Business White Paper

Healthcare Cloud Backup & Disaster Recovery:

5 Considerations & Best Practices

ClearDATA
SECURE • HEALTHCARE • CLOUD

Healthcare Cloud Backup & Disaster Recovery:

5 Considerations & Best Practices

Table of Contents

Information technology outages and failures at the enterprise level are extremely costly for all organizations; in the healthcare space, those outages can be catastrophic on multiple levels. According to the Ponemon Institute, the average cost of a data center outage has risen from $505,502 in 2010 to $740,357 in 2016, a 38% increase. Depending on the scope of the issue and systems affected, an organization could lose thousands of dollars per minute through the loss of data or access to applications.

For healthcare organizations, those costs are compounded by the impact on patient safety and the ability of caregivers to effectively administer treatment without access to key clinical applications and electronic chart data. While hospitals and other providers typically have emergency plans in place, falling back on manual methods could result in clinical or medication errors. IT failures can also bog down the continuum of care, from admissions through treatment to discharge.

That's why data and application back-up and disaster recovery solutions are so important in healthcare. They not only ensure access to critical applications and data, they are also required under provisions of the Health Insurance Portability and Accountability Act (HIPAA) and other legislation.

Increasingly, healthcare organizations are turning to public cloud solutions for their back-up and disaster recovery needs. According to Markets and Markets, global adoption of cloud services in healthcare will grow from $3.73 billion in 2015 to nearly $9.5 billion in 2020. The 2014 HIMSS Analytics Cloud Survey found that 83% of healthcare provider organizations were using cloud services. The majority of these implementations involve the public cloud. The study also found that found that 77 percent of healthcare IT executives planned on moving additional systems to the public cloud within the next year.

The transition to the cloud has been driven, in part, by the increasing pressure placed on healthcare IT departments as they struggle to keep pace with demand for storage and compute capacity. With the expanded use of electronic health record systems, online patient portals, advanced imaging systems, and other new technologies, the volume of data and need for large amounts of storage has exploded. Many hospitals, insurers, and other stakeholders have also invested in big data and analytics solutions to better utilize that data to conduct research and improve patient outcomes.

By using cloud resources for storage and application hosting, healthcare companies can eliminate or reduce the burden of purchasing, securing, and maintaining their own servers and data centers. They have access to storage and compute capacity that can be rapidly scaled up or down depending on their needs, as well as to on-demand services that can be fully managed or DIY. The public cloud also makes it easier to address geographic diversity by providing secure, centralized access to data and applications across multiple campuses and for partners in different areas of the country.

Cloud-based disaster recovery is also a critical component in data security. While many disruptions are due to natural disasters or technical failures, there has been an increase in ransomware and similar attacks in the healthcare industry. These attacks are costly, can damage an organization's brand, and even after the issue is resolved the company is still vulnerable to future attacks. With a cloud-based back-up that is isolated from the live data source, companies have more options to successfully deal with these attacks because they have a safe copy of their files and applications separate from the ones affected by the ransomware encryptoin.

All of these benefits reduce the costs of managing the IT infrastructure, while shifting the remaining costs from capital expenditures (CapEx) to more manageable and predictable operating expenditures (OpEx). Costs remain low, while IT flexibility is greatly increased.

Cloud Backup & Disaster Recovery Basics

Disaster recovery and back-up are two related but different concepts. Data back-up simply means that you have created a copy of your data on another device or at another location. Disaster recovery is the ability to recover all files, software, and functionality as quickly as possible. In the case of a server or data center failing, just having a duplicate of your files is not very helpful. Disaster recovery gives you the ability to rebuild a server or group of servers to restore all of your files and all of your application functionality.

It's also important to distinguish back-up and disaster recovery from replication. Replication a real-time process that creates an ongoing, continuous back-up. Replication is typically reserved for essential applications or data because of the prohibitive expense associated with this type of process. In a healthcare environment, Tier 1 applications like the electronic medical record (EMR) may require replication.

While disaster recovery is critically important, especially as healthcare organizations are increasingly the target of hacking and malware, many companies do not have a detailed disaster recovery plan. They may not have a second site established for encrypted data, or no plan for Tier 1 application outages (including patient and physician notifications). However, the most recent HIMSS Cybersecurity Survey indicates that spending has increased in this area.

When evaluating cloud-based disaster recovery services, there are two key measures that are important to look at: the recovery point objective (RPO) and recovery time objective (RTO). These will tell you how long it would take to fully restore the affected systems and how large of a gap there would be in your data set from the time of the failure to the point of restoration.

Generally, the public cloud offers highly scalable, flexible, on-demand services that can better meet the RTO and RPO objectives of healthcare organizations. They can also provide a more affordable and manageable alternative to managing these processes in house.

