IRON MOUNTAIN®

HAS HEALTHCARE REACHED THE TIPPING POINT OF DATA GROWTH AND CYBERSECURITY?

INDUSTRY FACT:

WITH HEALTHCARE DATA PROJECTED TO GROW AT A CAGR OF 36% THROUGH 2025 (IDC), AND ROUGHLY 60% TO 80% OF IT BUDGETS ALLOCATED TO MAINTAINING LEGACY APPLICATIONS AS WELL AS MAINFRAME COMPONENTS, HOW CAN IT LEADERS MAKE THE INVESTMENTS REQUIRED TO KEEP PACE WHILE PROTECTING AGAINST CYBERTHREATS?

INTRODUCTION

Storing all of your data in the cloud is expensive, especially since most data is inactive. In order to evolve with the ever-expanding security risks of today's virtual healthcare environment, IT leaders need to rethink how to protect growing archives of data as well as the hardware and systems used to manage it.

In this paper, we will explore a multi-tiered approach to data protection that helps keep costs down while advancing data security and innovation. You will learn how to:

- increase security against ransomware
- reduce long term data archiving costs
- support innovation through seamless refresh cycles and platform upgrades

DATA AND INNOVATION ARE OUTPACING INFRASTRUCTURE

Today's healthcare ecosystem is complex. Data is growing at a CAGR of 36% with information being captured and utilized in multiple formats, languages, geographies and subject to unique regulatory and operational requirements. While many organizations have shifted to the cloud and/or hybrid IT to help manage this complexity, it remains challenging to keep track of where data lives and if it is protected appropriately. This is not only due to the sheer volume of data being created but also the speed at which cyberattacks evolve to exploit data protection gaps as they emerge in the healthcare ecosystem. For example:

Growth is outpacing infrastructure: There are seemingly infinite sources and formats of data and this continues to grow rapidly. At the same time, roughly 60% to 80% of IT budgets are tied up in maintaining legacy applications and mainframe components. In the face of these dynamics, it is extremely difficult for health IT leaders to allocate the full scale of budget and resources required to ensure their data protection infrastructure and policy keep up.

Connected devices are creating new vulnerabilities: The increased adoption of connected devices has advanced the quality of care and transformed care delivery. Yet, it has also introduced new cybersecurity vulnerabilities that elevate risk. Criminals pose a threat to PHI but now also have the means to deploy attacks that put patient health and safety at risk.

Softened security requirements in the wake of COVID: Regulatory bodies relaxed security requirements to enable providers to quickly spin up telehealth and scale COVID-19 testing sites. While this change was necessary to safely and rapidly meet care delivery demands, it has created gaps in healthcare providers' data protection programs that have left them vulnerable to cyberthreats.

THE FINANCIAL IMPLICATIONS

THESE DYNAMICS ARE STRETCHING IT BUDGETS TO THE BRINK.

Storing all data in the cloud is expensive, especially since data is growing exponentially and most of it is inactive – that is, while it may need to be kept for archival purposes, frequent access is unlikely. In addition, most cloud providers and hyperscalers offer one-size fits all storage options that charge fees to ingest data and move data. These solutions also do not offer options for managing legacy systems and data.

With data growing exponentially, IT budgets continuing to tighten, and the increased risk of cyberthreats, the current approach must evolve to keep up.

WHERE DO WE GO FROM HERE?

In order to evolve with the ever-expanding security risks of today's virtual healthcare environment, IT leaders must rethink the manner in which they protect their growing archives of data and the hardware and systems used to manage it. Shifting to a multi-tiered data protection strategy is proving to be an effective means by which healthcare providers can control costs while keeping up with the changing face of cybersecurity threats and requirements.

A multi-tiered data protection strategy addresses archiving, backup, recovery, and cybersecurity requirements by aligning the data protection method to the data use. This approach is founded upon the following tiering best practices:

ACTIVE DATA THAT IS FREQUENTLY ACCESSED SHOULD REMAIN IN A NEARLINE STORAGE TIER.

INACTIVE DATA THAT IS INFREQUENTLY ACCESSED SHOULD BE MOVED TO AN OFFLINE STORAGE TIER.

DEVICES, SUCH AS LAPTOPS, TABLETS AND MOBILE DEVICES, SHOULD BE BACKED UP TO A STORAGE TIER THAT OFFERS FAST RESTORATION AND DISASTER RECOVERY CAPABILITIES.

LEGACY DATA AND SYSTEMS SHOULD BE PROTECTED USING A FULLY-MANAGED SERVICE THAT PROVIDES RESTORATION SERVICES AS NEEDED.

BEST PRACTICE APPROACH FOR AN EFFECTIVE TIERED DATA PROTECTION STRATEGY

Of course, how a multi-tiered data protection strategy is implemented is just as critical to success as the development of the strategy itself.

The first step is understanding the data in your ecosystem - what's active and needs to be readily accessible online and what's inactive and can be stored offline and retrieved by request. Most organizations find that 80 percent of their data is inactive and by moving that data to a cold storage solution - or onto the archive data tier - they can save up to 40% in storage costs.

For active data, cloud object storage is recommended so data remains quickly accessible. Inactive data can be stored offline using a mix of cloud and tape, so data is retrievable via the cloud but secured in air-gapped, cost-effective storage.

