

Solution Brief

Nasuni and HIPAA Compliance



HIPAA Compliance Challenges

Healthcare organizations and other entities that handle personal health data must operate under increasingly strict and complex governance. The Health Insurance Portability and Accountability Act (HIPAA) and similar regulations – while effective at securing electronic Protected Health Information (PHI) – make it difficult to select IT solutions that store, protect and manage electronic PHI in a compliant and scalable manner.

Traditional storage architectures can no longer keep pace with the twin healthcare demands of scalability and compliance. IT organizations are constantly refreshing or expanding on-premises SAN and NAS infrastructures in a futile effort to keep up with the explosive growth in image size for modalities like CT, ultrasound, tomography, and MRI. For example, a move from 2D mammography to 3D increases image size by about 20-fold, and each patient study may require 4 images where, before, only 1 was required. Budgets are further compromised as each primary storage expenditure requires commensurate investments in backup infrastructure, DR sites, datacenter floor space, and IT cost. Most importantly, care provider efficiency and patient outcomes are impacted by insufficient capacity and inadequate recovery points and recovery times.

Nasuni: The New Cloud-Scale Solution

Nasuni cloud-scale enterprise file services is the new strategic platform for storage, data protection, and global file access in healthcare. Backed by leading private and public cloud object stores, Nasuni's cloud-native global file system

Highlights

Accelerate collaboration among care providers with secure, enterprise-wide file sharing

Secure patient data with file encryption and policy-driven access control

Improve patient outcomes with reduced downtime powered by built-in backup, rapid file restores, and easy disaster recovery

Support shared service strategies with centralized storage provisioning and management

combined with local caching appliances is the ideal solution for highly scalable, HIPAA-compliant healthcare file infrastructure.

HIPAA Compliance Requirements

While there is no official HIPAA certification body or seal of approval for technology products, the act does establish a set of regulations and recommendations for protecting digital medical records and other PHI, while ensuring data confidentiality, integrity and availability. The HIPAA Security Rule defines the standards any organization handling PHI must meet. These rules, in combination with additional regulations and penalties set forth by the Health Information for Technology and Clinical Health (HITECH) act, outline administrative, physical and technical safeguards.

For example, PHI needs to be backed up and always recoverable in the event of a disaster. The regulations also outline standard security best practices such as access control, minimum password lengths, and encryption.

How Nasuni Facilitates HIPAA Compliance

Nasuni is an enterprise file services platform powered by Nasuni UniFS®, the first global file system designed to reside in cloud object stores such as Azure, AWS, IBM Cloud Object Storage, and Dell EMC ECS. UniFS stores the “gold copies” of all files in the cloud, while Nasuni Edge Appliances located on-site provide fast, secure access to the frequently accessed files through standard NAS protocols. Rounding out the platform is the Nasuni Management Console, which enables IT to centrally manage all Edge Appliances, and Nasuni cloud services, which orchestrate Global Version Management, Global File Lock, and data propagation.

Nasuni meets relevant HIPAA and HITECH regulations in many ways:

1. Nasuni Edge Appliances in each office reside on-premises, within the physical and electronic security perimeters of each location, and are thus protected by existing security controls and safeguards.
2. Nasuni Edge Appliances can be physical or virtual. Physical appliances use self-encrypting hard drives or SSD to protect PHI, while virtual appliances leverage the storage controls of existing virtual infrastructure.
3. Nasuni Edge Appliances integrate with Active Directory and LDAP for authentication and access. All existing organizational and management controls for passwords and file access control are maintained.
4. Nasuni provides detailed file audit capabilities that track every change to every file.
5. Nasuni uses customer-controlled encryption keys to protect all data before it leaves the security perimeter of any location on route to cloud object storage. Neither Nasuni nor any other outside entity can decrypt or access that electronic PHI without the customer keys.

