Business White Paper

Best Practices in Healthcare IT Disaster Recovery Planning

Leveraging the cloud to enhance compliance, improve recovery objectives, and reduce capital expenditures

ClearDATA
SECURE • HEALTHCARE • CLOUD

Best Practices in Healthcare IT Disaster Recovery Planning

Table of Contents

Executive Summary

As a healthcare organization, you face a mountain of responsibilities when it comes to dealing with electronic patient information. You need to comply with government mandates, protect the privacy of your patients, and ensure critical data is available to clinicians in the event of downtime or disaster. And in order to maintain patient care standards and meet business objectives,you need to do it all faster and with a limited capital budget.

In recent years, the cloud has matured, becoming a viable option for healthcare data backup, and offering multiple deployment models that can get you out of the data center business and back to the business of treating patients – with better data recovery metrics and an OPEX pricing model that saves budget resources and maximizes your reimbursements.

This white paper will help you assess your readiness, determine the best deployment option for your organization, and map out the steps required to get there.

Modern Healthcare Organizations Face a Variety of Challenges

The pervasiveness of electronic health records (EHR) has been an incredible boon to the healthcare industry. These digital files make it much easier to access and share medical information, and thus dramatically improve the quality of patient care, as well as lower costs through efficiency gains. But they also create multiple responsibilities around managing and protecting patient information – called protected health information (PHI) – against theft, loss or disruption.

The following are some of the major issues healthcare organizations face relating to planning for disaster recovery and business continuity:

Clinicians need fast access to patient data at all times

Disasters and unexpected downtime are a fact of life. And business continuity is especially important for healthcare organizations; the worse the disaster, the more critical it is for you to get back in business quickly with accurate, up-to-date patient records.

Regulations and requirements abound

Because of the sensitive nature of EHR, a vast array of regulations and requirements has sprung up around PHI, mandating how your organization handles private patient data. For example, the HIPAA act alone requires your organization to implement data safeguards that impact every aspect of your operation, from the bedside to your business partners. And that's just one of the regulations and requirements you are subject to follow.

Are you in compliance?

Just a few of the regulations and requirements you may be subject to include:

- The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule
- The American Recovery and Reinvestment Act (ARRA), specifically the 15th core criteria for Stage 2 Meaningful Use
- The Health Information Technology for Economic and Clinical Health (HITECH) act

Big Data and bring your own device impacts are real and growing

Add to all of this the fact that the amount of PHI you deal with is immense –and growing fast – especially when it comes to medical imaging and picture archiving, and communication systems(PACs) data. And data is likely to exist in your facility, as well as on your clinicians' laptops, tablets or phones. According to a recent healthcare survey, 66 percent of respondents believe that supporting bring-your-own-device (BYOD) mobile technology is changing the future of patient care delivery.[1] At the same time,your backup requirements may be growing as well; many healthcare organizations are required to store PHI for a staggering seven to 20 years.

The budget isn't growing as fast as protected health information

Healthcare is a business, and the pressure is always on to reduce costs. But despite the enormity of PHI and the challenges of storing and protecting it, the budget isn't getting any bigger. In fact, many healthcare providers find themselves cash-strapped after complying with the first round of ARRA Meaningful Use requirements.

[1] HIMSS survey: "Health IT Leaders High on Mobile," December 2012

There is a better way

All of these factors put increasing pressure on your entire organization – especially IT – to provide business continuity and disaster recovery(BCDR) plans that answer all of the above challenges. This is leading many healthcare organizations to look for ways to get out of the IT business and get back to the business of treating patients.

These organizations are seeking new ways to deploy cost-effective,yet robust, secure and scalable solutions for BCDR. Many of them are turning to the cloud to deploy a consistent, centralized and standardized backup and restore architecture that will reduce costs and risks.

But moving to the cloud is not a decision to be undertaken lightly. To get the maximum benefit from a cloud strategy, it needs to be designed in light of your organization's specific requirements and capabilities. And before you can even begin to consider moving to the cloud, you need to understand what cloud services for healthcare BCDR involve.

