Introduction

Healthcare organizations increasingly rely on data and applications for a dizzying number of tasks, from populating EHR databases to storing radiology images. Beneath it all, data is what makes critical patient files storable, retrievable, and searchable when needed most. However, disasters large and small continue to occur that thwart the best efforts of institutions to store, protect and share patient information.

In the event of a system outage, response must be swift, enacted confidently and without delay so that the business of patient care can continue with minimal disruption. But as the recent events of Hurricanes Sandy and Irene show, some hospitals remain unprepared for disasters that can wipe out vital repositories of patient data. In fact, even relatively small failures such as data corruption can prove disastrous when appropriate protection and recovery procedures are not in place within these environments.

A new frontier for healthcare IT

As healthcare providers increasingly come to rely on computerized systems in the course of caring for patients, healthcare IT is under more pressure to protect, retain, and ensure constant availability of this vast amount of medical data. The adoption and expanded use of Electronic Health Records (EHR) increases daily and federal support for programs to improve the quality of patient care will continue to drive the exponential growth of digital data within
the healthcare environment. For example, the HIPAA HITECH Act provides financial incentives for hospitals to quickly adopt EHR technology and inflicts financial penalties for those who don’t. With such forces at work, systems that were once a luxury at many healthcare facilities have quickly become essential to surviving in the current regulatory environment.

The proliferation of medical data worldwide and its astounding rate of growth has resulted in backup and disaster recovery becoming a top priority for healthcare IT. As providers become ever more reliant on their systems in the course of diagnosing and treating patients, it becomes critical that data is readily available. Even one hour of downtime for a hospital’s EHR could negatively impact patient care – and extended outages have had even more severe effects. In such cases, what are healthcare providers to do? The old recourse was to “go back to paper.” But, as hospitals rapidly adopt all-digital models, paper-based records have become obsolete.

Today, a typical community hospital in the United States may have dozens of TBs of electronic data, depending upon when and how aggressively they adopted digital systems. With this volume of data, it becomes economically and physically impossible to back it up on a daily basis. So how do hospitals protect this vital business asset?

In an era when storage and protection is vital to providing adequate patient care, many organizations are taking a closer look at their plan for protecting data from disaster. It is important to remember that only by understanding the nature of the data can healthcare IT professionals devise a comprehensive approach to healthcare disaster recovery.

Why healthcare data is different
Like any other business, a healthcare organization uses many different software applications to run its day-to-day activities. However, unlike other businesses, most of these systems directly or indirectly impact patients – any unexpected downtime in critical applications may jeopardize patient care. Healthcare IT is charged with keeping these systems available 24/7 and, in the event of an outage, is tasked with restoring operational capacity as quickly as possible. In the event of a large-scale disaster, the entire hospital must execute its business continuity plan to ensure minimal disruption to patient care. Healthcare IT plays its part by executing the disaster recovery plan perfectly to ensure that these systems continue to function in all conditions.

While the stakes may be higher for healthcare IT, are the data protection and disaster recovery requirements fundamentally different than those of any other business? In many ways they are not, but in one key area they are: Healthcare organizations generate a large percentage of static data, the nature of which requires a particular approach to healthcare disaster recovery. For vast amounts of unchanging, unstructured or semi-structured data, archiving is a better approach than backup for protection purposes. By creating a few geographically dispersed copies of the data on multiple media types, hospitals are best positioned to meet Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for hospital systems. For example, in the event of a disaster, a PACS database which is archived can be recovered as quickly as the Health Information System (HIS) and Radiology Information System (RIS), and then pointed at a secondary copy of the image archive, preferably extant on storage in a secondary data center.

This combination of backup and archiving enables an optimal strategy for protecting all types of data in a hospital. By understanding the nature of the data found in clinical systems, healthcare IT can deliver both realistic and acceptable RPOs and RTOs to the business-side interests of healthcare institutions. In the event of a disaster, the organization can rest assured that mission-critical applications will be available when needed. And doctors and nurses can get on with the business of patient care rather than distracting themselves with the business of healthcare IT.
Real world disasters: it can happen anywhere, any time

Unfortunately, even with all that is known about the importance of maintaining a robust data recovery and protection plan, many hospitals still encounter scenarios that put patient data in harm’s way. The most common root causes of failure are data corruption and user error, and during the recovery phase, almost all hospitals discover that there is an application or set of applications that they haven’t been sufficiently protecting.

