A Guide to Healthcare IT Disaster Recovery

How to prepare for and mitigate unforeseen events in your datacenter

INSIDE:

INTRODUCTION: Delivering Highly Available Patient Care
CHAPTER 1: Expect the Unexpected
CHAPTER 2: Start with an Intelligent and Virtual Foundation

CHAPTER 3: Disaster Recovery Myths and Realities
CHAPTER 4: Disaster Recovery Best Practices — Top 10
CONCLUSION: A Quick-Start Guide to Disaster Recovery
APPENDIX: Disaster Recovery 101—The Basics
The goal of every healthcare provider is to deliver the highest quality patient care. To provide that care, healthcare IT depends on its datacenter infrastructure and applications to work securely and reliably not just some of the time, but all of the time.

As clinicians demand even more mobile and always-available patient-system access, IT must respond with more automated solutions that ensure reliable day-to-day operations and access to critical patient-care applications—from electronic medical records (EMRs) and ambulatory care systems to picture archiving and communication systems (PACS) and radiology information systems (RIS). To keep healthcare organizations in compliance, robust and highly reliable solutions also must be in place to keep the organization running in the event of unpredicted downtime.

You know VMware as the virtualization company that has been the market leader for the past 11 years. In fact, according to Gartner, more than 80% of all virtualized applications in the world run on VMware today. This ebook highlights the VMware perspective on disaster recovery in the datacenter.

Deploying automated disaster recovery (DR) is the way to protect IT and healthcare organizations from unpredictable events. The following chapters explain the basics of DR and the required infrastructure. They also offer DR hidden realities and best practices with real-world advice.
YOUR DATACENTER IS YOUR CASTLE. That’s where all your critical IT components — hardware, data, and software — reside. You protect it with the latest bulletproof security solutions and make it reliable through redundant multiprocessing, highly scalable platforms, and super-fast optical networks.

And yet, it is not fully protected from forces beyond your control such as natural disasters; man-made events like road closures; security procedures or partner service interruption at a specific site.

Downtime and loss of data, even if temporary, can have long-lasting effects for healthcare providers and can contribute to the demise of the otherwise well-lubed organization:

- Loss of revenue from your inability to treat patients
- Diminished credibility and patient trust, resulting in churn
- Penalties for violated government and industry regulations, such as HIPAA, HITECH and JCAHO
- Costs of recovering and repairing the lost data
- Legal costs of meeting internal and external compliance requirements

How do you balance the disaster recovery risk and investment equation? Is the potential risk greater than the investment? Let’s put it in perspective:

- 43% of companies experiencing disasters never reopen, and 29% close within two years.¹
- 93% of businesses that lost their datacenter for 10 days went bankrupt within one year.²
- 40% of all companies that experience a major disaster will go out of business if they cannot gain access to their data within 24 hours.³

“CIOs and IT organizations should consider scenarios in which normal operations could be disrupted and adopt/adapt practices and technologies that enable them to deal with potential disruption from hostile, external actions as well as internal system failures.”

—Gartner’s Top Predictions for IT Organizations and Users, 2011 and Beyond

The stakes are high, and it is within your power to mitigate the risk.

¹ McGladrey and Pullen
² National Archives & Records Administration
³ Gartner, December 2009
Until reliable virtualization management solutions became available several years ago, DR solutions fell well short of satisfying healthcare organization requirements due to the following:

- High Cost
- Complexity
- Lack of Reliability

With traditional manual DR solutions, the high cost came from the need to deploy a second failover site with dedicated infrastructure, software licenses, and human personnel. The complexity was high because, to ensure the recovery of entire business services, the recovery plans had to manipulate many individual components and moving parts: applications, hosts, network, and storage. The lack of reliability of these procedures was diminished by low automation and inability to test any recovery procedure.

Many organizations had limited confidence in meeting their Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in the event of a disaster. IT departments were hesitant to expand disaster protection, uncertain whether the quality of the insurance was really worth its cost.

