Planning for Disaster: Later is Too Late

DATA-PROTECTION LESSONS LEARNED FIRST-HAND

By Cynthia M. Pittmon, CHBME

To comply with the ever changing federal guidelines, I took my medicine like most others in this profession and prepared our Disaster Recovery Plan (DRP).

The goal of the DRP is to guard against the exposure or loss of Protected Health Information (PHI), in the event of an emergency or disaster.

Never in my wildest dreams could I have imagined the recent devastation wrought by hurricanes Katrina and Rita. Although not directly affected by Katrina, we were threatened by Rita and spent a great deal of time reviewing our DRP. The experiences of a fellow HBMA member helped shape some changes we made to our DRP, and with her permission I will share some of the lessons she learned.

An effective emergency plan depends on the ability to proactively maintain company-wide communications and access to key emergency information.

The HIPAA deadline of April 20, 2005 included the Administrative Safeguards section (164.308) of the security rule including the contingency plan standard. This plan requires that covered entities "*establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.*"

The rules continue to include requirements for *"…an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures…to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed."*

The following definitions put the planning process into perspective:

DISASTER:

1) *A sudden, unplanned calamitous event causing great damage or loss.*
2) *Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time.*
3) *The period when company management decides to divert from normal production responses and exercises its disaster recovery plan.*

DISASTER RECOVERY:

1) *Activities and programs designed to return the entity to an acceptable condition.*
2) *The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.*

The contingency plan standard contains these five implementation specifications

(A) **Data Backup Plan** *(Required). Establish and implement procedures to create and maintain retrievable exact copies of PHI.*

The intent of backing up data is to help ensure its availability by transferring and storing duplicate data at a secondary location. However, simply transferring data to another environment without verifying its integrity or the ability to restore it within a defined business timeframe is a recipe for disaster. At the time Katrina hit, my friend was utilizing two computer systems, one traditional in-house server system and one remotely-hosted Application Service Provider (ASP) version. Prior to the hurricane's arrival, she sent a copy of her back-up tapes from her in-house system via overnight courier to her vendor for safekeeping. Unfortunately, she later learned that the back up tapes were unusable, necessitating a restoration from back-up tapes that were one week old.

The data on the ASP system was unaffected as its servers were several states away. This enabled her employees and other authorized users to have immediate access to the data. Claims processing and billing could continue without much difficulty as soon as power and Internet access was available or once her staff relocated to an unaffected area.

(B) **Disaster Recovery Plan** *(Required). Establish (and implement as needed) procedures to restore any loss of data.*

In its simplest form, disaster recovery can be described as the ability to restore vital and/or critical technology systems in the event of a business interruption—be it from human, technical, or natural causes. Recovery focuses mainly on technology systems, encompassing critical hardware, operating and application software, and any tertiary elements required to support the operating environment. Your software and hardware should be inventoried and monitored.

(continued on page 16)

(***Contemplating Compliance*** *continued from page 14)*

Once back-ups were restored and Internet service was reestablished, work could begin anew for those affected by Katrina. However, the 20-foot wall of water that hit the office destroyed twenty years of business documents in filing cabinets and all of the PC's that had been placed protectively on desktops Future plans will include moving those files and PC's to a higher floor if available. Another option will include scanning and emailing important papers to a mail host such as Yahoo or MSN.

(C) **Emergency Mode Operation Plan**. *(Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.*

Think of your emergency operating plan as the action plan that defines how your business will operate under less than optimal conditions. The intent is to train and prepare employees for what will be required to maintain operational integrity. However, in the case of Katrina, office buildings were destroyed and many employees suffered either severe or total home destruction. Basic infrastructure was not just damaged, it was obliterated.

It is very difficult to operate when one-third of your workforce cannot or will not return to the area or their spouses are transferred to other parts of the country. Communication in the area was impossible immediately after the storm. Six weeks later, telephone service was still unreliable, making it very hard to contact employees, clients, and vendors. This caused a revision in our own DRP to include the use of an alternate toll-free telephone number with a geographically remote vendor where employees can leave messages and contact information.

Key operating processes linking people with technology are vital to the ongoing operations of any business, but receiving electronic information may be impossible when even a hospital's systems are inoperable. Generating an effective emergency operating plan depends on the ability to proactively maintain company-wide communications and access to key emergency information. Each action plan requires mock exercises along with employee training, but nothing envisioned could prepare the affected businesses or employees for Katrina. Our revisions now include e-mailing our DRP to key personnel at their Yahoo or MSN e-mail for easy access if our intranet is inoperable and staff can be relocated outside of the affected area.

(D) **Testing and Revision Procedures.** *(Addressable). Implement procedures for periodic testing and revision of contingency plans.*

An important step toward business continuity is exercising each action plan to determine vulnerabilities and strive to reduce them. Complete elimination of all business vulnerabilities is impossible, but a well-developed, process-oriented exercise can reduce the likelihood that unplanned interruptions will cripple business operations.

