



LYVE CLOUD— HEALTHCARE'S HOLISTIC APPROACH TO STORING DATA

HIPPA-compliant storage as a service that satisfies the need for greater availability and security—find out why it's just what the doctor ordered.

CONTENTS

- 03** INTRODUCTION
 - 03** EXECUTIVE SUMMARY

- 03** EVALUATING CLOUD SERVICE PROVIDERS
 - 03** WORKLOAD SELECTION
 - 04** IMPACT TO CURRENT IT OPERATIONS
 - 04** FINANCIALS
 - 04** HOW TO EVALUATE HIPAA COMPLIANT STORAGE

- 05** WHY LYVE CLOUD FOR HIPAA MEETS HEALTHCARE NEEDS
 - 05** STANDARDS-BASED COMPLIANCE
 - 06** HIGH AVAILABILITY & DISASTER RECOVERY
 - 07** PRICE AND PERFORMANCE
 - 07** LTO TAPE MIGRATION MADE EASY
 - 08** SECURITY

- 10** CONCLUSION



Introduction

As the healthcare industry continues to achieve higher levels of patient care while navigating pandemics and numerous regulatory rules, its need for greater data availability and security is paramount. Healthcare organizations increasingly rely on partnerships with cloud providers to offload overfilled and understaffed datacenters while guaranteeing the security, immutability, and availability of patient data.

Seagate® Lyve™ Cloud is a HIPPA-compliant cloud solution that provides a holistic approach to data storage. This white paper examines how to evaluate cloud providers and describes how Seagate meets the stringent healthcare industry standards through our world class pricing, high availability, superior performance, and services to make IT infrastructure more efficient.

Evaluating Cloud Service Providers

When selecting a cloud service provider, several key questions come to mind:

1. What workloads make sense to move?
2. How will moving data to a cloud provider impact my IT department?
3. What are the financial impacts to leveraging the cloud?
4. How do I know my data is safe?

Let's consider each of these points.

Workload Selection

To store medical records of all file types it's increasingly important to enable healthcare and IT companies to collaborate in order to drive the growth of healthcare data storage and reduce IT workloads. With healthcare data expected to grow at 17% annually through 2026¹, there are several key themes to consider when deciding what files will make the greatest impact to move and why.

The first is data, and knowing which application generates the most data and its requirements for Storage as a Service. In most healthcare environments, 75% of data is content created by various modalities usually residing in a Picture Archiving and Communication System (PACS). Data stored in a PACS are either stored as a file or an object depending on the original design of the system. These archives are usually in the petabyte+ club, and in many cases scale to the 10's of PBs.

Hospital groups usually have this data on premise and then replicate it to another datacenter across town or to a co-location data center in the region. Additionally, there may be legacy systems with copious amounts of tape that result in additional costs, labor burden, and frequent technology migration planning. But there's value in this data and it needs to be preserved for compliance reasons, yet these legacy systems might not allow organizations to use and activate the data efficiently. The time, expertise, and cost usually mean that they will simply ignore the problem until a solution presents itself.



Another area for datacenter offloading is backup. All major backup vendors support S3 Cloud Storage as a backup data repository. The integration is very easy and all you must do is cut and paste the S3 Bucket URL address into the menu with login credentials and start writing data to the cloud over the internet or on a private connection.

The final datasets to consider are data lakes for patient data AI and ML analytics. Most progressive healthcare organizations are beginning to farm their datasets for insight and enhanced diagnostics. When analyzing this data, intense short-term compute is required to run these scientific studies. “Elastic compute” is perfect for these jobs, while data is perpetual and is used repeatedly for various studies. These are workloads most well suited for the cloud and its operating model.

IT Operation Impacts

Outside of the huge reduction in floor space, power, and cooling, the next greatest impact is system maintenance and upkeep as well as regular system, data storage, and other technology migrations. Cloud providers perform all upgrades including the most current software patching and vulnerability testing, removing this from the IT team’s responsibilities. Dynamic scaling means never having to make anyone wait for the global supply chain to come through with the goods, and the availability of services in real time makes it easy to adopt new capabilities. Let’s call this group of advantages “time to market” features. For the diehard IT Specialist, the one difficult thing to relinquish is control over how things are delivered outside of your configuration. When buying IT as a service, trust and overtime performance is the only thing that can relieve that feeling of concern and helplessness.