Virtualization is fundamental and critical to the success of DR planning. Virtualization abstracts the complexity of hardware and software and allows standardization of processes, thus making planning and automation of the recovery procedures much more reliable and repeatable.

In fact, in a recent IDG survey, 70% of customers achieved improved BC/DR with virtualization.1

An intelligent virtual infrastructure based on VMware is the right foundation for the modern DR solution. Highly adaptive and scalable, it is optimized for business-critical workloads with built-in intelligence.

The VMware DR solution provides:

- The simplest way to replicate applications to a secondary site
- The simplest way to set up recovery and migration plans
- Fully automated, most reliable site recovery and migration

---

1 IDG Research, Benefits of Virtualizing Business Critical Applications, March 2011
**Cost-efficient DR:** With the rapid adoption of virtualization and the evolution of replication technology, DR is becoming more cost-efficient. Virtualization enables infrastructure consolidation at the failover site. Less costly replication options are more broadly available, using lower-end storage appliances or stand-alone software solutions. With these advances, DR can protect large-scale mission-critical IT assets, as well as smaller sites and Tier 2 applications.

**Automated DR:** In virtual environments, clinicians and other end users are shielded from the complexity of managing each step in the recovery process. Now, a DR solution can automatically execute and coordinate all the steps required to ensure the desired level of protection. Traditional runbooks are no longer “good enough” to manage recovery plans and are replaced with software-driven recovery plans. Setting up a recovery plan in a virtual environment is as simple as selecting RPOs and RTOs for each business service.

**Reliable site recovery and migration:** With virtualization, healthcare organizations get a much stronger assurance that they can meet their RPOs and RTOs. Virtualization provides the ability to test recovery plans frequently in a non-disruptive manner. Manual recovery processes are now replaced with automated recovery, eliminating the risk associated with user errors and ensuring predictable recovery.

The chart below shows how organizations with virtualized infrastructures utilize DR capabilities along with other benefits of virtualization.

How would you describe your organization’s usage of the following virtualization features/capabilities with its production environment-based virtual machines? (Percent of respondents, N=119)

<table>
<thead>
<tr>
<th>Feature/Capability</th>
<th>We currently use this feature/capability</th>
<th>We plan to use this feature/capability within next 12-24 months</th>
<th>We have no plans to use this feature/capability</th>
<th>Don’t know/Not applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated restart of virtual machines in the event of a physical server hardware failure</td>
<td>65%</td>
<td>22%</td>
<td>12%</td>
<td>2%</td>
</tr>
<tr>
<td>Backup and recovery solutions integrated with the virtualization platform</td>
<td>60%</td>
<td>24%</td>
<td>14%</td>
<td>3%</td>
</tr>
<tr>
<td>Site recovery solutions for virtual machines</td>
<td>57%</td>
<td>24%</td>
<td>14%</td>
<td>5%</td>
</tr>
<tr>
<td>Live migration of virtual machines based on CPU, memory, and network utilization policies</td>
<td>54%</td>
<td>31%</td>
<td>11%</td>
<td>4%</td>
</tr>
<tr>
<td>Live migration of virtual machines</td>
<td>54%</td>
<td>31%</td>
<td>11%</td>
<td>4%</td>
</tr>
<tr>
<td>Live migration of storage associated with virtual machines</td>
<td>51%</td>
<td>34%</td>
<td>11%</td>
<td>3%</td>
</tr>
<tr>
<td>Automated deployment of virtualized servers based on CPU, memory, and network utilization policies</td>
<td>45%</td>
<td>37%</td>
<td>15%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: ESG white paper: Enterprise Strategy Group, 2011: Virtualization Management Critical to Achieving Scale and Efficiency
Disaster Recovery Myths and Realities

Disaster Recovery is like an insurance policy that you can test without having an accident.

