthcare providers are reframing IT not as a cost to be contained but as a strategic lever for revenue diversification, clinical innovation, and patient acquisition. Cloud-based storage platforms with predictable pricing and operational flexibility allow CIOs to redirect capital from maintaining legacy infrastructure toward higher-value initiatives like digital front doors, remote diagnostics, and AI integration.

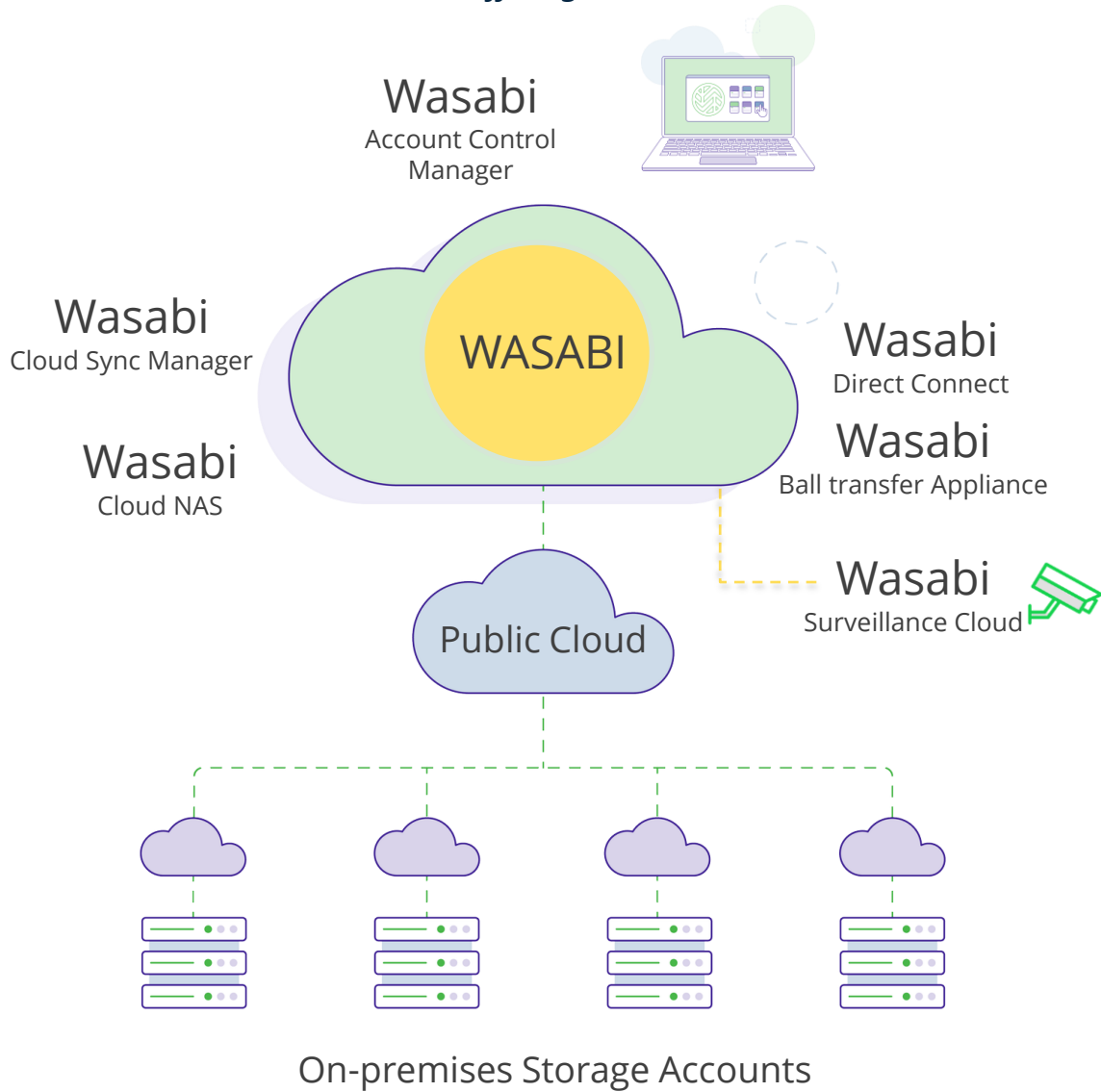
Considering Wasabi Technologies

Wasabi Technologies (Wasabi) is a United States–based cloud infrastructure provider specializing in object-based storage solutions that offer high performance, data durability, and economic predictability at scale. Wasabi's solutions aim to address the growing demand for cost-effective, compliant, and cyber-resilient storage infrastructure in healthcare. Its design philosophy prioritizes simplicity, security, and scalability, making it suitable for healthcare organizations undergoing modernization and transformation while managing increasing data volumes, regulatory complexities, and cyberthreats.

The portfolio features a core Hot Cloud Storage service designed for petabyte-scale workloads with flat-rate pricing, eliminating variable costs tied to data egress, API calls, and access operations. This model is meant to ensure financial transparency and simplify budgeting, particularly for healthcare organizations with fixed-cost funding or lengthy procurement cycles. The platform is built for high availability and durability, supported by native security and compliance features aligned with HIPAA, SOC-2, and other regulations. Key features include object lock and immutability to protect clinical imaging and audit records by preventing unauthorized data deletion or modification during a retention period. In addition, native MFA and single sign-on (SSO) enhance access control and streamline identity management, while features like Wasabi's MUA add an extra layer of authorization for critical account changes or deletions, mitigating insider threats. Compliance locking maintains strict data governance by ensuring that data sets remain compliant until retention policies expire. Last, Wasabi Direct Connect (WDX) provides secure, high-bandwidth private connectivity from on-premises datacenters, optimizing data transfer and reducing latency. If users already have healthcare data in a public cloud environment, Wasabi can also facilitate cloud-to-cloud data migrations via its Cloud Sync Manager (WCSM) service.

