Vendor-neutral, cloud-based medical image archiving

Healthcare organizations worldwide struggle to manage the exploding growth and complexity of digital patient information—across disparate facilities, applications, and data silos. If your health organization is like most, you may not be equipped for the demand this deluge creates on your IT resources.

Traditional solutions, including picture and archiving communication systems (PACS), continue to manage patient information using proprietary formats. With clinical content locked away in these systems, patient care and safety may be compromised. A lack of data liquidity and accessibility can increase complexity, making it difficult and costly to pursue new opportunities, clinical strategies, business models, acquisitions, and other initiatives.

Vendor-neutral archive (VNA) solutions—from Perceptive Software, powered by Acuo, and leveraging the Microsoft Azure cloud platform—can help your health organization reduce the cost and complexity of clinical data management.

- Eliminate PACS and storage vendor shackles on clinical information, delivering true data liquidity and interoperability.
- Help reduce the time, cost, and complexity of managing and maintaining medical imaging content.
- Scale up or down quickly in response to market opportunities and fluctuating business needs.
- Help ensure business continuity and disaster recovery, with less technical effort and capital expense.

Content access that benefits patients and providers

A non-proprietary enterprise solution for image mobility can help you take control of your unstructured clinical content—including all enterprise medical images—accelerating patient information to the point of need while reducing healthcare integration costs, inefficiencies, and long-term total cost of ownership. The virtualization of storage, network, and application resources, combined with a service-oriented delivery model, helps enable providers to quickly sync their medical imaging systems with the Microsoft Azure cloud-computing platform.

This creates a trusted data hub that enables anytime, anywhere data access to both providers and patients.\(^1\) The Perceptive VNA solution can help your health organization achieve full interoperability across multiple disparate systems by consolidating long-term data management.

- Liberate clinical data from departmental silos.
- Help ensure interoperability across all PACS and data storage solutions.
- Take advantage of extreme IT flexibility, virtualization, configurability, and scalability.
- Exercise the freedom and agility to pursue strategic objectives.

The Perceptive VNA solution’s embedded intelligent workflow capabilities, including clinical and business analytics, can help you increase operational efficiency and enhance patient outcomes. Streamlined access to clinical data can benefit all patients, helping your teams to provide faster, more accurate care at a lower cost to your health organization.
A solid foundation: technical perspective

The multifaceted Perceptive VNA solution can capture and control all enterprise clinical data—including all forms of DICOM (Digital Imaging and Communications in Medicine) and non-DICOM content—to help improve medical collaboration and decision making. And provides the foundational data infrastructure to enable content-based EMRs.

Clinical abstraction
Maximizes access, routing, and control of all DICOM and non-DICOM clinical content through standards and a rich set of web services, including:

- **Medical image virtualization.** Standards-based integration to the PACS and RIS through a rich set of DICOM services. Connects clinical imaging systems, and enables image migration and bi-directional HL7 support for pre-fetching prior studies and updating/merging/deleting actions.
- **Non-DICOM virtualization.** Through fully integrated XDS and XDS-I support, manage and access all types of non-DICOM content.
- **Service orchestration.** Provides the integration gateway to share clinical content through industry standards like WADO, MINT, web services, RESTful interfaces, HL7, and OData.

Intelligence engine
Couples the clinical abstraction and life-cycle management features through clinical workflow, compliance, and contextual capabilities, including:

- **Replication.** The ability to synchronize metadata between datacenters and to create a highly available platform with business continuity features tightly integrated with the storage infrastructure on-premises and in the Microsoft Azure cloud.
- **Compliance.** Fully compliant with DICOM standards and audit standards through syslog and IHE ATNA support.
- **Context.** The ability to support data contextual properties to enable multitenant, multidomain, and multiology capabilities.

Life-cycle management
Provides the functionality to manage data on a long-term basis and to optimize best-of-breed storage platforms, including:

- **Storage abstraction.** Delivers multitenant support for appropriate storage utilization, multithreaded actions for storage interaction, and abstraction to ease migration/consolidation of storage platforms.
- **Clinical data integration.** Provides metadata integration to API-enabled storage platforms to optimize storage strategies.
- **System and application health.** Use integrated dashboards to monitor and receive alerts about VNA performance.
Reduce cost and complexity

Built on Microsoft’s global foundation of datacenters, the Microsoft Azure platform can enable your healthcare organization to take advantage of the agility and scalability the cloud offers by delivering HIPAA-compliant, highly available, geo-redundant data storage, compute, and networking capabilities at a fraction of the on-premises cost. These capabilities help optimize data management costs and reduce complexity for your IT organization—without any infrastructure investment.

Focus on opportunities, not infrastructure

Supported by an industry-vetted Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement, the Azure platform can enable you to quickly expand or contract resources automatically to meet volume demand. Provide a foundation for mergers, acquisitions, divestitures, and imaging system consolidations. And convert upfront capital expenses to lower operating costs.

• Use Microsoft economies of scale to help reduce storage costs.
• Shorten setup and cycle time for adding storage capacity and infrastructure resources.
• Migrate large amounts of data to the cloud.
• Free up valuable on-premises infrastructure and resources for high-priority workloads.

By extracting your IT resources from the management burden datacenters customarily consume, they can refocus their energies on previously cost-prohibitive new opportunities. Or divert more attention to mandatory projects like Meaningful Use of Electronic Medical Records and ICD-10.

Always be prepared

Convenient offsite storage can better prepare your organization to weather catastrophic events—like earthquakes, wild fires, and tornados.

