When Disaster Strikes, Will You Be Ready?

Disaster recovery planning always seems to get pushed to the bottom of the to-do list, despite constant reminders that it’s a wise thing to do. The devastating impact of Hurricanes Katrina and Rita on individuals and businesses is the most recent reminder of the need for disaster preparedness.

Taking steps today can help to expedite computer data recovery should a disaster such as a flood, earthquake, fire, or terrorist act occur.

A HIPAA-Approved Plan

If you have determined that you must comply with HIPAA, then you are automatically required by law to develop and regularly test a computer disaster recovery plan. Even if you are not required to comply with HIPAA, having such a plan is good practice because it will help you to think through all of the steps that may need to be taken to securely recover any lost data.

Below is a sample Computer Data Disaster Recovery Plan for solo and small group practices that is part of the larger compliance process associated with the HIPAA Security Rule. Larger practices with significant staff and computer systems can start with this plan and add steps as needed. If you work in a large institution, talk with the HIPAA Security Officer about your institution’s disaster response plan.

Sample Computer Data Disaster Recovery Plan

This plan assumes that regular back-ups of important computer data are being created and stored in a secure offsite location.

Pre-Disaster Plan

Choose someone to be in charge of developing, implementing, and testing your plan; this person will become your Security Officer. In a solo practice, this will be the individual psychologist. In a small or large group practice, one of the psychologists or office staff can be designated as the Security Officer.

1. Create regular backup copies of important computer data on tape, CD or external hard drive and store the backup in a secure offsite location. If you run a busy practice with a lot of data activity each day, you may want to back up daily or several times a week. For others, preparing less frequent backups may be sufficient.

2. Establish a relationship with a computer technology support service or person. Such services can be obtained through retailers, in the telephone book, or by referral from a colleague or friend. Engage them to do a maintenance review of your system to ensure that all software is up-to-date and that your computer is virus-free. This will also give them an opportunity to get to know you and your computer system.

3. Provide your computer support person with a list of the computer hardware and software you will need in case of a disaster.

4. Keep a list of all of your user names and passwords in a secure off-site location for easy access in an emergency.

5. Add an uninterruptible power supply to your computer system. The battery will provide power for about ten minutes after losing commercial electricity. This is enough time to save important documents and shut down your system in an orderly fashion.
Disaster Identification and Notification
Staff encountering a computer data disaster situation (such as a flood, hurricane, fire, earthquake, etc.) will immediately report the disaster to the Security Officer. A disaster is defined as a major event that halts business operations, threatens the physical security of the office, and/or destroys or could potentially make important computer data unavailable for more than 72 hours. The Security Officer determines if the disaster requires implementation of the Computer Data Disaster Recovery Plan. If so, the Security Officer immediately informs all staff who may be affected.

Disaster Recovery Plan
Mitigation – Under the direction of the Security Officer, staff immediately begins taking steps to mitigate any obvious and apparent security breach(es). Staff attempts to restore, recover, salvage and secure any computer hardware, software, or files that are no longer secure due to the effects of the disaster.

Staff and the Security Officer supervise emergency or other workers assisting with disaster recovery to ensure that such workers do not inadvertently come in contact with confidential information.

Staff reports any security breaches to the Security Officer, who takes steps to inform appropriate individuals or entities of the breach, the steps taken to mitigate the breach, and how the computer data has been secured, if required and/or appropriate.

Recovery – The following list of activities is used only as an example. Generate your own list of the activities unique to your practice and determine the order in which to restore them.

In the event of a computer data disaster, the following activities will be undertaken in this order:

Obtain Space for Disaster Recovery Operations
The Security Officer immediately takes steps to find a location in which to undertake computer disaster recovery operations. The space will be physically secure (e.g., it can be locked securely), and provide the services needed for computer data disaster recovery (e.g., electrical power, compatible computer(s), telephone connections, etc.).

Restore Computer System and Backup Data
1. The Security Officer will obtain appropriate computer hardware and recreate the computer system.
2. The Security Officer will load the required software onto the computer hardware.
3. Using backup data, the Security Officer will restore files containing patient data and other critical business functions in the following order:
   a. Practice management software and backup data
   b. Financial software and backup data
   c. Calendaring/Appointment software and backup data
   d. Email communications software and backup data
   e. All other necessary software and backup data

continued on page 6
4. The Security Officer will take steps to ensure that the recreated computer system and software are password-protected and regular data backups are made.

**Configure Space to Support and Provide Services**
If appropriate, the Security Officer and staff obtain the office equipment needed to configure the computer disaster recovery space to support and provide services. If appropriate, staff communicates with patients about the temporary computer system and the steps being taken to recover and secure confidential information.

**Declaration of the End of Disaster Recovery**
If, after evaluating the disaster recovery operations, the Security Officer determines that the disaster is no longer a threat and that the office systems have been appropriately restored and made secure, the Security Officer will inform staff that computer data disaster return to regular operations.

**Post-Disaster Evaluation**
Following a return to regular operations from disaster recover operations, the Security Officer and staff will evaluate the disaster recovery plan and make any appropriate modifications.

**Regular Testing and Evaluation**
This disaster recovery plan will be tested annually by the Security Officer and all relevant staff and modified if appropriate.

FIND OUT MORE

To learn more about backing up your important computer data, visit the Practice Management section of APAPractice.org.