Cloud Business Continuity and Disaster Recovery Services for Healthcare

Many healthcare organizations currently handle BCDR in-house using tapes and other physical media. But in recent years, improvements in cloud security – coupled with staggering increases in the amount of PHI that must be stored and protected – have led organizations like yours to consider using the cloud for some aspects of BCDR. Some of the main reasons include:

Easier HIPAA/HITECH compliance

Moving to the cloud with a provider that is HIPAA-compliant and well-versed in the requirements of the healthcare industry will make it easier to ensure you are maintaining compliance with current and emerging regulations.

What is "the cloud"?

At a basic level, "the cloud" is an Internet-based environment of computing resources comprised of servers, software and applications. Cloud solutions can be private, public or a combination called "hybrid cloud." To find the approach that is right for you depends on your requirements and readiness.

Better recovery objectives

While off site, offline or nearline physical media storage will protect data, these solutions offer recovery time objectives (RTOs) of several hours to several days and recovery point objectives (RPOs) of a day or more depending on your backup schedule. While online backups are the fastest for restore, in the event of a large disaster the online backups may likely be lost as well. To mitigate that risk,online cloud backups, while somewhat slower for return on investment(RTO), provide protection that may be worth the trade-off depending on your specific requirements.

Understanding recovery objectives

Recovery time objective (RTO): how long it takes to recover data after a disruption

Recovery point objective (RPO): how recently the data was backed up (i.e. how much data will be lost in a recovery event)

Moving expenditures from CAPEX to OPEX

Shifting BCDR initiatives from capital expenditures – related to purchasing equipment – to operational expenditures via a cloud service model delivers multiple benefits, including lower upfront costs, budget predictability and the ability to have 100 percent of the cost reimbursed through your Cost Report.

Fast deployment and enhanced scalability

An established cloud provider can provision resources for your organization very quickly. And cloud resources can be scaled up or down as needed with tremendous flexibility.

Is the cloud secure enough for PHI?

The cloud offers price and performance benefits that are enabled by sharing infrastructure, which is referred to as "multitenancy." For the healthcare industry, the main concern with multi-tenancy is ensuring that proper security and isolation procedures are in place to protect PHI from loss, misuse or privacy violations. Secure multitenancy technologies today are robust enough to protect sensitive PHI, making the move to cloud possible – and even advantageous – for healthcare providers.

Getting out of the data center business

With cloud services, you can rely on an expert partner that is well versed in the technical aspects of BCDR, who delivers on your requirements for increased performance, security, storage space,cost requirements, and so on. You can also cut costs related to staffing and supporting in-house operations and let your IT staff focus on initiatives that enhance patient care.

Best Practices in Business Continuity and Disaster Recovery for Healthcare Organizations

The cloud offers tantalizing benefits for BCDR, and cloud technology and security techniques have advanced to the point where the cloud is even more secure against data breaches and losses than your own data center. However, the options for moving BCDR into cloud are many, and the healthcare industry has very particular needs around data protection and recovery objectives. Ensuring you get the right solution requires a formal approach to selecting and validating your solution.

Follow this step-by-step process to assess your readiness, determine the best deployment option for your organization and map out the steps required to get there.

Step One: Health-check your existing BCDR environment

The best way to start planning for a BCDR strategy that adequately safeguards PHI is through an IT health check. This will help you critically assess where you are now, what's working well and what needs to be improved, clearly spelling out existing and near-term issues. A thorough health check includes:

1. Risk Assessment Check

Assess the risk to your organization if any of the applications you rely on were to become unavailable. When making your calculations,keep in mind local recovery versus remote recovery options;remote recovery will extend RTO by nature, unless the environment is protect by replication technology as opposed to data backups. Steps include:

- Identify all critical applications
- Calculate the clinical risk for each application if it were to go down