Case Study 1: flooded hospital data center

At one critical access hospital, a significant weather event rendered several departments uninhabitable. The hospital closed immediately, and data recovery wasn’t even attempted for three days. The data center was flooded, and hospital staff could not reach equipment for some time due to police activity and general disorder. Once hospital IT staff finally reached the data center, they discovered that untrained staff had removed the servers but left the SAN storage underwater – with the hospital’s backup tapes in a cardboard box next to it.

Data on SAN storage and tapes remained underwater, and there was no storage hardware available to support restore when staff finally could begin the process. A rented space was used for recovery, and data was backed up from SAN following a lengthy drying process in order to make it available for recovery onto the new systems. This was a critical problem in part because, in order to fulfill payroll, the vast majority of MEDITECH servers in this hospital needed to be restored due to the dependencies between modules. It was over six months before the hospital saw another patient due to physical infrastructure issues. Eventually, the hospital merged with a regional organization.

Case Study 2: data corruption impact

At a large hospital chain, the MEDITECH EMR disk slowly corrupted over several months yet went undetected because the corruption was not significant enough to disrupt the EMR. Backups to tape continued to occur on a daily basis, dutifully backing up the corruption. As corruption progressed, the hospital’s server became slower and slower, prompting staff to reboot the server, only to discover it was no longer operational. When the previous night’s backup was restored, it contained the corruption and would also not boot.

Although the hospital had replicated MEDITECH data using array replication technology, the replicated copy was corrupted as well, rendering the failsafe useless. Eventually, the health IT team found a good, months-old backup with no corruption; however, they were faced with a difficult decision: to restore from a known “good” backup that was months old and lose significant portions of EMR data, or wait for a solution to resolve the corruption? The hospital elected to try and fix the corruption, and consultants were able to “transplant” the Master File Table (MFT) from the good, restored disk to the corrupted disk, and the solution worked. The hospital was able to recover back to the time of the reboot, but still had to re-enter and fix data. The net downtime for the EMR was over 36 hours.

Lessons Learned

So, what are the lessons learned?

It’s extremely important to keep many generations of backups, and to combine archive and backup to ensure protection with appropriate RPO and RTO for all types of hospital data. The vast majority of MEDITECH restores come
from monthly (or yearly) tapes. Array-based replication is a useful tool, but it does not eliminate the need to keep many generations of backups, particularly offsite. Any hospitals using array-based replication in MEDITECH should be certain they are achieving application consistent points in time. Adding archive to backup can improve protection by reducing the amount of data in the backup pool, shortening recovery as well as backup windows.

It’s critical to define decision-making responsibilities in advance of disaster. Hospitals need to determine who is responsible for making the decision to keep a system down in order to get back to a better point in time. More importantly, who in the organization would determine if losing several months of data in order to get back up and running sooner is a worthwhile decision?

Test recovery on a regular basis to ensure that all critical data are protected and recoverable. Disasters are by nature unpredictable. A SAN can fail due to a bad firmware upgrade, or a sprinkler system could self-activate due to high heat, flooding servers and storage systems. Disasters take many forms, and evidence grows daily supporting the investment in a comprehensive data protection and backup strategy.

**Best practices checklist**

By now it should be clear why disaster recovery continues to be a top concern for healthcare IT professionals. The proliferation of computerized clinical systems and the rapid adoption and reliance upon them by healthcare professionals mandates that healthcare IT ensures constant availability. In the event of a system outage, a plan must be in place to recover quickly and efficiently, prioritized by the importance of each system as it relates to the business of the hospital.

Organizations should keep a basic checklist in mind for achieving these goals:

- Establish realistic RPOs and RTOs for all applications;
- Maintain geographically dispersed protection with multiple sites and multiple formats;
- Plan for deep generational protection (monthly and yearly backups);
- Ensure consistent backups are performed on all MEDITECH applications (ISB, IDR, MBF);
- Ensure PACS/DICOM have both geographical and generational protection;
- If data is stored at multiple sites, ensure resources are in place to backup secondary datacenter;
- Establish and circulate a documented plan for disaster recovery;
- Ensure staff is well-trained and knowledgeable in hospital’s preferred backup product;
- Know who in the organization can make critical decisions involving data loss and recovery in the event of a disaster.

The protection and recovery of hospital systems is somewhat complicated by the static nature of the majority of healthcare data – clinical images and scanned documents that rarely change once created and that consume vast quantities of disk storage. In order to optimize efficiencies, healthcare IT must protect this data in a way that meets the availability requirements of the organization while containing costs. A strategic combination of backup and archiving technologies is the best method to ensure that all data types within a healthcare organization are adequately and cost-effectively protected.