Financial Impacts

When it comes to your financials, it’s important to be sure that your cloud spending doesn’t grow faster than your revenues. It can often be difficult to understand cloud pricing when signing onto a new service. Numerous bills show up in complex formats that are often alienating from the original service. An all-inclusive offer would be more appealing than hard to understand, metric-triggering bills. As IT operating budgets are easily the largest expense for most businesses, it’s rewarding to find a solution that meets your needs and your budget. That’s why Lyve Cloud operates with zero add-on charges for egress or API calls and delivers predictable cloud TCO and data storage savings of about 70%. You can scale without limits thanks to elasticity and best-in-class cloud storage efficiency based on Seagate’s decades of data storage and management experience.



Security Impacts

How do you evaluate a HIPAA-compliant storage as a Service cloud provider?

When deciding what cloud storage solution best aligns with your needs as a healthcare provider, the decision on which HIPAA-compliant Storage as a Service cloud provider to work with should be based somewhat on security impacts. With an increase in digital storage expected to reach as high as 36% by 2025ⁱⁱ, the collection of data must be seamless to ensure security, communication, and availability of real time data.



For example, in a Picture Archiving and Communication System (PACS), you must decide the level of availability and performance you need for your system and if that solution will protect your data. When looking at your data, you have identifiable data that needs to be protected by HIPAA-compliant storage services. However, for non-anonymized data you can still use HIPAA-compliant storage or utilize storage providers in other regions for more availability with additional choices in proximity.

On top of that, you need higher compliance checks and balances to properly use that data. Most cloud service providers will not have all data centers HIPAA certified. However, that enables you to use whatever amount of storage centers that are HIPAA certified as well as their storage centers that aren't HIPAA certified for other data storage use cases.

A HIPAA-compliant cloud provider like Lyve Cloud meets these needs with stringent security that is further backed by ISO 27001 and SOC2 Type 2 certifications. Lyve Cloud has both HIPAA-compliant data storage centers and non-HIPAA-compliant storage centers with compute resources. While you can store your identifiable data in a HIPAA-compliant storage center, you can also store your anonymized data and take advantage of our compute resources to do more with your data.

Why Lyve Cloud for HIPAA Meets Healthcare Needs

Seagate built Lyve Cloud to be the industry leader for the healthcare sector, with core tenants around: resilience, compliance, performance, and value. According to Health and Human Services (HHS.org), Lyve Cloud is a “No View” SaaS provider—meaning Seagate can never see the data based on data in-flight and at-rest encryption, where the customer has a secret key from their own key management system (KMS). By doing this, we always ensure complete protection of the data under our care. Lyve Cloud uses a standards-based approach that produces the highest level of compliance and security in the market today. Our rigorous risk management program aligned with ISO 27001, SOC 2 Type 2, and HIPAA certifications protects a wide set of personally identifiable health data including hospitals, medical providers, employer health, and more, enabling us to deliver the highest level of HIPAA compliance available today.

Standards-Based Compliance

For a hospital group with hundreds of clinical applications and medical devices—HIS, RIS, PET, CT, and more—being accessed by thousands of individuals across many different networks, a biannual certification would make sense. But Seagate Lyve Cloud is a global manufacturer of storage and has the highest level of ISO 27001 and SOC 2 compliance. SOC 2 is customized by industry and audited annually, making it long term and continuous. Together with a HIPAA audit partner, annual audits are performed with remediation. For hospital groups, assessments every two years are tough enough. However, for a manufacturer and storage-as-a-service cloud provider, annual assessments are required. For a no-view storage-as-a-service provider like Lyve Cloud, a standards-based approach is the most appropriate since we do not view our customers' data.



High Availability and Disaster Recovery

Let's talk about Lyve Cloud's high availability and disaster recovery capabilities. Lyve Cloud offers multiple use cases for healthcare entities—the first is single site regional data centers. These sites offer 11 9's of data durability, making it almost impossible to experience any type of data degradation based on the underlying design while also supporting workloads that do not require HIPAA compliance.

