

Disasters in the digital age...

As we transform from an analog based x-ray system to the new and better digital x-ray systems, we have new challenges that we did not have with film and chemicals. These challenges are not insurmountable as long as you practice good techniques and go with a supportive vendor who can deliver the who package without crazy tie-ins.

There are several important parts to any digital system: x-ray generation, digital capture, display, image storage, image communication, ease of use, ability to integrate with practice management, support, and disaster recovery. One of the least talked about and most important parts of any digital system is the solution to a massive problem: disaster recovery. Computers crash, get stolen, get viruses, get spyware, and components fail.

All hard drives fail. The chance of your hard drive failing is exactly 100%. When they fail, they can take all of your data with them and make them irretrievable. It's as if your old films and associated records vanished overnight.

This article refers to film a lot, but keep in mind that all of the principles here apply to all data including your practice management system, photos, emails, etc.

Digital vendors can help protect you against disaster, but ultimately it is your responsibility to protect your own data. Think of it like this: you wouldn't leave food burning on the stove and then ask your home builder to be sure that your house doesn't burn down. The time to talk to your home builder was during the construction and then there are still steps to take to protect against disaster at home. You buy fire extinguishers and smoke alarms. You also buy insurance. All of these same principles that you take into account with your home apply to data backup.

So, ask about what your digital vendor does to protect against disaster. And, if their answer ties you to them permanently or makes it very costly to protect or recover your data, run the other way. I can't tell you what other vendors do, but I can tell you what SimonDR does. And what we do is how I protect my own data.

First on all systems, we provide multiple harddrives so that the data is duplicated and you have a local internal backup. This will protect you from a single harddrive failure but leaves you open to fire, theft, vandalism, viruses, etc.

Traditionally, with your other data, you'll backup everything daily using a tape cassette and always make sure that you have one offsite copy. This is always a safe thing to do, but in my experience, tapes are less reliable than harddrives for recoverability. External harddrives are great, but should only be part of the backup scheme.

The advent of the internet and the recent progresses in high-speed service has enabled the online backup business to grow. Services like SimonBackup.com (OK, yes – that's a plug for one of my other companies) allow you to backup all of your data off-site and securely at a reasonable rate. Online backup is highly recommended as the most important part of you data backup scheme.

Long story short: to properly backup your data, have duplicate data to begin with, keep a third copy locally across your internal network, and do online backups. As the last step in the process, test your backed up data regularly performing alternate location restores to ensure that your data has retained it's integrity.

To try SimonBackup for free for 90 days, go to www.simonbackup.com/downloads and click on the link to download the client software for either Windows or Mac. Run the software and create your account. You are then given up to 20 gigabytes of storage for free for 90 days, no strings attached. Should you require more space, please send me an email and we'll arrange it for you. If you need help setting up your software, email me and let me know a good time to have a technician call you, or call my office at 800-835-3852 x130.