Health Information Compliance Alert

Disaster Planning: Is Your EMR System Disaster-Ready?

Tip: Rate potential disasters from full-fledged crises to small-scale events.

Most hospitals, nursing homes, and practices are dependent on electronic medical records (EMR) these days. That means it's more important than ever to have a plan to secure access to that data even when a disaster strikes your area. Read on to see how you can plan ahead.

Where do you start and what should your disaster plan include? "One of the things we have seen across the country is severe weather," says **Jean Acevedo, LHRM, CPC, CHC, CENTC,** president and senior consultant with Acevedo Consulting Incorporated in Delray Beach, Fla. "While it has always been important to have a plan as to what to do if a hurricane, tornado, flood, or other disaster impacted the practice, now that so many physicians and hospitals keep patient information only in electronic format, the plan needs to expand beyond where will the doctor see patients if the office is not usable."

Let us walk you through the steps to creating a solid plan that will, hopefully, keep your practice up and running even if Mother Nature throws a curveball your way.

Rank Potential Emergencies

You don't want to bog your staff down with a separate action plan for each disaster that might come your way. Start your disaster prep planning by rating potential disasters from full-fledged crises to small-scale events. Then simply educate your team on how to handle each disaster level. This sort of approach could cut your training and response times in half, experts say.

Examples: The aftermath of Hurricane Katrina can be considered a disaster; however, a pipe bursting in a waiting room is a smaller-scale emergency.

"Just as a physician should rate the risk of losing clinical information or a hacker getting access to his EMR, and prepare first for those scenarios that are of the highest risk, disaster planning should follow a similar rating structure," Acevedo explains. "I'm in Florida, so having a plan as to what to do in the event of a hurricane when electricity can be lost for a week or more and how to prevent the office and contents from flooding are the main priorities."

Important: There are some things you simply cannot plan for. As much as you prepare your practice for a variety of scenarios, something may happen that you just aren't prepared for. But having some basic emergency plans will help in any situation.

Do this: Develop a disaster plan based on the amount of resources you'll need to recover.

For instance, if a pipe burst in your waiting room, you might have to cancel or reschedule patients' appointments. That cost, along with any other financial investments (including repair and refurbishing expenses), would correlate with one emergency category. The resources required to recover from a catastrophe like Hurricane Katrina would correlate with a different emergency category.

Work As A Team

Dealing with disasters isn't a job for just one person in your practice. Everyone has to work together, or your disaster recovery plan will fail.

Good idea: Help your staff members, from the front desk clerk to the physician, see how interdependent they are by

asking each one to list his duties within your facility. Next to his duties, ask him to explain how he'd do his job without any outside help. Explain how each employee's role fits into a larger chain. That will help your staff see the importance of working as a unit rather than by themselves.

Focus on Patient Safety, Data Recovery

The first priority in any disaster plan should be the safety and health of not only your staff, but also any patients that are in your office when disaster occurs. "Safety of people, both staff and patients, must always be priority number one," Acevedo says. "Consider having a telephone tree so that everyone knows who to call to let the practice know they are safe, and when the office may expect to open."

Your patient information is your most valuable resource; you just can't recover without it. You must backup your data ⬜ and test those backups ⬜ on a regular basis.

- **Try this:** Coach your disaster recovery or technology team to recover three or four random patients' data each month. That way, if there's a problem with your backups, you'll discover it in time to remedy the issue before a disaster strikes.
- The three most common ways to recover data for a medical practice are:
- **A hot site:** A hot site has exactly the same computers and applications online and ready to take over if your system fails. You can determine an amount of time between when the system goes down and the hot site takes over or it can roll over automatically. The location of the hot site depends on your risk analysis. It can be across town or across the country.
- **Example**: A medical office in Virginia may choose to have a hot site in San Diego.
- **A cold site:** A cold site has most of the same equipment, but is neither powered up nor supplied with a completely current image. You have to manually bring up backup tapes, power up your computers, and possibly rely on fewer machines. This is not the option to choose if you need immediate recovery.
- **A warm site:** A warm site falls somewhere between hot and cold. The equipment is ready, but it may not have the most current backup of your image. This option is more immediate than the cold site, but there is still a delay in recovery.
- **Critical**: You must store your backup files in a secure location. The worst place to store your backed up information? Your office. Choosing an offsite location for data backup is a smart plan. Keep your files in a place that's not subject to the same emergencies as your facility.

Consider geographic disasters as well as the random things that everyone experiences. For a facility in California, earthquakes could affect structures within a large radius, so backups should be sent to an area less prone to that type of disaster.

Opportunity: Many vendors offer secure, remote hosting for your backup files. That way, you save the files electronically and the vendor maintains them in a data center thousands of miles away.

Good news: Web-based solutions allow you to access your files from any location with an Internet connection.

Teach Your Team

Teach ⬜ don't just tell ⬜ your staff members what they should do if disaster strikes. You have to coach them on how to execute their specific part of the plan. And practice will make perfect. When there's a disaster, you want your staff to act on instinct rather than just read from a paper.

Get your employees ready by simulating a disaster and watching how they respond to it, experts advise. "In fact, it's a good idea to run through the documented protocols at least yearly," Acevedo suggests.

Example: Ask the medical records director to call her other key person in the middle of the night. Then ask the key person to produce a telephone list of key people who must show up to handle a disaster. After your staff members go over and agree on a disaster recovery plan, ask them to sign the plan and keep that signature for your records.

The bottom line: Disasters will strike, but you can help your staff feel confident in their abilities to handle the crisis by

practicing, mitigate any privacy or security breaches by producing documentation that shows you coached your employees on how to respond in a crisis, and increase your chances of continuing "business as usual" despite disaster by being prepared. Be proactive rather than reactive. Don't wait for disaster to threaten your practice. Start preparing now.