

What to do about backup?

When one of our customer's office was burglarized and some computers stolen, I was asked to start researching offsite data backup options. Until this time my company had always recommended a tape drive or REV drive (which consists of small disks, like a ZIP drive), but this practice had over 150 GB of data and that did not fit easily onto any removable medium. So, off to the Internet I went looking for the best solution to the question of 'How do we safely backup our practice data?'. It turned out that even this question needed more clarifying as in: safe from what? Burglary? Flood? Fire? Computer failure? The answers turned out to be different depending on what you are trying to avoid, for example keeping your server in a locked rack bolted to the floor will certainly protect you from theft, but definitely not from Hurricane Katrina. And copying your data to an unspecified site via the Internet would protect it from fire or flood, but how do you restore it to be able to use it again? And since the topic of backup turned out to be more than enormous, in this article I am going to go over some considerations regarding what to think about when looking at your options. I will go in-depth on solutions in subsequent articles.

How much data do I have (that I want to save)? This is obviously where you start, you want to include your financial data of course, your patient's charts (assuming they are in a database somewhere), all documents, email correspondence (if it could contain critical communication), patient photos, lab results, ultrasound images, etc.

What do I want to save it from? It is important to assess the probabilities of impending disasters in order to decide the mode of backup with which you are most comfortable. Of course no one can predict or foresee every catastrophe, but you can plan for those that seem more probable when deciding on Internet, tape, redundant drives, etc.

How often do I want to back it up? For most businesses that should be every day, but of course you want to run an incremental backup every day, not a full backup. An incremental backup is only going to take those files that have changed since the last backup and replace them. However, due to mechanical failure of backup devices and the fact that most are a form of magnetic media, some IT people recommend rewriting the full backup every year or so.

How long does it take? In the case of our customer with 150GB of data in two separate Sybase databases, it would take about 8 hours to write a full system backup to a tape device. This gets into a very complicated topic because there are so many types of solutions that are based on many different variables including: the speed of the physical device, the speed of the hard drives, the software used to write it, the file format of the backup, even the speed of the Internet connection all play a part in the overall time it takes and also leads us into the next question:

How quickly do I want to get it back? If someone had stolen our customer's server with all her software (practice management, scheduling and EMR) and data on it, it would not simply be a matter of just pulling out a tape cartridge with a backup copy on it, sticking it in the tape drive and then start seeing patients. The software programs have to be reloaded onto a temporary server, all the other workstations would need to reference the new temporary server, plus the backup software would still take over 8 hours to restore a file to a format that could be read by the software. Now the question becomes: do you know where your installation disks are for your practice management, scheduling, and EMR software? I have seen many cases where the physical installation disks have not been seen for years. If our customer had chosen Internet offsite backup they will mail you a copy of your data via FedEx or UPS so add that time in as well.

Where do I want my data stored? Internet storage really sounds like a good idea; it is someone else's problem to maintain integrity, etc. but the more I started thinking about

it, I wondered: What if they got broken into? What if they had a fire/flood/tornado? Where is the data stored, is it in this country? Who has access to it, and how do I know if they're telling me the truth? It is going to take some more due diligence before I am comfortable sending my Quickbooks file to an Internet backup company and I would definitely read everything on their website before transferring any data. Also, if their website is vague, I would ask about their disaster recovery plan(s) as well as HIPAA compliance.

Keep in mind that backing up data is really for the very short-term; for an immediate need to recover. Long term storage is a fallacy; it is really a string of short- to medium-term solutions that are replaced every few years. The tape drives and CD-ROM's that we are using today will become obsolete in a few years and everything will need to be rewritten to a new medium in a new format as technology advances.