Is Your Practice's Information System Protected?

Alan Sivek, C.P.H.I.M.S.

July 21, 2005

Once again, we are in the midst of hurricane season and South Floridians are concerned with their preparations for the threat of a hurricane. It is imperative that your disaster plan includes appropriate protection for your information systems. Although hurricanes seem to be the imminent threat, you need protection year round from a multitude of potential threats.

As technology increases, more and more information has become computerized, such as billing, appointments, accounting, payroll, and medical records. It is important to have a comprehensive, update-to-date plan for protecting and recovering your practice's information systems. Currently, the foremost threat on people's minds is a hurricane, but possible threats range from external threats (hackers, viruses, fire, and other disasters) to internal threats (employee sabotage, hardware breakdown, and software corruption). Did you know that **94% of businesses that suffer a major data loss go out of business within 2 years?** Today more than ever, it is necessary to utilize appropriate technological policies and have a disaster recovery plan, which are both requirements of HIPAA.

Are You Prepared?

The following questions are a basic self-audit. Do you have a recovery plan, and is it update? What issues should you address so that you will be prepared for future disasters?

- Do you have a written Disaster Recovery Plan? If yes, when was it last updated?
- Have you identified your critical and non-critical files?
- Do you regularly back-up your files, both critical and non-critical? Have you verified the backups, to ensure they are working properly and your files can be restored from those back-ups? Are back-ups taken off-site?
- Do you have a plan for emergency communications with your employees? Do you have current contact information for your employees?
- Do you have a plan for emergency communications with your patients?
- Do you have a procedure for closing the office during normal business hours?
- Does your plan include all insurance policies and contact information?
- Does your plan include contact information for vendors, in case you need to replace supplies and equipment?
- Do you have a current inventory of equipment, supplies and paper records?
- Have you discussed your plan with your staff and assigned responsibilities?
- Do you have at least one copy of the plan off-site?

While we hope to never have to employ our disaster recovery plan, it is more than likely that we will have to prepare for a hurricane. With a properly maintained plan, the staff will have the necessary information on how to efficiently handle the office preparations. Once the office is prepared, if necessary, you can close the office early and allow your staff to prepare their personal lives. For tips on hurricane preparedness, see the Palm Beach County Medical Society's website, www.pbcms.org.

Ongoing Protection

While a disaster recovery plan prepares you to weather a storm, you need to protect your information systems on a continual basis to prevent disruption of your day-to-day operations. Ongoing protection includes virus protection, firewalls, anti-spam programs, password maintenance, updating applications, etc. Most practices connect to some entity (e.g. the local hospital system, a clearing house, an insurance company, regulatory body, email, etc) through the internet. It is imperative to have anti-virus and firewall software that is updated frequently, on your computers to protect your practice's information, just as you should with your home computer.

Equally important to the ongoing protection of your information system is password maintenance. Each staff member in your practice should have their own password, some practices have one password that several staff use to logon to the computer system. Also, if the security in the software always you to specify what a user can and can not do. You should setup different rights for different users. Finally be sure to delete the passwords of employees who have left the practice.

As more and more information is processed and stored on your computer systems, you must constantly preserve and protect your information system and data.