Cold storage also provides a defense against ransomware and other cyberthreats. Here's how it works :

- Organization uploads the data on their storage devices (cloud, hard drive, etc.) to a secure storage target (S3 bucket).
- Data is tiered (nearline/offline) based on organizational requirements (i.e. 0-90 days stored in object storage; 90 days and older stored in secure offline storage).
- Data stored nearline is accessible for retrieval via a S3 bucket based on SLAs (within minutes).
- Offline data can be retrieved using multi-factor authentication methods and is also available using a S3 bucket based on SLAs (within hours).

This approach decreases storage costs, reduces risk, and ensures compliance.

> GIVEN THE MANY COMPETING PRIORITIES IN HEALTHCARE TODAY, THE LARGEST CHALLENGES HEALTHCARE PROVIDERS WILL FACE IN INSTITUTING THIS APPROACH IS GAINING THE INTERNAL BUY-IN TO OVERTURN THE STATUS QUO AND THE RESOURCES REQUIRED TO SUPPORT IMPLEMENTATION.

Legacy data can also be migrated to the cloud based on business requirements or it can be protected using a managed service that stores the data offsite and provides restoration tools to retrieve data when needed.

The keys to overcoming these challenges are:

1. Build a strong business case. By effectively transitioning to a multi-tiered data protection strategy that aligns tactic with date type and use, you can generate both hard and soft savings. Run the numbers and capture the associated soft benefits.
2. Find a trusted, neutral advisor with expertise in developing a platform agnostic approach. This will help you seamlessly navigate any obstacles that may emerge due to existing terms such as lock in with your existing platform or vendors.
3. Communicate, communicate and then over-communicate some more. As you know everyone today is challenged to do more with less. That means minds are distracted and resources are stretched. You'll need to get buy-in from the top down to support implementation and clearly attribute roles and responsibilities throughout the process.

TAKING A CLOSER LOOK: CASE STUDY EXAMPLES

This approach has been implemented across a number of healthcare providers and organizations in highly regulated industries across the US. The outcomes consistently prove the multi-tier strategy effective in delivering the following results:

- secure, reliable and accessible archiving that meets retention requirements and is compliant with privacy regulations
- simplified administration of backup and recovery processes
- reduced backup costs with improved data protection
- improved ROI for archiving cloud data when compared to the organization's previous storage approach

THESE FINDINGS WERE PROVEN ACROSS SEVERAL CASE STUDIES:

Case Study 1: An organization faced rising costs of tape backup infrastructure for archival data and wanted to modernize their data protection strategy. Iron Cloud Secure Offline Storage replaced tape infrastructure with a cloud model for long-term data retention, and cost savings on storage, software licenses and hardware while also meeting compliance requirements.

Case Study 2: An organization needed a compliant way to audit cloud backups to validate recovery in the event of a disaster or other trigger event. Iron Cloud Secure Offline Storage provided a way to replicate a third copy of the organization's data to validate the restore and recovery process as well as improve the organization's cloud storage infrastructure, networking and bandwidth with an estimated savings of $120K annually. This approach also ensured compliance with data retention policies.

Case Study 3: Leaders at an organization were concerned that IT costs were out of control due to rapid data growth. They wanted to reduce the burden of managing tape backup infrastructure onsite. Leveraging a mix of cloud storage and data restoration services, they migrated go-forward data to a secure cloud and outsourced the management of tape infrastructure and legacy data. This approach offered $2M in savings, eliminating software and hardware costs and traditional cloud fees (egress/ingress fees).

Case Study 4: An organization had a CIO mandate to modernize IT and reduce IT costs while mitigating security and compliance risks. Leveraging a multi-tiered data storage approach that included Iron Cloud Secure Offline Storage (data aged 3 months to 7 years), Iron Cloud Object Storage (data aged 0 to 3 months) and Data Restoration and Migration Services for legacy systems and existing tape backups. More than 250TB of data is now tiered based on how it is used, reducing storage costs by more than 50%.

CONCLUSION

A multi-tiered data protection approach that strategically aligns data use to the tactic of management can help healthcare organizations:

- **Keep Up With Data Growth.** Healthcare data will experience a CAGR of 36% through 2025 (IDC). Using a multi-tiered approach can help ensure data is in the right place at the right time without breaking the budget.
- **Save Money.** With roughly 60 to 80% of IT budgets spent on maintaining legacy applications and mainframe components (Becker's Healthcare), establishing a cold storage tier can help organizations get control of long-term storage costs by archiving inactive data and retiring onsite storage hardware and legacy backup infrastructure.
- **Improve Security.** The healthcare sector has spent more than $160 million on ransomware recovery in the last four years (Health IT Security). Healthcare organizations can increase security against ransomware and other cyberthreats with an air-gapped gold copy of data stored offline.
- **Strengthen Compliance.** Ransomware attacks are known to cause data loss with data breaches costing more than $7 million dollars each year (Health IT Security). By storing inactive data offline with fast retrieval options, you can adhere to long term data retention requirements while significantly reducing risk of breach.

IRON MOUNTAIN®

800.899.IRON | IRONMOUNTAIN.COM/SOS

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.

USHLT-SB-021221A