Health Information Compliance Alert

Security: Don't Let Disaster Recovery Wipe You Out

Expert guidance for a quick, cost-effective recovery plan.

You've written HIPAA privacy and security rule policies, trained your employees and signed business associate agreements. Enter the unthinkable: fire, flood, earthquake. Would you be able to recover from a disaster without losing your shirt -- or your patients' PHI?

Deep Impact?

When you develop your disaster recovery plan (DRP), you have to decide "which information assets containing PHI need to be recovered in the event of an extended outage and in what order," explains **Nancy Place,** a managing consultant with **IBM Business Consulting,** HIPAA National Practice in Armonk, NY.

Good Question: "What is the most important thing you do that must be restored to maintain the flow of business?" asks **Frank Bresz,** senior manager of Security & Technology Solutions at Pittsburgh-based **Ernst & Young.** The highest priority processes are most likely driven by revenue, he says.

Example: You have five different applications, but you can only build a DRP for two of them. If you have one application that generates $1,000 of revenue per day and another that generates $200, you have to center your recovery efforts on the former, Bresz explains.

Still not sure how to focus your plan?

Ask yourself: "How important is this information to our organization? How quickly do we need it? How long can we survive as a business without it?" says **Rick Oppenheimer,** a senior security consultant with **Breakwater Security Associates** in Seattle, WA.

Strategy: "Ask those who own the information what is vital to your business," Oppenheimer suggests. Information owners are responsible for the daily operations of their departments, he says.

Example: The head of radiology is responsible for the radiology department -- including people and data, Openheimer says.

Remember: Evaluate all your information, not just applications, experts remind. "Patient demographics, clinical records and billing information should be given higher priority than assets of a less critical nature, such as appointment schedules," Place advises.

Feel The Heat

Disaster recovery can be expensive, Place warns. Luckily, you have some options. You may choose to use "a hot site, a redundant system in another location or merely recover from recent electronic backup media," she lists.

The most common ways to recover are:

Hot site: A hot site has the exact same computers and applications online and ready to take over if your system fails, Bresz affirms. 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, he says.

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, Bresz informs.

Cold site: A cold site has most of the same equipment, but is neither powered up nor supplied with a completely current image, Bresz explains. You have to manually bring up backup tapes, power up your computers and possibly rely on fewer machines, he says. This is not the option to choose if you need immediate recovery.

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, Bresz notes. This option is more immediate than the cold site, but there is still a delay in recovery.

Power To The People

Your DRP has to "minimize the decision process in a crisis," Oppenheimer says. "People need to have their roles programmed in advance so that they'll know what to do and know what to do first," he says.

Good idea: "Simulate a disaster," Bresz suggests. This will test your computers' ability to start up in alternate locations and allow your employees the chance to run through procedures, he counsels.

Be sure to include in your DRP how your office will conduct business during a downed period, Place reminds. Make this the focus of employee training so that you can continue operating during down time, she advises.

"The worst disasters never happen," Oppenheimer says. Your disasters will mostly likely be the result of a pipe burst or an application failure. However, if there is a full disaster, your employees are your top priority. "You must ask if the people are well protected," he says.