Next, Lyve Cloud offers high availability (HA) due to in-region HIPAA Compliant data center sites that are comprised of three geographically separate data centers all interconnected with dedicated dark fiber in a regional cluster. This allows for continuous, uninterrupted access to data even if an entire data center goes offline. Additionally, if a customer requires disaster recovery (DR) capabilities, we offer multi-zone clusters that you can replicate your data between, delivering the highest level of data protection and availability possible today in a cloud SaaS offering. So as a healthcare organization, we can support your non-HIPAA workloads, HIPAA workloads that are HA second copies (target site), and source side HIPAA workloads that can also have second copies in a multi-zone DR configuration.



Price and Performance

When it comes to pricing, Lyve Cloud was built around the same principles that led Seagate to become the worldwide leader in storage quality and value. In that same vein, Lyve Cloud is one of the highest performing, S3 storage products on the market for the healthcare industry. With our simple and predictable cloud storage architecture, we deliver high performance, low latency object storage in a highly available HIPAA compliant offering for the cost of archive solutions.

Cloud-based electronic healthcare media and medical records are much more attainable than once thought, and their widespread use is a beneficial change to the healthcare system. But when it comes to cost, what's the bottom line? On average, a cloud based electronic healthcare record system costs about \$233,000 USD for the first year for a five-doctor practice with \$5,000-\$10,000 USD in upfront costs. However, the benefits begin right after your service is implemented. You don't have to wait for complex installations or on-site training, so it's easy to integrate and easy to learn. This unique and flexible cloud-based solution allows you to complete tasks or work from outside the office or between patient appointmentsⁱⁱⁱ.

Many life science and healthcare organizations face costs when it comes to moving their systems to the cloud. However, that opens a door for opportunity. When using Lyve Cloud, you can still perform cutting edge research and data analytics while moving your practice into the modern age without breaking the bank. Seagate's Lyve Cloud has zero add-on charges for egress or API calls and delivers predictable cloud TCO. On the other hand, that service is inclusive of our tape migration and storage services that enable healthcare entities to put all their data (legacy and current) into motion for less than the cost of storing it on tape or on premise.

LTO Tape Migration Made Easy

Lyve Cloud's tape migration and storage services enable organizations to bridge the gap between the cloud and useful legacy data stored on LTO tape. Physically stored media can be difficult to access and requires time consuming technology upgrades and migration efforts for data preservation. But migrating that LTO media and storing it in Lyve Cloud's S3 data repository means healthcare organizations can easily and securely access and make use of their data globally, in real time. Not only does this enable healthcare and life science organizations to stop media migrations, but it allows them to re-focus their IT staff, resources, and budgets so they can address other priorities. Lyve cloud's storage as a service provides numerous benefits to your organization:

- Move data across your enterprise with a pricing structure that won't lock you in
- Achieve better and faster results when using that data in a service of your choice
- Create new revenue streams and improve the quality of human life
- Reduce your operational and archival cost of physical storage



Security

How do you know that your data and patient data are safe?

Lyve Cloud is new and more modern than most traditional providers and was built for the most stringent security upfront.



Data Transfer over the Internet—Transport Security

The Lyve Cloud service enforces standard TLS 1.2 with 256-bit advanced encryption standard (AES) Galois/Counter Mode (GCM), otherwise known as AES-256-GCM, to establish secure communications to the customer. As an authenticated encryption algorithm, GCM provides proven security of the symmetric-key cryptographic cipher that has been widely adopted for its performance.

Customer

Lyve Cloud



Authentication, Authorization, and Data Integrity

Authentication, authorization, and data integrity are handled in every transaction with the Lyve Cloud API through the authorization header. The authorization header contains both the account’s access key and a cryptographic signature. By validating the account access key and verifying the signature which contains a checksum of the data chunk, the Lyve Cloud API can ensure the validity and integrity of the request before processing it further.

