OROCK TECHNOLOGIES

For the Healthcare Industry, It's (Past) Time To Modernize Your Storage Solution

Table of Contents

For the healthcare industry, it's (past) time to modernize your storage solution

Overwhelmed by a perfect storm — explosively growing data use, crippling cyber-attacks, and a pandemic that's stressed operations to the breaking point — many health providers are turning to the cloud to protect their data and keep their storage costs under control. The good news is that migrating to a cloud storage solution is not only a lot easier than expected, it can help providers win efficiencies and new flexibility, while greatly enhancing their security.

There's no escaping the tsunami of data that now overwhelms every enterprise. But for heavily regulated industries like healthcare, having the proper storage solution is more than a matter of efficacy or even basic security: it's a matter of long-term survival.

And providers face unique pressures, especially now. The COVID-19 pandemic has wreaked havoc on their operations — stressing staffing, systems and revenue as never before — and IT departments, under pressure to cut costs and keep a lid on headcount, are stretched thin.

Unfortunately, those budgetary pressures have coincided with a rash of high-stakes, highly publicized ransomware attacks that have crippled hospital systems of all sizes: since 2016, such attacks have cost U.S. healthcare organizations $157 million, with the average ransom payment across all industries skyrocketing to more than $230,000 — and small-to-medium businesses the most vulnerable targets. More than 700 providers were hit by ransomware attacks in 2019, a number expected to quadruple by the end of 2020.

Of course, in healthcare the damage of lost data can't be measured in financial terms alone — it's also measured in human, reputational, legal and regulatory cost. Conscious of the special vulnerability of industry providers, some cybercriminals have begun to take the extortion to the next level: threatening to publicly reveal the protected health information (PHI) of patients if the ransom is not paid — an event that would then trigger the Department of Health and Human Services (HHS)'s HIPAA Breach Notification Rule.

Legacy technologies confront modern realities

When it comes to cyber risk, the trend is clear: it's less a matter of if than of when. Unfortunately, compared to other service sectors, the healthcare industry has been late to the digital-transformation party — and that innovation lag has become a drag on growth, operational bandwidth and security.

Consider the issue of how to handle the ever-thickening torrent of daily data — including electronic health records (EHR), PHI, medical imagery, clinical and wearables data, telemedicine records, pharma data and healthcare provider (HCP) information — required to operate. Consider, too, that our era of consolidation has led to an expansion of regional providers with multiple locations. Yet many providers still employ legacy, on-premises technologies with limited capacity for storage and backup — solutions which are increasingly unsuited to today's data realities and risks.

If all storage facilities are on-premises, the exponential growth in data means businesses must constantly keep expanding their data center(s) simply to keep up, in a perennial cycle of undercapacity. That means not only being solely responsible for the security of data and the underlying infrastructure — including technology refreshes, security upgrades, patches, etc. — but also for hiring a team to operate and maintain it 24/7. Conversely, some overspend on capacity, just to deep-store data that may never be needed again.

Clearly, for many providers, it's past time to update their data storage solution — not only to scale their infrastructure and protect their data, but also to gain the flexibility and efficiency they need to compete in an increasingly complex marketplace.

For a historically risk-averse, resource-constrained industry facing a once-in-a-lifetime pandemic with legacy technology, that is easier said than done. The good news is, it's also easier than many think.

With the cloud, necessity meets opportunity

Most midsize providers understand (at least in the abstract) that a cloud solution could help solve their capacity, backup and cost issues. But in our experience, many tend to underestimate the need — and overestimate the costs and risks — of a cloud storage strategy. Or they are simply uncomfortable with the cloud mindset.

Here's the reality: A storage solution that incorporates the cloud does not mean losing control of your data. It means future-proofing it, by expanding your capabilities and safeguarding your data — while lowering costs.

The process starts with assessing your current situation. What are you running now, on site? Where is your mission-critical data? What, if any, backup solutions do you have? What are your immediate and future needs? What do you need to keep where — from hot active storage to longer-term archiving?

If a ransomware attack or physical disaster were to hit you tomorrow, would you be able to quickly recover all your critical data and keep the lights on?

No matter the industry, there's no escaping the cloud: In late 2018, Gartner predicted that 80% of enterprises will use cloud-based infrastructure by 2025. A sophisticated cloud service provider can help you assess your unique needs, create customized, scalable, flexible options for your storage and applications — and enable you to make rational ROI decisions on what data can and should be moved to the cloud.

WHY SOME HEALTHCARE PROVIDERS ARE SLOW TO ADOPTING CLOUD COMPUTING

"We have it all on-premises, don't need a secondary copy."

"The cloud is too expensive, and startup costs are likely to be too high."