The platform enables integration with third-party clinical systems (e.g., EHRs, PACS, and VNAs), primarily through ecosystem partners such as Commvault and Rubrik. While direct integration with PACS/VNA platforms is not yet available, support is feasible via existing compatibility with infrastructure solutions like Dell Isilon and ECS, offering a scalable pathway for healthcare data interoperability. This enables healthcare providers to incorporate cloud storage seamlessly into their existing workflows without significant architectural redesign. As an option, users can also leverage Wasabi Account Control Manager (WACM) to facilitate operational oversight, promoting centralized governance across multiple storage accounts or business units (see Figure 2).

FIGURE 2: **Wasabi Architecture and Offerings**



Source: Wasabi, 2025

This feature is particularly valuable for large networks managing decentralized facilities, as it allows centralized management and provisioning of storage and enhances visibility into usage patterns, policy enforcement, and role-based access controls across the enterprise.

Challenges

While the demand for secure, cost-predictable cloud storage is growing in healthcare, several barriers to adoption remain. Many healthcare providers are still in the early stages of their cloud journeys and rely heavily on legacy systems, which makes modernization efforts slow and complex. Integration with entrenched technologies such as EHRs, PACS,

and analytics platforms often requires custom configurations, increasing implementation overhead. Despite platform neutrality, concerns about vendor lock-in and data migration costs persist, particularly for organizations managing decades of clinical archives. Security perceptions also pose a challenge. Although cloud platforms offer advanced protections like immutability and compliance locking, some healthcare IT leaders remain wary of offsite models, especially for PHI. Compounding this issue is a general shortage of cloud-native skills within provider IT teams, which can limit their ability to operationalize advanced features and maximize ROI from cloud investments. While Wasabi's infrastructure is well suited for healthcare and supports imaging system integration through ecosystem partners, the lack of native PACS/VNA integration may hinder adoption among enterprise providers seeking frictionless cloud transitions. Addressing this gap presents a strategic opportunity to accelerate uptake among imaging-heavy organizations and strengthen Wasabi's position as a turnkey cloud storage provider for enterprise-scale clinical archiving.

Conclusion

Secure, scalable data infrastructure in healthcare is urgently needed. Increased imaging volumes from AI diagnostics and digital pathology, for example, amplify the technical and regulatory demands on storage systems. Healthcare organizations confront rising cyberthreats and stricter compliance requirements, necessitating robust patient data protection, auditability, and operational continuity. Cloud-based storage platforms provide vital solutions with predictable costs, no hidden fees for data movement, and long-term archiving capabilities. These platforms enable cost reduction and IT modernization, helping organizations manage expenses, allocate resources for innovation, and comply with budgets in public and private health systems.

Regulatory alignment is essential. With budgets increasing for privacy, security, and data protection, cloud solutions featuring HIPAA-compliant capabilities such as data immutability, multifactor authentication, and compliance locking are critical for reducing organizational risk. In addition, platforms that integrate seamlessly with PACS, VNAs, AI workflows, and broader EHR ecosystems can minimize deployment friction and alleviate concerns about vendor lock-in and interoperability.

IDC anticipates that healthcare IT leaders will accelerate investment in cloud-first architectures not only for cost containment but also as a foundational pillar for data-driven, patient-centric healthcare delivery. As the industry evolves toward intelligent, distributed, and digitally connected care, storage vendors that secure data, reduce total ownership costs, and support regulatory compliance at scale will emerge as strategic partners in reshaping healthcare infrastructure. In this new modern era of data-driven care, storage is not just infrastructure but the backbone of trust, intelligence, and resilience. Healthcare providers looking to thrive rather than just survive must reimagine storage not as a sunk cost but as a catalyst for scalable clinical innovation and sustained operational impact.

Healthcare IT leaders will accelerate investment in cloud-first architectures not only for cost containment but also as a foundational pillar for data-driven, patient-centric healthcare delivery.

About the Analyst



Mutaz Shegawi, Senior Research Director, Worldwide Healthcare Provider Platforms and Technologies

Mutaz Shegawi leads the provider research practice at IDC Health Insights covering topics of most relevance to healthcare provider organizations looking to digitally transform and become more digitally native than their competition. Mutaz advises the executive, clinical, and technical leadership of the world's foremost health information technology supplier and buyer organizations by producing data-driven research and thought-leadership insights that help navigate strategic challenges in health information technology and transform complexity to clarity in decision-making that would decrease costs, enhance quality, optimize access, improve patient safety, and champion patient experience.

MESSAGE FROM THE SPONSOR

Wasabi is on a mission to store the world's data by delivering predictable economics, built-in security features, with unmatched simplicity. For the last decade, Wasabi has been supporting 1000s of healthcare clients across the globe. These customers have solved various challenges in back-up/recovery, long-term archival, cybersecurity, video surveillance, and medical image archiving. Customers and partners have been free to build best-of-breed solutions with the industry's fastest-growing ecosystem of independent cloud application partners. Learn more about how Wasabi is solving the healthcare challenges of tomorrow for hospitals and medical universities all over the world.



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

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.

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 helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA