Running out of Room for Data: HIPAA Requires Healthcare Organizations to Re-assess Data Storage

by Frank Brick

Computer systems are feeling the effects of HIPAA. That's because the act's privacy and security rules require covered entities to securely store and manage more data than ever before. The latest computers to feel the effect are those in small covered entities, where the security rule takes effect this month.

With organizations facing a growing demand for capacity, storage infrastructure has become integral to HIM strategy. Organizations require solutions that provide flexibility and control without dramatically increasing the cost of maintenance or decreasing their service capabilities. This is especially true of smaller organizations with fewer IT resources.

Many entities are seeking solutions off-site. Gartner, the IT research and consulting firm, estimated in 2005 that half of healthcare organizations with long-term preservation needs would turn to outsourcers in the course of that year. Off-site storage can offer help in expanding and managing data storage and in meeting HIPAA privacy and security requirements.

Data Retention Challenges

Retention requirements for patient information vary from state to state based on each state's laws. However, HIPAA states that covered entities must be able to produce an accounting of disclosures as long as six years after care and may rely on disclosure logs, authorizations, or other forms to comply. HIPAA implementation policies and procedures also must be retained for six years from the date of creation or the date when last in effect, although there is no HIPAA requirement that these be maintained electronically. The HIPAA security rule requires that all this information be retained in a secure manner.

Each information type must be stored, secured, and made accessible. For each of these different types of data, each with different lifecycles, it is likely that varying types of information will be handled and controlled by different solutions with varying degrees of security, retention, and accessibility as it moves from disk-based to optical or tape or some yet-to-be-invented storage solution. Add to this the complexity of geographically dispersed information and the handling of data as they move between health plans and healthcare providers, and the issue of data security and privacy takes on a life of its own. As a result, multiple storage solutions will need to seamlessly coexist within a healthcare organization to manage the various types of data. It is unlikely that any one storage solution can cost-effectively provide this degree of security, control, accessibility, and retention duration for all data types.

HIPAA should be viewed as more than just a package of policies, procedures, and penalties. With the growing complexity and regulation comes an equally unprecedented opportunity for healthcare organizations to re-evaluate their current storage management solutions, practices, and processes.

In turn, healthcare organizations of every size are evaluating new data protection solutions and the associated processes and controls to meet compliance requirements. But many are reluctant to migrate to complex or monolithic new storage architectures to manage this compliance. Others don't have the time.

Many businesses instead are looking for solutions that not only fulfill their compliance requirements, but also deliver added value such as reducing downtime, eliminating data loss, reducing storage costs, reducing human error, and enhancing operational efficiencies--all with a demonstrable return on investment.

Seeking Solutions Off-Site

Storing and protecting data under HIPAA is much different than in years past. Today's storage solutions must address the data resilience, security, privacy, and accessibility requirements of the different types of data across dispersed business locations. These solutions also need to guarantee service levels in order to provide healthcare organizations with the confidence, control, and protection they need to ensure HIPAA storage compliance, while dramatically improving the quality of the service they provide to their customers.

Remote data protection can help healthcare organizations quickly and cost-effectively move data off-site for backup reliability, offer multiple levels of data security, and deliver rapid on-demand restores--all without investing in new storage equipment or resources. Most importantly, key resources can stay focused on critical revenue-generating and customer-facing projects because of the fast start-up times and minimal resource requirements needed to set up remote data protection.

Remote data protection can contribute to HIPAA compliance in the following ways.

Reliability--Healthcare organizations need to identify and categorize data based on type and provide the appropriate level of protection based on the degree of risk and exposure for each type. Remote data protection uses disk-to-disk backup and retrieval. Data are then preserved on tamper-proof media. This provides long-term data retention to protect data and ensure ready retrieval while eliminating manual handling of removable media, which contributes to privacy compliance.

Security--With the increased visibility of viruses, hackers, and internal company sabotage, healthcare organizations may be uneasy about threats to security and privacy. From desktop to server to backup to archival, remote data protection protects data with a secure chain of custody. An organization's data should be stored at a highly secure, off-site location, ensuring that critical records and communications remain encrypted and protected until needed.

Centralization--It is estimated that 60 percent of company data are created and stored outside of the corporate data center.[1] Therefore, it is imperative to implement storage solutions that centralize these data to ensure they are properly categorized and protected according to the company's verifiable policies and procedures. The encrypted transport and storage of an organization's data to disaster recovery centers ensures information is protected at a secure facility away from the primary server facility and made accessible only to those authorized to access it.

Scalability--As the amount of data under regulatory scrutiny continues to increase, today's storage systems need to scale--seemingly on demand--without creating undue operational complexity or undermining reliability and performance. Furthermore, infinitely scalable storage infrastructure is designed to keep up with this capacity growth using data lifecycle solutions that meet even the longest-term data retention needs, while minimizing the amount of data storage required.

Accessibility--Today 24/7 access to data is the expectation. Data need to be readily accessible by doctors, nurses, and health plans. Remote data protection provides a secure, Web-based repository available for anytime, anywhere access by authorized personnel. Multilevel authorization ensures confidential restoration and search of electronic records.

Service quality--No two organizations' data protection needs are alike. Tolerance levels in recovery point objectives, recovery time objectives, restore times, and frequency of backups can vary significantly. However all organizations have the ability to provide the best service quality at the lowest possible cost. In turn, service quality directly affects the return on investment for the data protection solution. Hence, tuning the service quality to optimize the solution for the organization will ultimately determine its effectiveness, not only in ensuring HIPAA compliance but in proving value-added benefits such as reducing downtime and costs while improving backup frequency, reliability, and restore times. With remote data protection, service levels are often guaranteed, so service is financially backed to protect the organization from loss and downtime disasters.

Embrace the Future

The transformation to an electronic environment and HIPAA are changing the future of data protection. The question is how an organization responds to this change. Does it simply view HIPAA as a set of guidelines and rules to be enacted and complied with? Or does it see HIPAA as the catalyst for change; an opportunity to revolutionize the way it stores, protects, and recovers data? With remote data protection, the power to embrace chance is easier and closer than ever before.

Note

1. Sigarto, Sam. "Driving New On-Net Revenue with Remote Storage Services." XChange October 14, 2004. Available online at www.x-changemag.com/webexclusives/4ah14_112117.html.

***Frank Brick** (fbrick@arsenaldigital.com) is the chairman and CEO of Arsenal Digital Solutions based in Cary, NC.*

Article citation:
Brick, Frank. "Running out of Room for Data: HIPAA Requires Healthcare Organizations to Re-assess Data Storage" *Journal of AHIMA* 77, no.4 (April 2006): 56-57,64.