Below, we've outlined five key considerations and best practices for utilizing the public cloud for back-up and disaster recover services.

1. Determine RTO and RPO Objectives

For most healthcare organizations (particularly hospitals or providers), the RTO should be as brief as is possible in order to ensure a seamless transition from the failed IT infrastructure to the new resources. This will minimize operational disruptions.

To reiterate, the recovery point objective (RPO) is the maximum tolerable period in which data may be lost from an IT service. It is the point from which the data ceases to be current. For example, if you backed up data from a device two hours ago, the RPO would be the data state from that time.

The recovery time objective (RTO) is the time within which you want business processes or systems to be restored after a failure or disruption. The RTO is how long it will take to restore the affected systems in order to avoid additional costs and negative consequences.

By running applications in the public cloud and subscribing to offsite back-ups at a second data center for disaster recovery purposes, healthcare organizations can build multiple recovery plans that optimize both RPO and RTO in a way that is affordable and ensures a secure and timely response to data center outages or disruptions.

While cloud services don't intrinsically change the RPO (back-up timing would be dictated by the organization's needs and other requirements), they can have an impact on the duration of the RTO. You can bring systems online faster in the cloud than if you had to install a new server at an in-house data center. Potentially, the cloud allows you to bring systems back on line and restore them much more quickly and with much less effort.

While duplicating your data and application environment may sound costly and complex, there are now a variety of approaches that can provide full recovery while minimizing the required resources.

One approach is to use a "pilot light" infrastructure, offered by Amazon Web Services, which make a copy of the configuration on a small server. The data is regularly copied and kept up to date. That server operates in the background, essentially in an "off" state, at a relatively low cost.

When there is an outage event, the size of that pilot light server can be expanded to production capacity for disaster recovery, while bringing up alternative web and application servers in the cloud. The environment can be turned on at full size. That provides much faster RTO but without the cost of paying for two environments simultaneously. There are also "hot standby" environments that enable rapid failover.

It's also important to note the difference between disaster recovery and maintaining a high-availability (HA) environment. There will always be a gap between the data as it was when the failure occurred, and the status of that data and systems once the restoration is complete.

A high availability design minimizes disruptions by providing IT continuity through redundant or fault-tolerant components. In other words, HA designs keep systems running even when parts of the IT environment are not available; disaster recovery allows you to restore the environment to its state at a certain point in time prior to the failure.

Both HA and disaster recovery systems should be regularly tested to validate failover and recovery processes, and to ensure that there are no issues with certificates, paths, firewall ports, permissions, ad other elements.

2. Identify Critical Systems & Dependencies

Data and applications aren't the only things that have to be backed up or replicated in the public cloud. Just as important are the dependencies of those critical services, such as databases and middleware, and the protocols employed when those systems interact. Those dependencies must be protected in the public cloud.

To effectively migrate these systems and services to the cloud, you have to have a clear fundamental understanding of what those dependencies are to ensure they are replicated accurately within the cloud infrastructure. That means the cloud instance needs to be configured so that applications start in the correct order, i.e. making sure the database is up and running before applications launch, and that permissions, certificates, and other elements are maintained.

Applications should also be prioritized by their criticality so that the most important systems are restored first in the case of a disruption. In hospital environments, for instance, clinical systems might take priority over inventory management; at an insurer, claims processing might trump HR applications. There are costs associated with the speed at which each system can be restored, so only the most important applications or servers should be given those shorter RPO and RTO parameters.

Applications may also need to talk to systems at third-party locations. For example, a hospital may need its applications to communicate with a company that provides prescription fulfillment. The machines in the disaster recovery environment should be able to talk to those third-party services as soon as they go live.

The cloud service provider can take "snapshots" of the servers themselves, so that the cloud environment is a "like for like" copy of the original infrastructure.

3. Consider Requirements for Targeted Recovery

Users tend to think of disaster recovery in terms of catastrophic events (natural disasters, security breaches, etc.), and worst-case scenarios in which an entire data center's worth of infrastructure has to be rebuilt from the ground up. But in many cases, recovery may involve a single system, one application, or even a single file.

It is much more common for users to need to restore a corrupted file or application than to bring up an entire server or group of servers. However, traditional disaster recovery approaches often copy all of an organization's data as a large, single file at the secondary location. In order to find a particular file within that larger copy, the user would have to effectively restore the entire package. That's an inefficient and potentially expensive solution.

With a public cloud service, organizations have the ability to copy files over in their original configurations. You can simply search for the specific data you need on the off-site server and restore it.

The same is true for individual servers. You can keep a complete copy of a particular server in the cloud and turn it on when necessary. This is a much more efficient approach, and provides flexibility to your users so that they can identify and restore a single application or file on demand.