• **High availability: Geo-replication.** Your data is replicated three times on three different storage nodes across three fault domains within your primary datacenter, and then replicated again three times at a secondary datacenter. The end result? Six copies of your data are maintained for the price of one. And you can have the peace of mind that comes when you’re able to meet HIPAA data recoverability requirements.

• **Disaster recovery: Seamless geo-failover.** DNS entries are automatically updated to point from the primary location to the secondary location, so existing storage resource locators will work. You don’t need to change your application’s URIs; all existing URIs will work the same before and after a geo-failover, enabling you to maintain your own service level agreement (SLA) for information access with your internal constituents.

Always be prepared

Convenient offsite storage can better prepare your organization to weather catastrophic events—like earthquakes, wild fires, and tornados.

• **High availability: Geo-replication.** Your data is replicated three times on three different storage nodes across three fault domains within your primary datacenter, and then replicated again three times at a secondary datacenter. The end result? Six copies of your data are maintained for the price of one. And you can have the peace of mind that comes when you’re able to meet HIPAA data recoverability requirements.

• **Disaster recovery: Seamless geo-failover.** DNS entries are automatically updated to point from the primary location to the secondary location, so existing storage resource locators will work. You don’t need to change your application’s URIs; all existing URIs will work the same before and after a geo-failover, enabling you to maintain your own service level agreement (SLA) for information access with your internal constituents.

Put to the test

In an independent test of Cloud Storage Providers, the Microsoft Azure platform delivered the fastest Read/Write/Delete operations across different file sizes, the fastest response times and the fewest errors, posting zero errors during 100 million read/write operations. Read the complete report.

Best-in-class performance builds confidence

Meet organizational SLAs for accessibility. The Azure platform delivers best-in-class cloud storage performance through a new Flat Network Storage architecture that leverages software-based instead of hardware-based load balancing, to help improve transaction times.
Safeguard all your electronic protected health information

Contrary to common perception, a HIPAA-compliant public cloud environment may reduce the risk of breaching the privacy and security of patient information; the depth and breadth of Microsoft’s security investments help safeguard your data against unauthorized use and disclosure.

Security

Microsoft Azure platform in-depth defense—from data encryption, updated anti-virus patches, and security features built into applications to physical controls that can prevent unauthorized individuals from obtaining access to equipment—helps ensure that should any one area fail for whatever reason, compensating controls in other areas can help maintain your data security. Here’s how:

- **Physical layer.** Azure servers are stored in the datacenters run by Microsoft Global Foundation Services, applying best practices and industry standards like video surveillance and access control.
- **Network layer.** Microsoft deploys VLANs and packet filters to segregate network access between different organizations’ data, management systems, and the Internet, helping to ensure traffic isn’t accessed by any undesired hosts.
- **Data layer.** Access to data is controlled through strong storage access keys that you control. Communication to the data can be secured using SSL, and the data itself can be encrypted inside of storage.
- **User layer.** Azure provides robust account management services with training, awareness, and screening. Azure also offers open, interoperable Access Control Services that can be configured to authenticate using existing identity information.

Privacy

Privacy: It’s at the heart of Microsoft Trustworthy Computing and an integral part of Microsoft’s product and service life cycle.

- **Data location.** You can specify the geographic location(s) of the Microsoft datacenters where your patient data will be stored. Except as directed by you, or where necessary to provide support with your approval, or to comply with legal requirements, Microsoft won’t transfer your data outside the region you specify, enabling you to meet patient data privacy requirements.
- **Data use.** We only use customer data to provide cloud services. This may include troubleshooting aimed at preventing, detecting, and repairing problems affecting the operation of the services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (like malware or spam).
- **Disclosure to third parties.** Microsoft won’t disclose your data to a third party (including law enforcement, other government entity, or civil litigant) except as you direct or unless required by law.

Compliance

Meet rigorous standards for the storage of data in the cloud. Microsoft’s HIPAA Business Associate Agreement for Microsoft Azure was created specifically for, and by, the health industry—a collaboration that engaged academic medical centers, government agencies, providers, and health plans. You can effectively and efficiently manage compliance with the physical, technical, and administrative security safeguards for electronically protected health information required by HIPAA, and receive breach notifications in half the time required by Health Information Technology for Economic and Clinical Health (HITECH).

Microsoft compliance with various industry security standards is independently verified through regular audits:

- ISO/IEC 27001:2005 Audit and Certification
- SOC 1 and SOC 2 SSAE 16/ISAE 3402 Attestations
- Payment Card Industry – Data Security Standards Level 1 Attestation of Compliance
- Provisional Authorities to Operate from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board
- EU Safe Harbor, in accordance with the EU Data Protection Directive

Find out more about Microsoft Azure compliance.
Focus on the business of healthcare

You can make medical imaging content available at the point of need to help improve the quality of care you deliver. A non-proprietary enterprise solution for image mobility that leverages the Microsoft Azure platform’s high reliability and best-in-class performance offers timely access to this critical content. Helps you comply with healthcare regulations. And untethers your IT specialists from the time-consuming, costly task of infrastructure management. So everyone on your team can devote their attention to the business of healthcare.

To learn more, contact your Microsoft or Perceptive Software Account Manager.

microsoft.com/health

---

1 An appropriate device, Internet connection, and supported browser and/or carrier network connectivity are required. Data charges may apply.
2 Microsoft solutions may not support all devices at the same level of features, functions, capabilities, and security.