**MYTH 1:** Disaster Recovery is a luxury feature; it’s expensive and resource consuming.
**REALITY:** VMware vCenter™ Site Recovery Manager (SRM) gives you the flexibility to define failover scenarios that meet your choice of coverage, speed, and cost of recovery. For example, while a dedicated recovery site is a robust solution (and yes, more expensive), in many cases it is sufficient to have an active bidirectional approach where two or more datacenters are complementary with enough capacity to pick up critical applications. Therefore, no resources are wasted and business continuity is maintained.

Overall, SRM customers consistently report significant savings of money, resources, and time.

**MYTH 2:** Architecting and properly managing a DR solution is a complex task requiring special skills and expensive resources.
**REALITY:** Not with VMware. Physical DR can be complex because of duplicate and siloed infrastructures and configuration synchronization issues across sites. Virtualization encapsulates servers, operating system and applications, including all configuration data, so the complexity is greatly reduced. Virtualization and automation ensure that recovery plans are simple, complete, and can be reliably executed by staff with no special skills required.

With SRM, setting up an automated recovery plan is effortless and can be done in a matter of minutes, instead of the weeks required to set up manual runbooks.

**MYTH 3:** After all the planning, you never know if recovery will be successful in a real disaster.
**REALITY:** A recovery plan is not a complete plan without testing. In fact, the recovery plan can and should be tested with sufficient failures, and retested to ensure validity. SRM enables frequent non-disruptive testing of recovery plans.

**MYTH 4:** DR expense is a sunk cost, like a protection plan that’s most likely never used.
**REALITY:** Even if the big disaster never happens, the recovery plan can be used as a migration plan with similar steps, helping you during planned downtimes such as site migrations. In addition, DR planning helps to fulfill compliance where disaster recovery plans are required. The outcome of recovery testing proves disaster preparedness and the ability to meet RTOs.
How it’s done at Adventist Health System

Adventist Health System (AHS), a healthcare organization in the U.S., supports 37 hospitals and cares for roughly four million patients annually. AHS Information Services (AHS-IS) serves hospitals in nine states and employs more than 500 people.

To ensure AHS-IS can provide excellent care, “Mission Zero” initiative aims to provide the highest levels of service and minimum downtime for critical healthcare systems like Cerner’s charting and electronic medical record applications.

Adding SRM to its VMware infrastructure allowed AHS-IS to streamline operations even further by automating DR planning and testing. “VMware SRM makes managing and testing our recovery plans as easy as pushing a button. The fact that we can run tests as often as we want gives us a high degree of confidence in the recoverability of our systems,” says Kenneth Newball, senior disaster recovery administrator at AHS-IS.

Business results:
- Reduced RTO by 75%, from 48 hours to less than one hour
- Eliminated the cost of flying a team of seven people to test remote DR
- Cut hardware purchases by 84.5%, maintenance by 93.1%, and power consumption by 90%
1. **Virtualize.** Virtual environments are much more agile and easier to migrate. Virtualization hides the complexity by shielding the individual components and moving parts, thus simplifying the planning and increasing the visibility into the DR process. It also allows you to use hypervisor-based replication that is far more flexible and cost-efficient than storage-based replication.

2. **Automate.** Don’t let human error stand in your way. Use automated recovery plans, not a stack of notes in a binder. With the proper automation, a recovery plan can be done in a matter of minutes instead of weeks. Automation shields clinicians and users from having to manage many of the recovery steps, and automatically coordinates activities such as preconfiguring networks and virtual machines, configuring the recovery infrastructure, and restarting applications.

3. **Verify and test.** Test your DR plans often. Use nondisruptive testing of your recovery and failback plans. Study a detailed report of the test outcomes, including the RTO achieved. With this information, you can gain the confidence that your disaster protection plan meets the business objectives. It will also provide the necessary training to the staff and show any possible issues early so they can be addressed.

4. **Set achievable goals.** Automated disaster recovery can be very powerful, but it’s not magic. For example, 100 virtual machines containing Exchange, Oracle SQL, and SAP cannot be failed over and started in 30 minutes. Set your RTO realistically. To set your baseline, run a test under different conditions and see what you can achieve.

5. **Act early if you can.** If you have warnings, use them! Act early to execute your well-tested DR plan before an actual disaster strikes to avoid a DR event altogether. IT confidence is a byproduct of a good, solid DR plan that has been tested. Examples are a forecasted storm or a potential network outage threat.

6. **Be proactive when at risk.** Most outages are not caused by actual disasters, but by planned procedures gone wrong. Examples: software or network upgrades, data maintenance, facilities repairs, etc. By proactively migrating your critical patient-care applications, you can mitigate the risk and greatly reduce a possibility of outage or service degradation.

7. **Assign responsibilities.** Assign everybody involved in the DR plan a specific task. Don’t expect the relevant personnel to always be at the disaster site or to be in control immediately. Implement necessary duplication and redundancy for people, just like you would do with computers.
8. **Keep your recovery data as current as possible.** It is a good practice to prepopulate your failover site with the data that doesn’t change often, or by much. This will allow you to focus only on the fast-changing critical data at the time of failover, and ultimately meet your RTO with less effort.

9. **Prepare for failback.** Create and test a failback recovery plan, set up replication in reverse, and know when to trigger it. Agree on what to consider the “end” of the disaster so your healthcare organization can go back to normal.

10. **Don’t just throw money at DR.** Utilize cheaper, commodity failover site assets, or use the repurposed hardware left over after your primary datacenter has gone virtual. Consider bidirectional or shared failover sites, use more software in the cloud (SaaS), and also look at non-IT DR means (UPS or backup generators, fuel reserves, better fire protection, etc.).

“VMware Site Recovery Manager makes managing and testing our recovery plans as easy as pushing a button.”

— KENNETH NEWBALL
SENIOR DISASTER RECOVERY ADMINISTRATOR
AHS-IS
While your datacenter is critical to your ability to conduct high-quality patient care, events beyond your control (or even planned ones) can make patient-care applications and IT services unavailable or highly limited. This situation, however rare, could be very damaging to the integrity of your organization, your market credibility, and your patients’ satisfaction and loyalty.

You can mitigate this risk by implementing a DR solution to protect your critical patient-care applications and IT assets. A well-designed DR solution built on an intelligent virtual infrastructure can provide the required RTO and RPO while keeping the costs in check. Your DR plans can be tested in a nondisruptive way and benefit your IT department in areas beyond the typical DR needs.

Your IT infrastructure plays the most critical role for the feasibility and the ultimate success of your DR plans. Virtualized infrastructure proved to be the most reliable and cost-effective platform for DR by allowing you to abstract the moving parts and components of your datacenter, simplifying the replication architecture and requiring fewer resources overall.

So how do you start the journey to protect your patient-care applications and IT assets? Use this quick-start list as your guide:

1. **Identify your most critical applications and data.** What applications directly affect patient care, maintain safety, help you achieve meaningful use, or are otherwise critical to business continuity? What data is absolutely critical for your clinicians and patients, your internal accounting and finances, or compliance?

2. **If you have not yet, consider virtualizing your key applications.** This will not only cut much of the operational and maintenance costs by removing unnecessary complexity and operational cost, but it will also make your environment better suited for effective DR planning.

3. **Agree on the target RTO and RPO.** What data can you lose? For how long? When do you want to be back online with your critical applications? Make sure your goals are realistic.

4. **Define the triggers for DR to bring all the planned activities to action.** This can be a business decision based on the data you are getting, or a technical event automatically triggering your DR.

5. **Identify what DR replication, failover and failback options you want to implement.** The resulting solution will be a compromise among level of protection, speed of recovery and costs.

6. **Select the solution vendor.** Beware of vendors pushing specific hardware, operating system or other limiting choices that don’t align well with your environment. Study the level of your team’s expertise required to maintain the solution or the amount of resources you need to allocate. Make sure you can test the solution without waiting for an actual disaster.

We hope you will never need to use your DR solution to recover from the unexpected. But if you ever do, VMware is here to make sure you are well prepared.

For more information on VMware vCenter Site Recovery Manager or free 60-day evaluation, please visit [VMware SRM](https://www.vmware.com/solutions/). For details and hints on SRM implementation, and thoughts on delivering data protection, high availability, business continuity and disaster recovery with VMware, we welcome you to read our [blog](https://www.vmware.com/blog/).
Disaster Recovery 101 — The Basics

**Disaster Recovery is a Key Part** of a healthcare organization’s business continuity initiative to ensure the availability of integral IT-dependent patient-care applications and processes and prevent any long-term negative effects of both planned and unplanned disruptions. The goal of DR is to restore critical IT services as quickly as possible and minimize patient care disruption.

Nothing impacts your ability to recover more than the agility of your IT and applications infrastructure. Just like fire safety must be built into the building before the fire occurs, and a car’s safety features are engineered to reduce crash impact, the design of your IT infrastructure can make or break the success of your DR program.

**IT and Applications Infrastructure**
Your datacenter’s infrastructure plays an instrumental role in the effectiveness of your DR solution. The infrastructure can make DR very complex, hard to implement and sometimes even impossible; or it can help to make your IT reliable, verifiable and effective. The next section explains how.

*Two Key processes for simple and reliable disaster recovery:*

**Failover**
Failover is the capability to switch over to a redundant or standby server, system or network upon the failure or termination of an existing asset. Failover should happen without any kind of human intervention or warning.

**Failback**
Failback is the process of restoring a system or another asset that is in a failover state back to its original state. Effective failback returns the system to the state of operation before the disruption.

**Key metrics for planning and measuring success of the procedures.**

**RPO**
Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization, generally called an “acceptable loss” in a disaster situation. It allows an organization to define a window of time before a disaster when data may be lost and is tightly dependent on the type of data replication used. The higher granularity of data replication, the shorter the RPO.
While RTO is purely a technical metric, the decision to trigger the failover is a business one, and RTO can often take much longer than the actual DR itself. Whether initiated by humans or by an automatic trigger, the lead time to start DR should be also accounted for and included in RTO. Replication is a key element of any DR process in most cases, usually provided by the specific DR solution used.

### Replication
In the context of preparing for a failover, replication provides intentionally architected redundancy of your IT resources: hardware, data, software, networks or all of them together. There are several factors in determining the depth and amount of replication needed: type of services to be protected, criticality of different components, technology and cost.

### Disaster Recovery Scenarios
Various DR scenarios and techniques are available to meet your specific requirements and cost objectives. The right architecture can make your DR procedures more efficient, cost-effective and predictable. Here are a few commonly used configurations from which to choose:

- **Active-Passive**: This is a more traditional DR scenario, where a production site running applications is recovered at a second site that is idle until failover is required. In this scenario you are paying for a DR site that is idle most of the time.

- **Active-Active**: Use your DR site for non-critical workloads when you are not using it for DR. Configure it to automatically shut down or suspend the virtual environment as part of the failover process so that you can easily free up compute capacity for the workloads being recovered.

- **Bidirectional**: Provide bidirectional failover protection so that you can run active production workloads at both sites and fail over in either direction. The spare capacity at the other site will be used to run the virtual environments that are failed over.

- **Local Failover**: Some workloads need to be able to fail over within a given “site” or campus; for example, when a storage failure occurs or when maintenance forces you to move workloads to a different local lab.

- **Shared Recovery Sites**: In the standard one-to-one deployment, a single datacenter is protected by a single recovery site. You may also choose to protect multiple datacenters using a “shared” recovery site. All protected sites are visible and manageable within this single instance of the DR solution at the shared recovery site. Healthcare organizations that have several sites that need protection will find this feature appealing. This topology can be implemented using the shared recovery site feature.