Reprinted from the April 2011 issue of Impact magazine with the permission of the Private Practice Section

Backing Up Or Bowing Out?

By Steven Presement

Consider this. You sit down in front of your computer system and instead of the usual bevy of icons, you are confronted by the blue screen of doom. Moving our story forward, you have had several people look at your computer, escalating all the way to finally calling in a professional to take a look. The news is not good. Somehow, your hard drive has been wiped out. It is, after all, a simple piece of electronics, full of moving parts, that has a limited life span. The "techie" turns to you and suggests that this is a simple problem—you'll get a new hard drive and then all you have to do is restore your backup.

And this is when it hits you: Either you have no backup, or what you have is ancient. You begin to prepare a mental inventory of what was on your computer. E-mails. Correspondence. Client records. Financial information. The gravity of the situation begins to settle in—you have nothing. You don't even know who owes you what. If the IRS or some federal oversight agency walked in tomorrow, you'd be done.

Ask yourself, "Could this happen to me?" Be honest—if you feel at all unprotected, this is something you need to deal with immediately. There are 3 key questions to consider when developing your backup strategy: what, how, and when.

The first question is *what* needs to be backed up? Windows does a generally good job of keeping your most important documents in one area, either under your "My Documents" folder or in a directory called "Documents and Settings." Unless you specifically save documents elsewhere, all of your created documents should reside in one of these locations, along with your favorite websites and Outlook e-mail data. Remember, if you are using accounting or practice management software, be sure to include those files in your backup; it is doubtful they will be included automatically.

Next, the key question: Exactly *how* are you going to perform these backups? All backup methods can be funneled into two categories: on-site and remote.

On-site backups involve you copying your relevant data to a local storage device such as a backup hard drive or flash drive, something that you physically attach to and detach from your computer. Typically, you are the one to manage this process. You plug in the backup device, wait for the backup to be performed, and then unplug and store the device. Backup devices can include an external hard disk drive or a flash drive (those little memory sticks). Many external backup hard disk drives come with software or have a "1-button" approach that essentially makes a complete copy of your computer's hard disk drive to the backup device. Some devices will even allow you to schedule this process. If you use a flash drive, you will generally need to copy your important documents manually.

The downsides of employing on-site backups are substantial: (1) you have to remember to actually do the backup, (2) it can be a time-intensive process, and (3) unless you are prepared to take the backup device offsite each night, you are not protected against theft and fire. One other major concern with locally made backups: What would happen if your flash drive were to become lost or fall into the wrong hands? Are all your data password protected? Chances are, they are not—and on that memory key is absolutely everything about you, your clinic, and your patients.

With the enhancement of Internet bandwidth and security, remote backups are becoming an increasingly attractive option. A program is installed on your computer that sends your data, via the Internet, to a remote backup storage service. This can be scheduled to happen at the same time each day (generally after hours) so that your key information is stored automatically offsite every night. There are no hard drives to worry about, no flash drives to lose, and most important, you don't have to remember to do anything—it all happens in the background. It

TECHNOLOGY, continued on page 35

TECHNOLOGY, continued from page 33

is very simple to access and restore your information, all via the web, should it be required.

There are a few downsides to remote backups, the main one being that it does tie up your Internet connection while the backup is happening (which is why it is usually run in the middle of the night). Computers on a wireless network or with poor Internet access may not be able to use this technology. The other downside, minimal as it is, is the cost. Firms like Norton, Mozy, and Carbonite offer this type of service for as little as $5 per month; even a server can generally be backed up for less than $20 to $30 per month.

> Ideally, you should perform a backup once a day, generally at the end of the day.

One last item to consider when comparing these two backup methods: On-site backups keep overwriting themselves; each day, you overwrite the backup from the previous day. If you accidentally mangled a document 2 days ago and your backup has been done since, you won't be able to retrieve the pre-mangled document. Remote backups generally keep a history of backups, making it possible to go back and grab something specific from several weeks ago.

Of course, the other concern with offsite backups has to do with your data. Exactly who is storing this information and how safe is it? You obviously need to find a remote backup company with strong credentials, one that employs data encryption and is fully HIPAA compliant.

Once you have decided how you are going to perform your backup, you need to decide *how often* to do so. The question to ask yourself is, "How far back am I willing go to play catch-up?" Remember, if you only back up once per week, then there is a chance you will have to go back and reenter everything for the past week should you run into trouble. Ideally, you should perform a backup once a day, generally at the end of the day. If you elect to use a remote backup solution, then it is quite simple to set your backup to occur at the same time every day automatically. On-site backups should be your last order of business each day. Remember, on-site backups should leave the clinic with you.

Whatever method you employ, and however often you choose to employ it, is better than not doing anything at all. The cost and time to perform backups is minuscule compared with the cost and time involved in recreating the past. ■

Steven Presement is the president of InTouch Practice Management Software systems and can be reached at steve@getintouch.us or at 888/298-4562.