- Calculate the impact, in dollars, for each application if it were to go down
- Document how each is being backed up and protected
- Determine how long it would take to recover each application under the current BCDR strategy
- Determine your desired RTO and RPO for each application
- Compare your desired RTO/RPO targets to the current state to determine your exposure gap
- Document readiness of downtime procedures, including training and testing

2. IT Performance Check

Examine the speed and efficiency of your current backup and recovery system to identify bottlenecks and improvement strategies. Specific checks include ensuring that:

- Data is backing up within your windows
- In-house IT staff is meeting operational-level agreements (OLAs)
- RTO/RPOs are established per application, and the recovery plan is monitored to meet or exceed these objectives

3. Backup Integrity Check

Next, analyze your file systems and databases to determine if data is at risk. Specific steps include:

- Tracking backup success and failure rates
- Tracking and resolving failed backup jobs
- Ensuring backups are recoverable through testing
- Checking that recovery capabilities are granular to the file level
- Ensuring that data is protected "at rest," that is, encrypted on your storage medium or target

4. Restore Capabilities Check

This is the time to assess your BCDR plans to determine whether you have the right processes and capabilities to restore PHI in the event of a disaster. Specific checks include:

- Ensuring there is a formal recovery plan in place, including the switch from downtime procedures back to information systems and the needed resynchronization
- Testing BCDR systems and processes on a regular basis through live tests and table-top scenarios
- Analyzing operational recovery procedures
- Evaluating data integrity and recoverability readiness, including sequence or restoring and restoring interfaces
- Doing a gap analysis of recovery goals versus capabilities
- Ensuring there is redundancy built into your systems
- Identifying new applications in the environment and updating your risk assessment
- Identifying any retired systems and confirming that they have been removed from your BCDR platform and plan

5. Other considerations

- How much time is your IT staff dedicating to backup activities?
- Is there a hardware refresh or other IT capital expenditures on the horizon?
- Are you looking at adding more storage capacity in the near term?

The answers to these questions will provide more insight into how moving to the cloud can benefit your organization in very specific areas. At the end of this health check, you will have a clear snapshot of your current capabilities and an understanding of where you need to increase the efficiency and reliability of your backup systems and restore procedures.

Step Two: Perform an impact analysis

Moving your BCDR operations to the cloud is a process that can be accomplished in multiple steps. Determining which aspects of your operations you should move to the cloud – and when – can be accomplished with an Impact Analysis. This is an important exercise that helps you determine which functions are the most critical for your organization and will help guide your adoption strategy.

Start out by defining the costs, benefits and risks associated with moving aspects of BCDR to the cloud. Be sure to consider these major impact points:

- Financial/budget
- Personnel
- Technology
- Business processes
- Compliance
- Security
- Patient care/clinical
- Innovation/growth
- Other elements that you determine are critical for your organization

This will give you a clear picture of your current state of cloud-readiness, and lead you to a step-by-step strategy for moving to the cloud by highlighting:

- BCDR elements that can be migrated right away for immediate benefit
- BCDR elements that can be migrated in the near future
- BCDR elements that may not be a good candidate for cloud at this time but may be in the future as your business environment changes

For example, moving all backup activities to the cloud might have a positive impact on all of the above points with very few drawbacks,making it a good candidate for moving to the cloud right away, while moving business continuity to the cloud may require more preparation due to the technological, personnel and business processes impacts.

Step Three: Outline your solution requirements

Once you've determined which processes are good candidates for the cloud, you can begin to outline your solution requirements. Keep in mind that any solution will impact your organization from a business perspective and an IT perspective, so be sure to gather the requirements from each set of stakeholders. Then outline your requirements with as much specific detail as possible, including:

- RTO/RPO targets for specific applications
- Any application-specific backup requirements (e.g., MEDITECH, Epic, etc.)
- Regulatory requirements that impact cloud providers (business associates agreement [BAA], High Trust certification, etc.)
- Assurance that data is protected in motion and at rest
- Expectations around BCDR testing and remediation
- Solution deployment time lines
- Required features such as:
    - The ability to securely share PHI within your own network, on healthcare exchanges and with service providers
    - Support for mobility and BYOD
    - Granular search and restore capabilities
- Resource requirements such as:
    - IT resource requirements
    - Cost/budget requirements

The results of this exercise can form the basis of a request for proposal (RFP) that you can send to vendors so they can respond directly to your requirements with specific information on their capabilities. But be careful to create a list of solution requirements based on your own criteria.

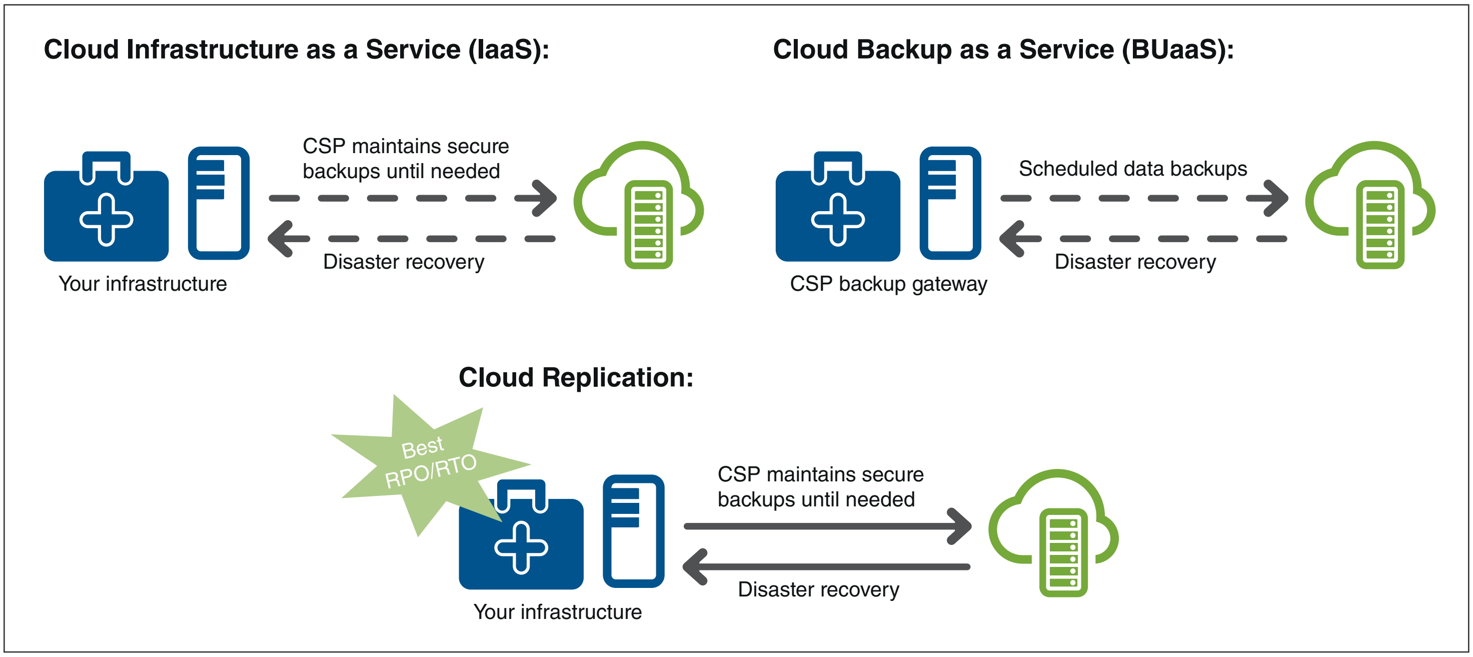
Step Four: Map your requirements to available deployment models

Now it's time to match your solution requirements to the various types of cloud-based solutions available. There are a variety of options available from a fully in-house, private cloud solution to a fully-hosted solution and points in between. An ideal scenario for your organization may be a mixed approach based on the application. If your goal is to restore a lost file or just one server, local or cloud backups is fine. If your goal is to protect the data foremost and the application second, cloud backup is ideal. If your goal is rapid recovery of the application to restore function to end users, consider a Cloud Replication solution.

