Complying with the Privacy Rule during a Disaster. Part 1: An Overview of Plan Development, Data Backup, and Recovery

by Aviva M. Halpert, MA, RHIA, CHPS

Disaster management for an HIM department is an iterative process with four identifiable phases that cycle continuously: plan development, back-up, recovery, and interim management. In subsequent iterations of the cycle, plan re-evaluation replaces plan development.

Regardless of which phase an organization starts with, it must go through them all. If a disaster occurs before a plan is developed, the institution must enter mid-cycle and start with whatever rudimentary recovery is necessary. It may even catapult directly to interim management.

This article outlines how healthcare organizations should deal with plan development, data back-up, and recovery during a disaster. It is the first in a two-part series. In May 2008 a second article offers a look at the management and privacy-related aspects of this special management topic.

Creating the Plan

The IS disaster management plan should be inextricably linked to the institution's overall disaster plan. Furthermore, although the security rule applies to electronic protected health information only, in order to comply with the privacy rule back up and recovery of all protected health information (PHI) must be provided, for regardless of its origin or medium.

The security plan requires procedures for restoring data, responding to a disaster that damages systems containing electronic PHI, recreating copies of destroyed electronic PHI, and enabling functioning in emergency mode.[1-4] But a functional back-up plan must go further. It must include processes for backing up all data on all systems, as well as steps for recreating all components of the health information system. This would include description and location of all components of the electronic, hybrid, or paper records, and the configuration of any network, hardware, and software deployed.

The functional back-up plan must include processes for recreating data tables, contracts, licenses, and policies and procedures. It must also assign responsibility for each component and include secondaries should key individuals be inaccessible or incapacitated. The plan should include an estimate of how long the institution or provider can continue to function at various stages of recovery.

The privacy rule, normally more prescriptive than the security rule, implies rather than mandates the need for a decision-making process that provides guidance regarding when to follow existing procedures, under what circumstances to operate in emergency mode, and how that decision will be communicated. Both the decision-making process and the emergency mode functions should be developed in advance of a disaster, when risks and benefits can be thoroughly and carefully explored.

The plan should lay out and standardize emergency mode functions such as:

- A communication plan for informing staff the scope of the outage, the extent of resources disabled, and the extent of recovery and restoration as it occurs
- Minimal documentation requirements
- Emergency registration sets that can double as a source of patient identification mid-crisis and, ultimately, a means of filing the patient's PHI
- An emergency paper chart that enables and expedites the standards agreed upon
- Downtime procedures for paper documentation

- Stickers for allergies and other emergency flags
- Standardized filing procedures based on a predetermined manual numbering system that can be accessed at a later date to retrieve emergency mode documentation

The plan should lay out the criteria that will determine how crucial decisions will be reached; for example:

- Whether emergency visits should be back loaded into the master patient index
- Whether emergency records should be integrated into existing records, regardless of whether they are in paper or electronic format
- If emergency records are not integrated into existing records, whether they should be interfiled or stored separately

The plan should account for the security of the premises, since the greater the disaster, the less likely that the perimeter of the premises will be secured and the greater the risk that PHI will be accessed inappropriately. Plans for physical security of PHI should be developed in advance for various degrees of disaster, including designating or preparing metal cabinets, preparing schemas for maintaining staffing rosters, and creating temporary ID badges for volunteers and other first responders who will need access.

Back Up

A disaster plan must comprise both a mechanism for backing up data before disaster hits and for recreating it when systems crash. It must also provide a procedure for documenting concurrent clinical findings during the disaster in a manner that will be retrievable after the disaster recedes.

The actual back up of all the elements outlined in the plan should be implemented as soon as feasible. In all likelihood there are a variety of smaller back-up plans and processes that are already in place. All existing plans and processes should be surveyed, evaluated for compliance, and either included in the plan or replaced with a compliant version. No back-up process should be discontinued until a replacement process is available for immediate implementation.

Physical security is vital at the back-up site and during the recovery process. Access to data backed up off-site should be subject to the same protective controls as access to on-site data. Only authorized personnel should have access to such back-ups during the storage process and any subsequent retrieval and recreation of lost data. All access should be tracked and monitored. Data that are carefully backed up on media that are not protected from theft, flood, fire, or other risk will be no more available if a disaster hits than data that were not backed up at all.

Recovery

Data recovery is the part of the process least affected by the privacy rule. It is important to remember, however, that in order to provide future patient access to medical records, enabling the right to amend a record or to respond to authorization to use and disclose PHI, the PHI must be restored in a usable format in a relatively quick and efficient manner. Standard data recovery principles should be applied during the planning and back up periods, including:

- Provisions for reading data that were created on applications that may no longer exist by transforming the data into readable format prior to “sun-setting” a system
- Implementing data retention policies that include predetermined data destruction timetables
- Maintaining the currency of the backed up versions of policies and procedures for recreating the network environment, as outlined above
- Developing a realistic estimate of how long the institution can go without preexisting data and creating an interim plan that realistically matches the anticipated recovery timetable

Once the disaster itself has subsided the recovery plan must take into account the eventual need to comply with patients’ rights, including the right to access their entire medical records or designated record sets, amend their records, and receive an accounting of disclosures. Documentation will be critical for billing, providing birth and death certificates, and for enabling patients to pursue—and the institution to defend against—litigation.

The obstacles to achieving these goals during the disaster are the makeshift nature of the documentation process, the inevitable shambles of the physical environment, the rupture in the communication process, and the unavoidable use of untrained volunteers. The long-term impact of these obstacles will be skimpy documentation and scattered chart components. The primitive and makeshift nature of filing and indexing will render later retrieval efforts problematic.

Despite the most carefully laid plan, disasters by their nature include circumstances that cannot be anticipated. Although a well-designed plan will anticipate many decision points, it will not be able to anticipate all of them. It should, however, provide a procedure for making decisions under fire.

Notes

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Law 104-191. 45 CFR 164.308(a(7)(ii)(B).
2. HIPAA. Public Law 104-191. 45 CFR 164.308(a)(7)(i).
3. HIPAA. Public Law 104-191. 45 CFR 164.308(a)(7)(ii)(A).
4. HIPAA. Public Law 104-191. 45 CFR 164.308(a)(7)(ii)(C)

Reference

Murphy, James C. “Disaster Recovery in Healthcare Organizations: The Impact of HIPAA Security.” Presentation. SANS Institute 2004, November 24, 2003.

Aviva Halpert *(aviva.halpert@mountsinai.org) is chief HIPAA officer at Mount Sinai Medical Center, NY.*

This article is first in a two-part series. See part 2 in May 2008 for a look at the management and privacy related aspects of this special management topic.

Article citation:
Halpert, Aviva M.. "Complying with the Privacy Rule during a Disaster. Part 1: An Overview of Plan Development, Data Backup, and Recovery" *Journal of AHIMA* 79, no.4 (April 2008): 60-61.