“We saw three sharply rising trends that made it clear to us moving to the cloud sooner rather than later was an absolute necessity, not an option: image size, quantity, and storage costs. That Nasuni built their solution on top of Microsoft Azure made us confident that our data would be secure. We get security, geo-redundancy, and disaster recovery all built-in. When it comes to retrieval, we can ensure clinicians have rapid access to images without cloud latency using Nasuni edge appliances, which intelligently cache files locally. We are also able to pre-load large, historical file sets if they are needed for a patient visit the next day. Overall, Nasuni/Azure provides a very comprehensive cloud solution. We would not be able to reach our projected 1.5 petabytes of mammography image storage without it.”

—R. Todd Thomas
CIO

Austin Radiological Association

[ARA Case Study \(Microsoft\) >>](#)

[ARA Case Study \(Nasuni\) >>](#)

- Nasuni inherits the security of its underlying cloud object storage partners. Data is stored in secured cloud data centers, and encrypted in transit and at rest.

Leveraging Our Cloud Partners' Compliance Efforts

To ensure HIPAA compliance, Amazon, Microsoft, IBM, and other cloud storage providers maintain physically and electronically secure data centers that institute security best practices. By designing UniFS as the first global file system to “live” in cloud object storage, Nasuni automatically inherits these best practices. Some cloud providers have taken the extra step of aligning with broader and more stringent regulations to satisfy HIPAA. Nasuni inherits these as well.

Microsoft Azure

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published ISO/IEC 27001, a set of security standards focused on ensuring information security and management control. Although it is not HIPAA-specific, the best practices laid out by 27001 cover all HIPAA requirements. Microsoft Azure has achieved ISO/IEC 27001 certification and submits to a third-party check every year.

Amazon Web Services (AWS)

To ensure its cloud services meet HIPAA requirements, AWS follows the security practices defined by FedRAMP and National Institute of Standards and Technology (NIST) 800-853, a broader, more stringent set of security rules that also satisfies HIPAA2 requirements.

Nasuni Benefits for Healthcare

Hospitals, regional healthcare providers, imaging centers and other organizations entrusted with PHI are all using Nasuni for scalable, HIPAA-compliant file infrastructure. Benefits include:

- Enhanced access to PACS images and Vendor Neutral Archives (VNA), with no limits on the number of users and images. More patients can be seen with less wait time. Diagnoses are faster and more accurate.
- Unlimited capacity without the need to upgrade or deploy new arrays.
- Improved business continuity and data protection through fast restores and 15-minute Disaster Recovery from any location.
- Ransomware mitigation through continuous versioning of file data that enables rollback to any point in time.
- Cost savings of up to 60% compared to on-premises NAS, backup, archive, replication, and DR infrastructure.

“We won’t consider implementing a technology until we’re sure it will comply with our HIPAA requirements. Nasuni and Azure passed all our tests. In terms of protecting patient data and leveraging a more scalable cloud technology, we feel like we are ahead of the curve by partnering with Nasuni. Just in terms of DR, we’re far beyond where we were. Now, if we lost our data center, all we would have to do is find a PC, install a viewer, and point to the Nasuni volume in the cloud. Or we could spin up a Nasuni edge appliance in any location that has cloud connectivity and start pointing clinicians to that. It would literally take minutes to recover data. And we didn’t have to build or lease a dedicated DR site.”

–Paul Feilmeier
Director of IT

Faith Regional Health Services

[Faith Regional Case Study >>](#)



About Nasuni

Nasuni (“NAS Unified”) is the leading provider of cloud-scale enterprise file services. Powered by UniFS®, the first cloud-native file system, Nasuni leverages private and public cloud object storage to integrate and surpass the “silo” capabilities of traditional Network Attached Storage (NAS), distributed file systems, data protection software, file synchronization solutions, and disaster recovery infrastructure. With Nasuni’s unlimited primary and archive storage capacity, industry-leading recovery points and recovery times, global file access, and unmatched scalability, enterprises can meet “cloud-first” and business growth objectives, extract more value from their file data, and transform expensive storage infrastructure into an affordable, as-a-service asset.

For more information on how Nasuni enterprise file services can help your healthcare organization, visit www.nasuni.com/healthcare or contact your local Nasuni representative or reseller at www.nasuni.com.