Which solution type you select depends on your unique requirements. For example, you may wish to maintain control over certain aspects of your strategy, but move others – like backup – to the cloud right away.

Some options include:

- Cloud Infrastructure-as-a-Service (IaaS): This cloud service offering provides a remote, secure repository for backed-up data. You own and manage your own backup software and hardware and just send a copy of data to the cloud service provider (CSP), then retrieve that data as needed. This complete backup solution is managed and owned by your organization.
- Cloud Backup-as-a-Service (BUaaS): In this scenario, the CSP delivers a complete backup solution at your site that provides failover capability to their cloud data center. They own and manage the entire process from beginning to end.
- Cloud Replication: If you have critical applications that need maximum protection with short RTO and little-to-no loss on RPO,you will want to consider replication as opposed to backups. Replication will continually update data and application state to the cloud, providing the most aggressive plan for rapid recovery. An experienced healthcare cloud service provider can help you understand the nuances and design the best mix of deployment models for your needs.



Step Five: Determine your vendor selection criteria

Now that you know what you are looking for, it's time to match vendor offerings to your requirements. Expect vendors to address all of your requirements, and then narrow down the field based on criteria such as the vendor's ability to:

- Demonstrate experience and expertise in the healthcare industry,including HIPAA compliance, High Trust certification and willingness to sign the highest level of BAA that includes the latest HIPAA omnibus rule
- Provide a Tier III data center environment that is SOC II and III and SAEE 16-certified, as well as HIPAA and PCI compliant
- Guarantee service-level agreements
- Provide set response times depending on the risk to your organization (emergency, urgent, standard and so on)
- Provide RTO and RPO targets that meet your risk assessment guidelines
- Deliver 24x7x365 live healthcare-level support
- Quickly provision additional services as necessary
- Provide a proof-of-concept so you can test your solution before committing

- Make recommendations to maximize the return on your current storage investment
- Demonstrate the ability to encrypt any data stored within the cloud with the most recent technologies such as full disk encryption, volume and virtual disk encryption, or file/folder encryption

Conclusion

When you're thinking of changing your BCDR strategy, you need a confident answer to the question: "Are we ready to outsource some or all of our BCDR operations to the cloud?"

On the business side, you need to ensure that any solution will enable you to:

- Maintain high standards of patient care
- Ensure that accurate, up-to-date patient data is available to clinicians at all times across multiple facilities on health information exchanges and mobile devices
- Protect your organization from liability and fines that may result from non-compliance with government regulations
- Manage your budget with an eye to the bottom line

From a technical standpoint, you need to ensure that any proposed solution will enable you to support the business objectives outlined above, which requires:

- Backing up and restoring massive amounts of data
- Optimizing bandwidth requirements
- Working within IT budget constraints
- Protecting data at rest, as well as when it moves across facilities, exchanges and mobile devices
- Selecting the best method for storing and restoring applications and data to ensure business continuity in case of disaster

A solution that meets both business and technology challenges will allow you to maintain compliance with government mandates,as well as provide excellent care for your patients while simplifying IT management and lowering capital expenditures. How much of your operations you move to the cloud will depend on your requirements and your readiness.

Using the steps outlined in this white paper will give you a better understanding of where you are, where you need to be, and how to get there.

For more about Best Practices in Business Continuity and Disaster Recovery for Healthcare please visit www.ClearDATA.com

To speak with a healthcare security consultant please call (800) 804-6052

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 platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

101 West 6th Street, Suite 310, Austin, TX 78701, United States ⌂
(800) 804-6052 ☎
www.cleardata.com 🌐

ClearDATA
SECURE • HEALTHCARE • CLOUD