Updates should be done quarterly on resource information such as contact, equipment, and vital records lists, which tend to change frequently. Reviews should be performed semi-annually on recovery strategies and procedures and should include a drill with employee training. A significant change, such as reorganization or implementation of new software, also requires reviews and updates. An exercise should be performed annually, at a minimum, and include alternate site tests (internal and functional). Orientation should be done for each new employee covering the DRP.

(E) **Applications and Data Criticality Analysis.** *(Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.*

Generating an effective emergency operating plan depends on the ability to proactively maintain company-wide communications and access to key emergency information.

A business impact analysis has several capabilities and objectives:

- To identify, prioritize, and assess technology systems, applications, data and processes within the daily operating environment
- To identify how long a particular system or application can be offline before the business is affected
- To identify when the information-recovery process begins and how much data may be lost between system backup time frames
- To identify the "hard" financial losses incurred during a business interruption

Findings of the business-impact analysis are the foundation for developing effective business continuity and disaster recovery plans.

WHERE TO BEGIN?

While writing a Disaster Recovery Plan has never been an easy task, the devastation faced by the victims of hurricane Katrina has given us all a lot of material to work with. Ask yourself the following questions to begin the process for your business:

- What is the purpose of our plan?
- What types of disasters might we encounter? Arrange them by severity from the worst case scenarios down to minor inconveniences.
- Where are the dangers to our *(continued on page 18)*

(*Contemplating Compliance* continued from page 16)

Management Information Systems relating to PHI? How will we protect it and how will we restore it?

- Does the Disaster Recovery Plan include procedures to log system outages, failures and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan?
- Where will the staff work if the office is destroyed or damaged?
- Have we conducted an assessment to categorize the functions in our office as to which is essential, necessary, and desirable?
- Who will be responsible for which areas of recovery? Have we written functional team job descriptions?
- What insurance coverage do we have? Does it cover business interruption? What types of disasters are covered?
- How will we communicate in a disaster? Remember that land-line telephones, cellular phones, and Internet service might be inoperable.
- Do we have a current database with the names, phone/page/fax/cellular numbers, e-mail, and postal addresses of everyone on the crisis team? (Give everyone a laminated card for their wallet with this information.)
- What are our recovery procedures?
- Have we reviewed our Disaster Recovery Plan at least annually?
- Have we tested the plan periodically to ensure that PHI and the systems needed to make PHI available can be restored or recovered?

IN THE MIDST OF A CRISIS:

Remember that employees may be facing their own difficulties in the time of crisis and no one will be as committed as the owner/manager. You will need to continue monitoring the crisis, acknowledge the company's responsibilities to its clients, take prudent action to resolve issues as quickly as possible, inform those affected by the crisis, and strive to keep everyone updated.

HIPAA's intent is to protect PHI and restore any loss in a timely manner. Therefore the DRP must be easily available to the necessary personnel at all times and they must be trained to implement the procedures. There is an old saying that "no one wants to buy an umbrella when the sun is shining," but now that we have seen what havoc a storm can wreak, let's make sure we are ready for the next one. ▲

RESOURCES:

Disaster Recovery Journal
Federal Register

Cynthia M. Pittmon, CHBME, is the owner of Specialty Group Services in Longview, TX. She can be reached at cindy@sgsmedical.com.

(*Perspectives on HSA's* continued from page 17)

Consumer ownership

- 94% of consumers use generic drugs when available without a formulary
- 55% report being more likely to think twice about going to the doctor for minor health needs

What Do HSAs Mean to Billing Companies and Providers?

Many of the benefits of HSAs are derived by allowing the consumer to be in control of the financial transaction on an individual basis. In other words, if an insurance company is not responsible for the first $2,500 of the health costs for a patient, it will lower the premium costs. To billing entities, the first $2,500 becomes collectable from the patient's HSA (self pay) rather than from the insurance company.

To add insult to injury, most plans still require the provider to submit the claim to the insurance company for pricing and then, after adjudication, collect the funds from the patient's HSA using either a credit card or a check from the guarantor.

As HSAs become more popular, your clients will face delays due to the re-pricing requirement, additional costs in the credit card discount or fees, and perhaps greater collection risk due to employee turnover and a general lack of control over the HSA. For example, if an employee spends all the money in the HSA on prescription drugs that do not count towards the deductible on the HSA plan, then services rendered by the physician would be collected directly from the patient, which may be difficult.

There are many issues that we as billers will face with HSAs, all of which will add significant costs to the process of collecting physicians' money. Additionally, with the employees becoming the consumer, we are seeing more negotiation going on directly with the provider for elective procedures or non-plan costs. We have seen a few Web sites, much like e-bay, comparing services and costs of physicians.

I would say from my perspective as an employer and employee HSAs are awesome. As a billing company and software developer, I think they represent a potential cost increase which we can and have solved with technology (on-line bill payment, electronic access to HSA plans, etc). For physicians, HSAs will force them to answer more questions on what they are doing and why. They may even have to become more consumer driven. But in the end, people will pay for their health.

If you have comments or experiences, I would love to hear about your perspective. ▲

T. Scott Law, CPA, is CEO at Zotec Solutions, Inc. in Carmel, Indiana. He can be reached at slaw@zotec.com.