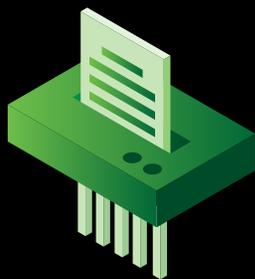


Default Data Encryption and Key Management

A key security feature of Lyve Cloud is that all data is encrypted before it's stored, regardless of whether it's encrypted at the source. There is no option to dial back the protection. Two options for encryption key management are supported:

- Server-side encryption with client-provided key (SSE-C)
- Server-side encryption with a key generated by the Lyve Cloud key management system (KMS) (SSE-S3)

In both SSE-C and SSE-S3, the key used for object encryption, the object encryption key (OEK) is uniquely generated using a cryptographically secure pseudo-random number generator (CSPRNG). The OEK is never stored in clear text; rather, it's stored in its encrypted form as part of the object metadata. The OEK is encrypted by the key encrypting key (KEK), which is generated by a key derivation algorithm using either the client-provided key (SSE-C) or Lyve Cloud KMS key (SSE-S3) and other object-specific metadata. The cryptographic primitive used for all the object encryption operations is AES-256-GCM.



Secure Erase

Lyve Cloud's envelope encryption uses strong AES-256-GCM, requires that either a client key (SSE-C) or the client's unique master key from the Lyve Cloud KMS (SSE-S3) is provided to derive the KEK that is used to encrypt the OEK that's stored in the metadata of the object. Without this access to the KEK, the data object is cryptographically secure. Cryptographic erasure, leveraging the same algorithms used in FIPS 140-2/3 compliance Seagate hard disk drive, is recognized by NIST 800-88 and ISO/IES 27040:2015 as a suitable and even preferred method of data/media sanitation.

When a customer chooses to end their tenancy with Lyve Cloud, they can be confident that their data will be securely cryptographically erased in compliance with recognized NIST and ISO standards. With client-provided keys (SSE-C), the key that's used to derive the KEK is only provided by the customer in the API request. Since this is never stored by Lyve Cloud, customers using SSE-C render the object data cryptographically erased by deleting or simply not using the key. In the case of SSE-S3, where the client's unique customer-managed key (CMK) is generated by the Lyve Cloud KMS, which is managed in a secure enclave, the CMK account is deleted upon tenant termination, effectively destroying the customer unique keys necessary to deriving the KEK.



Conclusion

HIPAA compliance requires rigorous security measures and training. On top of that, we are also ISO 27001 and SOC 2 certified. Our strategic and full commitment to HIPAA further demonstrates our responsibility to the most stringent, globally recognized data security standards. Lyve Cloud data center employees have been continually trained for years to meet our high security standards with Lyve Cloud. By using a standards-based approach in accordance with our annual HIPAA audit partner, Lyve Cloud is continuously scanning for and remediating vulnerabilities. Our high-performance tier paired with our high availability and disaster recovery offerings allow us to support all use cases at one low per TB monthly charge. Since we do not charge for data access or performance triggers, our customers have a bill with one line item: Average Daily Use × per TB charge rate. There are no additional charges, so your bill is transparent and trustworthy. With no extra charge for multisite high availability, it's the same low price as our individual data center offerings with no upcharge for HIPAA-compliant storage.

Although we're not your financial advisor, we think it's a no brainer.

Additional Resources

Lyve Cloud Security White Paper: learn.seagate.com/web-lyve-cloud-security-white-paper

Lyve Cloud Availability and Durability White Paper:
learn.seagate.com/web-lyve-cloud-availability-and-data-durability

Lyve Cloud PBBA White Paper: www.seagate.com/resources/enterprise/white-paper/Modernize-Data-Protection-Backup-and-Recovery.pdf

Lyve Cloud Product Brochure: www.seagate.com/files/www-content/services/cloud/storage/shared/files/seagate-lyve-cloud-product-brochure.pdf

Ready to Learn More?

Talk to an expert www.seagate.com/services/cloud/storage

Additional Resources

i www.thebusinessresearchcompany.com/report/healthcare-data-storage-global-market-report

ii www.hcinnovationgroup.com/interoperability-hie/cloud-computing-storage/article/13007784/the-cloud-more-affordable-than-you-think

iii www.hcinnovationgroup.com/interoperability-hie/cloud-computing-storage/article/13007784/the-cloud-more-affordable-than-you-think

seagate.com

© 2023 Seagate Technology LLC. All rights reserved. Seagate, Seagate Technology, and the Spiral logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. Lyve and the Lyve logo are either trademarks or registered trademarks of Seagate Technology LLC or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Seagate reserves the right to change, without notice, product offerings or specifications. TP756.1-23010US January 2023



SEAGATE