4. Big Data & Analytics Workloads

One of the reasons so many healthcare organizations are migrating to the cloud is because the volume of data they have to collect and store has grown so rapidly over the past decade. Armed with this mass of new digital information, hospitals, universities, insurance companies, and other stakeholders are looking for ways to put the data to use.

Big Data and analytics tools are helping healthcare organizations use these large volumes of collected data to identify population health trends, spot emerging outbreaks, measure effectiveness of treatment, and develop better clinical responses more quickly based on empirical evidence. These efforts dovetail with new

requirements for evidence-based treatment and the outcome-centered reimbursement strategies being rolled out by both public and private payers.

However, accessing that information often requires tapping into data sets that are in use daily by clinicians and other staff members. Analytics activities can consume system bandwidth and bog down servers and applications.

Cloud-based back-up and disaster recovery platforms provide a method for data to be encrypted, transmitted and securely stored, and then be made available for alternate data workloads such as warehouse and analytics processing. Instead of accessing the live data being used for ongoing operations and applications, teams performing warehousing or analytics tasks can access the same data without disrupting or straining those operational systems.

This is made possible because data can be stored in its native file formats in the cloud. Data that is copied to the cloud can be attached to a server. A data warehouse can be loaded into an analytics or big data environment from that copy instead of form the original.

Using this approach, healthcare organizations can more easily conduct PHI inventory analysis, big data analytics, cloud-based data warehousing, collaborative care data exchange processes, and large-scale upgrade or infrastructure transformation tests.

5. Security & Compliance

For health IT organizations, security and compliance are the overarching imperatives in any technology initiative. Cloud-based back-up and disaster recovery solutions are subject to the same HIPAA and Health Information Technology for Economic and Clinical Health Act (HiTECH) security requirements as on-premise solutions. In fact, HIPAA requires data to be backed up at an offsite location separate from the location of the original data, making cloud-based solutions an attractive option.

Because HIPAA/HiTECH violations can lead to fines, legal action, and brand damage, managing compliance will require staff and

expertise – something many healthcare organizations may lack. A do-it-yourself (DIY) approach to public cloud management may be a viable option in some cases, but the challenge of budget constraints, keeping up with regulatory requirements and speed to market with new clinical initiatives may make managed services a better approach.

A DIY approach means that internal staff, in addition to their other duties, must spend a significant amount of time ensuring that the cloud environment is maintained in a secure fashion and compliant fashion. Dedicating resources to those tasks can increase the cost of a cloud deployment and erase potential savings.

A cloud managed services provider (MSP) can offer the expertise needed to maintain compliance while freeing internal HIT resources to focus on clinical initiatives. The MSP can also provide guidance and support for failover and disaster recovery planning.

The MSP can provide 24/7 monitoring of all applications, users, and servers. A Health Information Trust Alliance (HITRUST)-certified provider can offer compliant and secure client-side and service-side data encryption and network traffic protection, along with anti-virus protection for each customer instance. MSPs can also provide multi-factor authentication, network monitoring, intrusion detection, and hardware/OS patching and updates, and other capabilities.

The MSP can also ensure that the solution remains in full compliance with HIPAA, HITECH, and other regulatory requirements. Using a HIPAA compliance dashboard, organizations can have visibility into how their systems compare to regulatory requirements by mapping each asset against the HIPAA CFR. This type of MSP-provided solution can also provide a real-time compliance audit trail.

Those capabilities and expertise may not be available within an organization's HIT department. As such, working with a cloud MSP for back-up and disaster recovery can relieve the internal IT department of these additional responsibilities, while also providing better assurance that security and compliance efforts are up to date.

Conclusion

Back-up and disaster recovery solutions offered in the public cloud provide the scalability and service options to meet almost any need, from large scale recovery caused by a catastrophic event, to the recovery of a single file or application caused by human error.

Cloud-based solutions also provide a variety of disaster recovery options that can optimize both the recovery point objective (RPO) and recovery time objective (RTO) goals of a healthcare organization. With their ability to cost-effectively provide large amounts of data storage and computing capacity, cloud-based solutions can help healthcare organizations rapidly restore data and applications, and minimize costly and potentially dangerous disruptions to their operations.

Using a cloud back-up/disaster recovery system that provides for data to be encrypted, transmitted and securely stored in native file formats can also improve big data and analysis initiatives by allowing backup data to be made available for alternate data workloads such as warehouse and analytics processing.

As with any HIT initiative, security and compliance are paramount for back-up and disaster recovery solutions. A cloud-based approach should ensure the necessary data encryption, as well as full compliance with HIPAA, HITECH, and other requirements. While some large healthcare organizations can handle these requirements in the public cloud, a managed services strategy may be the best approach to keeping on top of regulatory requirements and potential security breaches while giving internal staff more time to focus on clinical initiatives.

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

1600 W. Broadway Road, Tempe AZ
(800) 804-6052
www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD