Planning and Implementing Disaster Recovery for DICOM Medical Images

A White Paper for
Healthcare Imaging and IT Professionals

I. Introduction

It's a given - disaster will strike your medical imaging data at some point in time. No matter how good your IT network, some types of disaster cannot be prevented, including such natural occurrences as hurricanes and floods. Disaster planning and back up is essential to provide recovery of data lost to your system, or to prevent such loss. Beyond basic business and revenue considerations, the implications of data loss can be enormous, involving legal and liability issues and even jail time. The loss of medical imaging data can be particularly serious.

Planning for the unplanned involves a myriad of factors. But with a careful and methodical approach, a successful disaster recovery plan can be achieved.

This white paper will examine common types of disasters, disaster recovery strategies typical for medical imaging data, data storage medias and methods of implementation.

II. Types of Disaster

IT disaster scenarios that most businesses--including medical imaging facilities and departments--should address are numerous and varied. They include:

- **Hardware failures** - Servers, disks, tape subsystems/media, routers/switches, user stations, network interface cards
- **Software failures** – Viruses, software bugs or corruption, database crashes
- **User errors** - Deletion of files, misplacing files, turning off power, pulling plugs, spilling liquids on equipment
- **Localized disaster** - Data center unusable, electrical failure, network failure, hacking attacks, communications cable cut by construction
- **Area disaster** - Power loss, evacuation, flooding, fire, terrorist attack
- **Natural disaster** - Earthquake, forest fire, tornado, hurricane

III. Back Up Strategies

Disasters can be rated from mild to severe for their potential to interrupt access to data or to cause data loss. No single backup strategy is adequate for all disasters, and any disaster recovery plan must be tailored to meet each organization's needs and relevant compliance issues. The variety of data types in a medical facility, which all must be handled differently, further complicates matters, generally requiring multiple approaches

to support the various needs and priorities. This paper focuses primarily on DICOM imaging data and its related database information.

For the least significant disaster scenario, a simple on-site tape backup coupled with UPS (uninterruptible power source) units can be sufficient. A slightly more comprehensive disaster recovery plan requires remote storage of tape backup to protect against local natural disasters. The farther away the remote site, the better.

However, in the event of a disaster, this solution has numerous shortcomings. The time to transport tapes back onsite and the process of tape restoration, which is slow compared to other media, is generally beyond the required RTO (Recovery Time Objective).

Disk-based media is far more reliable than tape and utilizing it onsite provides a higher level of data security. Adding more protection, disk-based back up in one or multiple offsite data centers provides an even more effective safeguard.

Additionally, unlike tape, disk storage opens up the possibility of real or near real-time data back up, improving data security as well as the ability to work directly from back up media in the event of a disaster to ensure business continuity, as discussed in the next section.

Provisioning a remote data recovery center can mean the difference between being wiped out and having minimal downtime or data loss. Choosing a remote site for disaster recovery calls for consideration of such physical factors as relevant threats and probabilities for disaster, geographic stability and accessibility. Though the expense maybe considerable, downtime and data loss may be more expensive. Additionally, for critical data, real-time replication both onsite and off may be the only way to maintain compliance with regulatory requirements, including HIPAA.

Cost is also a factor in selecting a back up solution, and providing adequate and compliant disaster recovery in the most cost effective manner possible is vital. This expense must be compared against the likelihood that a disaster of a certain type will occur. For example, for facilities in hurricane zones, the cost of offsite storage is easy to justify. Additionally, a solution should be weighed against the cost of data loss. This is not just lost revenue, but the overall impact the data has on enabling the business to meet customer, employee, legal and financial obligations. Naturally, the consequences of the loss of medical images are significant both for patient care and financially, making a thorough solution imperative.

When tallying up the costs of a back up solution, consider operating and staffing costs as well as required hardware and software. Depending on the various factors, contracting with a managed back up solution provider may provide the most cost effective option.

IV. Backup Technologies

- ***Tape***

The most economical but least effective backup media, tape can be adequate for some applications.

Tape leaves the back up solution vulnerable to data loss due to difficulties managing a vast number of individual tape units and unreliability of the media itself. Tapes often fail in the restore process despite careful verification at the time of back up.

Also, tape backup is generally performed on-site on a schedule that leaves gaps in protection of data of 12 or 24 hours or more and is transferred physically to an off-site facility. This means a risk of loss and security breach during transport and, in a disaster scenario, a delay while tapes are retrieved from storage. With the legal, financial and ethical issues of medical image storage, using a better backup technology with greater reliability is important to provide improved speed of recovery with the potential for minimal downtime

- ***Disk***

Current disk-based systems are proving more useful, reliable and cost effective, especially for back up of mission critical data. Speed and reliability of recovery -without the failure of tape media - are the principal advantages disk-based technologies offer. Additionally, disk solutions are capable of and typically employed to replicate data in real time, not to back it up at set intervals. With this method, if the primary archive fails, the network can access data directly from the back up archive and business can continue as usual in this fashion until the original archive is restored.

Today, SANs (Storage Area Networks) and NAS (Network Attached Storage) systems that leverage high-speed FC (fibre channel) connections provide fast dependable disk-based backup options and are generally configured with standard and reliable RAID arrays with high throughput iSCSI hardware interfaces.

A SAN is a high-speed subnetwork of shared storage devices that together share the task of data storage, are recognized by the system as a single archiving device and make better use of each device's storage capacity than would a series of unrelated disks. NAS is a server or device dedicated to file sharing and delivering data to network clients. The purpose of both technologies is to provide access to data across a network, whether LAN or WAN, to all servers while also supporting easy expansion of available storage capacity through the addition of new storage devices to the system.

The backup storage array must avoid having a single point of failure (SPOF)—an architecture that allows a single interruption in the archive infrastructure to compromise both the ability to successfully backup data as well as restore it when needed.

An effective and reliable backup system might feature server clusters with carefully configured routers/switches and shared NAS and SAN storage. Data would be replicated both locally and remotely, especially in conjunction with remote servers/clusters. In the event of a disaster, this system would provide rapid access to data with failover to the back up system for business continuity as well as fast data restoration. Careful planning and configuration to avoid SPOF can prevent having a backup system go down along with the primary system when disaster strikes.

Replication creates a complete copy of data on the backup disk array and continually updates this as changes occur, versus copying and recopying the entire data set. Real time data replication may be either asynchronous or synchronous. Synchronous replication delivers RPOs (Recovery Point Objectives) measured in minutes, and recovery times measured in seconds, unlike tape which can be measured in days in the worst case--if recovery is successful at all.

Synchronous replication writes data to both the primary and secondary disk arrays at the same time, while asynchronous replication grabs data once it is written to the primary disk, and rewrites it to a secondary array. Because of performance issues, synchronous replication is better suited for localized use and asynchronous is best for remote replication.

Once replicated, data can be easily further replicated across multiple backup arrays to provide additional data security.

- ***Other***

Other technologies such as VTL (Virtual Tape Libraries), CAS (Content Addressed Storage) and CDP (Continuous Data Protection) can augment disk storage systems to address specific backup needs and provide greater flexibility and redundancy.

Virtual tape libraries mimic the functionality of tape libraries but utilize disks. CAS provides object-oriented storage that cannot be updated and is appropriate for data such as medical images that typically are not changed archived. More comprehensive CDP creates a storage snapshot for every data modification to create system restore points. CAS has the advantage of allowing restoration from clean data if a gradual corruption of data occurs and problems are replicated on other back up files.

VTL can provide a familiar interface and similar functionality to tape backup systems with the improved speed and reliability of disk-based systems. However, it shares some limitations in the time and frequency of back up and restoration speed.

For CAS, optical (CD or DVD) jukeboxes are particularly appropriate. Data stored to this media cannot be altered, safeguarding medical images. However, restoration and business continuity access is slower than with a SAN or NAS.

V. About HIPAA

HIPAA regulations regarding digital information storage are complex and are the same for data both in transit and a live environment. For tape backup, data must be thoroughly and securely encrypted to meet confidentiality requirements. An appropriate method must be selected that allows un-encryption at the DR site, even when that specific location is unknown in a multi-location set up. This is especially difficult for tapes deposited offsite at third-party repositories. While tapes may be safely encrypted, if the tape is damaged or the original systems lost, data access becomes impossible.

To ensure HIPAA compliance, disk array backup demands even more careful consideration. Sites must ensure that onsite errors are not propagated in the archive. Moreover, both onsite and offsite failover systems must have equal security. For installations with multiple sites, this means redundant security setups must protect not only data, but also the newly restored systems in the event of a second disaster.

During a HIPAA audit, healthcare facilities must prove that data on a restored system is as secure as the original. Naturally, restored systems will be under even higher scrutiny than the originals because the new system is unproven.