"The cloud is not secure, my board will never allow it."

"I can see the need, but the C-Suite will see it as a cost center."

"What if there are hidden charges when we really need to get our data?"

"What if we end up tied to a system that simply doesn't work for us?"

Future-proof your storage solution: Focus on competencies, not infrastructure

Cloud computing can lower costs and expand your capabilities, by enabling you to focus on competencies instead of IT and infrastructure. Crucially, it can also bring visibility, predictability and control into your financial planning — while offsetting some of your CapEx (capital expenditure) through an OpEx (operational expenditure) model.

The new EHR framework that's poised to change your IT practices

There's a quiet revolution going on with electronic health records: a next-gen framework called Fast Healthcare Interoperability Resources (FHIR). FHIR is a new, API-based standard designed to facilitate the seamless sharing of electronic health records across a wide variety of digital devices.

FHIR allows developers to create and integrate new medical applications into existing systems: another example of how cloud computing can help even smaller providers future-proof their data practices.

It's hard to underestimate the benefit of Infrastructure as a Service (IaaS). Public cloud storage is typically built on the latest-generation storage technologies with constant security and performance monitoring included. It takes the burden off of your organization's IT staff for managing the physical data center, hardware, software and monitoring. And importantly, it addresses the crucial capacity and scaling issue, giving you the flexibility to expand or contract when storage requirements dictate.

Storage is only the beginning of what you can accomplish with a hybrid cloud solution. Data is more than static stuff to be stored away: it is also increasingly the lifeblood of business — a strategic asset where data transfer is a two-way street, and data liquidity (how easily and securely it can be transferred) is central to the kind of interoperability that could unlock some of those benefits.

Storage best practices: As simple as 3-2-1

With the rise in data risk, proper information governance practices are essential. That starts with clarity on the different types of data you have — its purpose, proper location, retention periods, and how frequently you may need it for the short term. Regardless of where it resides, job number one is to safeguard your valuable data against any failure.

The 3-2-1 rule is a well-established practice for backing up your data, and ensuring its integrity under virtually any scenario. The essential principle is that organizations should have at least three versions of their data stored on at least two different forms of media, and one copy being off the physical premises. Typically, you would secure your first copy on your primary storage, back up a second copy on a different media (such as a tape drive or backup appliance) and keep the third copy off-site, such as via a cloud storage provider.

Critical in this age of ransomware, where hackers aim to compromise servers rather than just one device, is maintaining an air gap between your first and "off-prem" copy — essentially an unbreachable, physical separation between the two repositories

— hence sending the data to the cloud. Some backup solutions don't include an air gap: they simply back up snapshots in the same account as the primary system, making it possible for a hacker to steal or encrypt both copies of the data. That's why having an air-gapped, off-prem copy is important.

Following this best practice greatly enhances your organization's ability to recover from unexpected events such as data corruption caused by malware or ransomware, hardware failures, or data center outages, natural disasters such as fire, flood or earthquake. Crucially, it can also demonstrate compliance with data-privacy laws such as HIPAA.

ORock Technologies: Own your own cloud solution… safely, securely, strategically

Security, innovation and cost control aren't mutually exclusive — in fact, when coupled with the right cloud solution, they reinforce each other.

Midsize healthcare providers have specific data storage needs that require not only the highest standards of security and compliance, but also knowledgeable, attentive service — from design of the storage solution to migration and rollout, to maintenance and day-to-day support. They need to be able to quickly scale up or down as circumstances dictate. They need to maintain control over their environment: no vendor lock-ins to tie their hands when flexibility is called for.

And they need common-sense, cost-effective, predictable pricing.

These specialized needs go far beyond the remit of the mass-market brand names of Big Storage, where transfer and egress fees can quickly overwhelm the per-gigabyte cost of active and static storage — and where nobody answers the phone if you need help.

Between the onslaught of ransomware attacks, the cash crunch, and the endless need for more storage, healthcare companies know they have a decision to make. The wisest will look at the converging crises of today the strategic way: as opportunities in disguise. By modernizing your storage solution and transforming your cost structure, you also increase your flexibility, enable operational improvements — and put yourself in an infinitely better position to handle crises.

ORock Technologies is perfectly positioned to deliver the customized solution you need. With our government-grade security and compliant FedRAMP, HIPAA and HITECH certification, we specialize in working with heavily regulated, security-focused industries like healthcare.

We can help you modernize your healthcare-data storage solution — and win the efficiencies, security and resilience you deserve… today and tomorrow.

For more information on ORock's healthcare capabilities, please contact:

Don Poole
(571) 386-0201, ext 309
dpoole@orocktech.com