

Protecting Medical Records Before Disaster Strikes

By Bruce Eckert, MBA, CPHIMS

"Many of their records have been literally washed away."

- Dr. Carol Diamond of the Markle Foundation, referring to medical records for Hurricane Katrina evacuees

In an ideal world all healthcare organizations would employ electronic medical record (EMR) systems to safeguard medical data from disaster. But even having records in an electronic form does not guarantee their accessibility or preservation. Electronic data must be properly managed to be safe.

Consider the vulnerability of computerized records; all patient records are stored in a single, compact, centralized database, which allows fast and easy access from virtually any location. But, by concentrating all records in a single location, risk of loss is increased. If that centralized database is damaged, all the records are lost.

Headline-making disasters are not the only culprits in data loss. The cause could be as simple as a defective hard drive, a leaky pipe or a careless computer technician. Most practices back up their computer systems daily. But, where are those backups stored? At least some of each practice's backups should be stored away from the main office. Safe, off-site backups of computerized data are an organization's ultimate "fail-safe" protection against catastrophic data loss.

An effective off-site backup procedure incorporates four characteristics:

- **Geographic Separation** - Off-site backups prevent all copies of a practice's data from being destroyed in a single catastrophic event. Thus, the more distance between the various copies, the lower the risk. And, when selecting an off-site backup storage location, select a location that is not subject to the same risks as the main office.
- **Concurrency** - If a practice ever needed to use its off-site backups to restore its systems, all the data entered into the system between the

time of the catastrophic event and the time that the off-site backup was created would be lost. Thus, the more frequently backups are sent off-site, the lower the risk of losing data. A common off-site backup rotation cycle is a week, and this should be the bare minimum.

- **Security** - Under the HIPAA security regulations, a practice is responsible for the safety and security of its off-site backups that include patient information. Therefore, make sure that off-site backups are transported and stored securely. Use a bonded courier service to transport backups. Sending backups home with an employee, while easy and inexpensive, is risky. (Recently, a hospital received some unfavorable publicity when their backup tapes were stolen from an employee's minivan.) Use locking cases to carry and store the off-site backups. Investigate the security of the backup storage location: What would prevent an unauthorized person from gaining access to the backups? If the off-site storage location is not controlled by the practice, it is prudent to execute a HIPAA Business Associate Agreement with the storage location's owner. To further improve security, use backup software that encrypts and password-protects the backup data.
- **Availability** - While it is important that off-site backups be secured against unauthorized access, backups need to be available quickly when validly needed. Consider availability when selecting an off-site storage location: **What is the procedure for retrieving off-site backups? How rapidly can backups be retrieved? Are the backups available 24/7, 365 days per year?** Availability includes the ability to make use of off-site backups once they are retrieved. If your main server were damaged or destroyed, is another computer available that could be used as a temporary

server? Does this computer have the equipment, e.g., tape drive and software needed to restore data from the off-site backups? A "best practice" is to store a spare tape drive and CD with the necessary backup software with the off-site backup.

Online Backups

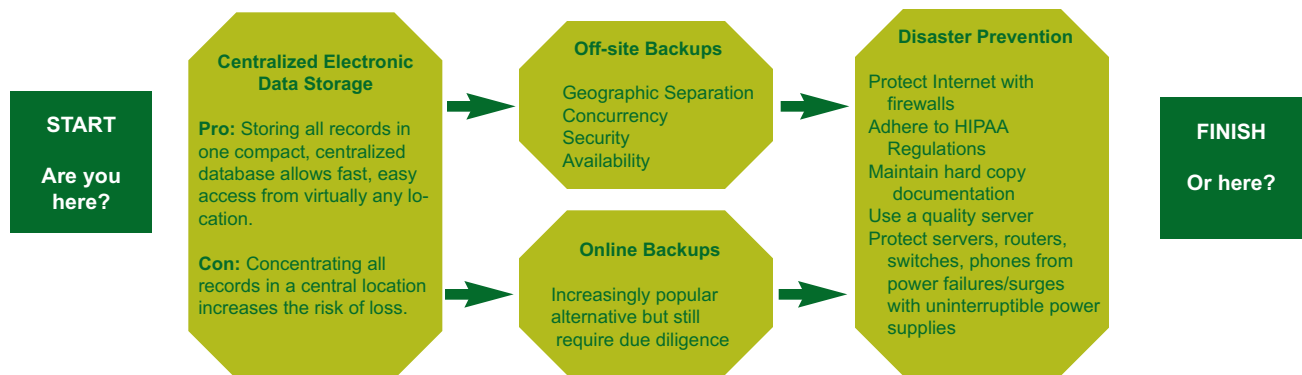
It is difficult to find a balance between security and distance on the one hand, and availability and concurrency on the other. To adequately meet a practice's needs, online backups are an increasing popular alternative that may minimize this conflict. Backups are sent over the Internet to a remote data center that may be hundreds or thousands of miles away. If a system needs to be restored, the backup is downloaded via the Internet. Some services even offer continuous, real-time synchronization with their customers' servers.

Prevent Disasters from Occurring

Off-site backups are a necessary fail-safe measure to protect computerized data from the worst-case

scenarios. But the best defense is to try to avoid information technology disasters. In addition to off-site backup storage, protect all connections to the Internet and unrelated organizations with firewalls. Adhere to good security practices, as outlined in the HIPAA security regulations; maintain up-to-date system documentation in paper form; use a quality server with as much built-in redundancy as possible; protect servers, routers, switches and telephone systems from power failures and electrical surges with uninterruptible power supplies (UPS); place servers and other critical computer equipment in locations with good air flow and cooling, and minimal chance of water damage, flood, theft, or other types of physical damage.

Still not all disasters are preventable. Thus, all healthcare providers must employ sound backup procedures, including off-site backups, to protect their patients' medical information and the organization's viability.



Bruce Eckert, MBA, CPHIMS, is an executive consultant for Beacon Partners. For more of Mr. Eckert's insight on Disaster Recover Planning, please contact beckert@beaconpartners.com.

Beacon Partners is one of the fastest-growing privately-held healthcare management consulting firms, coaching organizations in the development of strategies that are centered on maximizing Enterprise Yield performance. To achieve top levels of performance, an organization must factor strategic direction, physician alignment, economic incentives and overall market impact. Our experience has proven that focus on these critical success factors will strengthen an organization's position in the market and, ultimately, improve the patient's experience with the provider.

Please visit <http://www.beaconpartners.com> and Beacon Partners' special healthcare informational portal, <http://www.spotlightonhealthcare.com>.

1.800.4BEACON | www.beaconpartners.com
 BOSTON • SAN FRANCISCO • TORONTO