

Offsite Backup: A Strategy for Compliance, Security and Cost-Savings

By Marc Gonzalez

For organizations adopting electronic medical record systems, the task of doing backup (storing critical patient and operational data) has become increasingly complicated. There will soon be financial pressure to conform to regulatory requirements. Healthcare practices, like other straining industries, must bear the overhead to equip their facilities and engage IT professionals with the skills to handle security and compliance issues.

This scenario can sound like a daunting no-win situation. However, there are affordable technologies to help regulated industries meet compliance obligations and improve operational efficiency. The idea of offsite backup, or “Cloud Storage,” as it was defined in a recent article in the HIPAA Compliance Journal (www.hipaacompliancejournal.com) holds promise. It inherently achieves the first of five fundamental requirements of the HIPAA Security Rule.

To achieve all five, the solution must be rigorous. The above article lists compliance, long-term storage capabilities and, access controls as concerns when choosing an offsite backup service. These are valid qualifiers. The market is full of low cost solutions ideal for the residential customer, but which fail to provide enterprise caliber features.

Here are some guidelines to evaluate services for their ability to deliver compliance, long-term storage capabilities and access controls:

1. Are there specified integrity and identity controls (repudiation technologies) to ensure files being stored are not altered, and files in transit are not corrupted?
2. Is the encryption technology FIPS certified and will you control the encryption keys?

3. Does the platform afford authentication and authorization controls?

4. Does the service provide nearline, online, and archival storage, and offer systematic backup schedules to accommodate the need for continuous data protection?

5. Does the archival component have the capacity to retain documents for 6 years?

Tape is not a secure backup solution.

Authentication and authorization refers to “who” can gain access to your network and “what” they can access and change. These security and privacy controls protect data while it is on your network, but are lost when the same sensitive information is transferred to tape. Anyone in physical possession of tape can potentially gain full access.

Even if security and compliance were not an issue, the volume of data now required to manage a practice is stretching the limits of tape. Missed backup windows and corrupted tapes cost healthcare a great deal. It is not uncommon for staff within a healthcare setting to spend 15 percent of their time managing backup and recovery. Offsite backup, in contrast, can deliver the benefits of security and privacy without adding further financial strain.

Marc Gonzalez is Chief Operating Officer of Site 2, a technology firm located in Scranton providing disaster recovery and business continuity services to healthcare, financial, accounting, legal and governmental organizations. For more information visit www.site2bc.com