"I'VE NEVER SEEN THIS SCREEN/MESSAGE BEFORE, (GULP)"

Bill Palisano
President of Lincoln Archives

Okay, by now you're depending on your information systems to do it all for you, right? You're scheduling appointments, retrieving medical histories/files/charts/images, updating with diagnoses, scheduling procedures, billing insurance, managing staff, etc., etc., etc. Computers are neat, aren't they? They can serve up so much information, so fast, at the touch of a button, simultaneously accessible by the many professionals who care for their patients, and the people who manage medical practices. Yeah, they're really neat. That is, when they work... They don't always work though, do they? Communications are lost, files get corrupted and systems crash. We don't realize how dependent we are on them until they're not there. Then, it's like: 'Uh-oh, hope it's back up soon', or 'man, we can't do much while we're down' and of course (my favorite): 'Damn computer!'
But it's not until you experience a real system outage or data loss that you really understand how reliant you are on these information systems. Then you realize just how important it is that you are backed up and running: fast. Enter your backup plan. Two reasons that you have to have a backup plan: #1: Good business practice (Duh). #2: It's the law (HIPAA Administrative Safeguards Rule). I'm going to address these both, in very simple terms.

#1: Good business practice: "stuff happens". I'm not just talking about a fire, sprinkler discharge, roof leak, broken pipe, pepsi incident, flood, etc. That'll never happen to us, right? Wrong. This stuff does happen, and probably more than you think. There are also many 'quieter' risks: hardware failures (average life of a hard drive is 4.1 years), corrupted files, viruses and of course hackers (reach out to me privately and I'll tell you the story of a local firm who was hacked, and the (Eastern European) hacker encrypted the firm's data – didn't steal it, but held the encryption key for ransom and they paid it; they had no choice. They had 12 hours to wire transfer the money (overseas) or the data would be lost forever). In these cases, you don't even know you've lost data until you try to retrieve it. At that point 'the horse is already out of the barn.'

#2: It's the law: HHS REQUIRES a Risk Analysis, a Standard Contingency Plan, a Data Backup Plan, an Emergency Mode Operation Plan, and Procedures for Periodic Testing. These are all explained in 45CFR 164.306/308 "Administrative Safeguards." So, for basic compliance under HIPAA, you have to have a backup & recovery plan, and you must test it, document it, and revise it periodically.

To be compliant, there are several ways to back up your information. I've worked with medical practices for 21 years and have seen a lot of different ways it's been done. Some I do NOT recommend: Someone (or a s/w automatically) copying files to an external hard drive, and that drive stays right next to the server or primary storage device (it needs to be in a different location). Or, same scenario but someone takes the drive home, to a safe deposit box etc., but the data WAS NOT ENCRYPTED before being written, and leaves office: A BIG No-No. Any time data leaves the primary server or storage repository and leaves the protection of the facility, its security, its firewalls, etc. must be encrypted, period.

Other scenarios work, are fairly inexpensive, simple, and are low touch. You can buy an external tape drive, automatic backup s/w, and tapes for a few hundred dollars (tapes cost less than external hard drives. Hence, multiple backups will cost less vs. buying multiple ext. hard drives). If you go this route: MAKE SURE YOUR SOFTWARE ENCRYPTS YOUR DATA before written. Also, keep a minimum of five (5) full days backups (four of them off-site; 1 in tape drive and ROTATE). A better strategy includes adding weekly, monthly and annual backups. Repeat: encrypt then get backups off-site.

And then there's 'the cloud'. Nowadays, you can't swing a dead cat without hitting several cloud backup companies (just Google: "cloud backup Buffalo, NY" and you'll see). These scenarios can be fully automatic, low touch, highly secure and cost effective. Some require only software installed (no hardware necessary) which encrypts and then streams data off-site to providers secured vault for true Disaster Recovery protection. Some use a backup appliance attached to your network. These systems can be quickly deployed, installed, configured, and up and running. If the provider is good, he/she will assist in creating a backup and recovery strategy (selecting critical data to protect, how many generations of each file, scheduling the backups, creating a retention program), and will test the backups (and more importantly test the restores). He/she can also document the tests which meets HIPAA requirement). Another benefit is that these solutions are typically scalable (as your data needs grow, the solution accommodates it). Many charge only based on the amount of data protected or stored. Hence, there is no up-front cost (Cap-Ex), rather, a pay-as-you-go model (Op-Ex). You can change your strategy on the fly; increase or decrease your protection (and costs); very flexible. (Btw: if your data is hosted somewhere else, it doesn't mean it's backed up to another off-site location. It's just not at YOUR site and is still subject to risk. A good cloud backup provider can actually backup (and recover) your data from your hosted site, just in case...).

So, regardless of which way you protect your data, just make sure you do. And test it. Besides saving on compliance fines, you just might save your firm...