VI. Implementation

Building and managing an effective back up system calls for time, effort and funds. You may choose to implement it in-house, call in a consultant or outsource some or all of the system, depending on the specifics of your organization. But in all cases, this should be a carefully considered decision.

- ***In-House Installation***

Generally, installing a back up system is a major undertaking. It also is not something that existing in house IT staff generally will be trained to handle. An organization should carefully weigh its capability to provision the necessary infrastructure before making a decision to implement a solution in house.

Given this, many organizations elect to hire a consultant to set up the archive. Following set up, if the archive is to be maintained in house, the consultant likely will be equipped to carefully train staff on disaster recovery related issues and proper implementation of procedures.

However, organizations must keep in mind that increasing IT infrastructure, especially adding complexity, puts a strain on existing staff, who are often already stretched thin and stressed. Often back up maintenance will require the addition of new staff. Remote sites also increase this need, plus add additional management concerns.

Also consider that an archive installed in house, by contrast with one outsourced to a service organization, is subject to technology obsolescence. At some point legacy technologies will need to be upgraded, calling for additional time an expense.

In-house system implementation and management may be the most cost effective implementation for some organization. However, many facilities outsource the entire back up system.

- ***IT Consultants***

Hiring an expert consultant for system design can be helpful but increases costs. Once installed, most organizations will elect to maintain the system using in-house staff.

A consultant may have the expertise to help select the best back up strategy and technology for a facility's needs today and to grow with them into the future. A good consultant also will have the experience to provide installation with a minimum of disruption to the work environment, and, as noted, should also be able to train staff on system maintenance.

When hiring a consultant, experience with a medical imaging organization and working with DICOM files is important. Involve your IT staff in the interview process and have them evaluate several medical imaging solutions the consultant already has installed.

- ***Outsourced Solutions***

Contracting with a reliable outside service provider can alleviate many of the problems associated with developing and implementing a disaster recovery plan and infrastructure. A variety of providers are available, most notably organizations that will simply provide offsite storage of back up tapes a facility creates themselves as well as complete turnkey solution providers.

While preferable to no back up at all, as noted, tape back up is generally insufficient for medical image archiving applications, even when stored offsite.

By contrast, a turnkey archive service provider can implement a solution that is effective, efficient and cost effective for back up medical image archiving and related data. In many cases, such a provider actually can implement a solution at less cost overall than an in-house project.

Again, because of both the unique demands of DICOM archiving and stringent industry regulations, facilities should select a provider with a strong background or specialization in medical imaging archiving and backup. For more than 15 years, InSite One has been providing healthcare facilities with high-quality, specialized back up solutions for medical images and related data.

A turnkey back up service provider such as InSiteOne delivers a high value service that offers:

- Elimination of IT staffing training and maintenance costs.
- An economy of scale in archiving hardware and software with costs shared among it multiple client installations.
- An economy of scale in an offsite facility with cost shared among its multiple client installations.
- Elimination of hardware and software obsolescence due to timely provider upgrades.
- Built in scalability to accommodate archiving needs as they grow.
- Elimination of in-house IT training and maintenance staff costs.
- Elimination of HIPAA compliance issues.

In addition, InSiteOne, in particular, offers cost-effective, predictable storage pricing through an all-inclusive back up fee for the life of the study, whatever the image size. The service includes redundant archiving in two data centers in Connecticut and Phoenix, where disk array real-time replication combines with fixed optical media back up to provide multiple-strategy comprehensive protection. Should a disaster occur, data can be accessed remotely over the Internet so that your facility can continue to work from the remote archive until restoration is complete.

When evaluating a back up service provider, ask questions. In particular, find out specifically about the type of storage technology and media used, how often it is upgraded and whether this cost is passed on to you as a price increase. Inquire about the time involved in data restoration and whether the archive can be accessed before restoration to provide business continuity. Ask very specifically about hidden costs that may escalate your budget should a disaster occur. Obtain references. Your practice depends on access to your valuable medical data.

VII. Conclusion

Creating a data disaster recovery plan and technology infrastructure is vital for any medical imaging organization. Given the significant implications of data loss on patient care and legal and liability issues, disaster planning is particularly important for medical imaging providers. While no plan can provide protection for every type of disaster, a well-conceived, multi-tiered back up system can provide a high level of data protection as well as business continuity. Many healthcare organizations may find that outsourcing back up protection to a service provider experienced in DICOM archiving is the most expedient and cost-effective route to safeguarding medical image files. When selecting a provider, rely on due diligence and make a circumspect decision.