Oregon Healthcare News

orhcnews.com | Articles, Interviews and Statistics for the Healthcare Executive

Disaster Recovery: What's Your Plan?

By Kevin Villanueva
Senior Manager
Moss Adams LLP

A devastating earthquake. A raging storm. An unrelenting flood. Each of these natural disasters could easily disable or dismantle the best-built health care facility in the world, as recent events in Japan have made all too clear.

Obviously, whenever destruction of this magnitude takes place, the top priority is patient safety and protection. But even if patients are evacuated and removed from harm's way, their medical records could still be damaged or lost in the wake of a calamity.

Furthermore, if your medical records aren't adequately backed up or a solid disaster recovery plan isn't in place, you could find yourself in violation of the HIPAA Security Rule, which requires all covered entities, health care clearinghouses, and business associates to have a plan that ensures the availability of electronic protected health information (ePHI) in the aftermath of a disastrous event.

But many health care organizations don't know how to develop such a plan. What's more, disaster recovery is often seen as synonymous with business continuity. It's not.

Disaster recovery focuses on the technology infrastructure critical to an organization after a disaster. Business continuity, on the other hand, is more concerned with the critical business functions that will be available to stakeholders during a recovery effort. Keeping this distinction in mind will help narrow the scope of your disaster recovery plan.

The first step in developing a plan is identifying your organization's critical data. This can be ePHI, employee and patient records, or financial information. Those tasked with developing the disaster recovery plan need to work with process owners to identify what data is being processed, how it's acquired, who needs access to the data, and where it's stored.

Once the critical data has been identified, a business impact analysis (BIA) needs to be conducted to identify which business units, operations, and processes are essential to the survival of the organization. The BIA often involves business unit managers and staff who can provide realistic expectations of service delivery during a recovery effort.

This information helps in formulating recovery time objectives (RTOs)—goals for the time it should take to bring critical systems back online following an incident. An RTO is usually the maximum tolerable downtime for a critical system that must be met before significant impact to human safety, financial health, regulatory compliance, or public reputation is felt.

The BIA also helps determine the recovery point objective (RPO), the acceptable amount of data loss measured in time. In some industries, it may be acceptable to lose a day's worth of data as an RPO. However, in health care the RPO demanded is often as close to real

time as possible. Knowing your RTOs and RPOs for critical systems will help determine the priority ranking for recovery.

Your data backup strategy is likely the most critical piece of your disaster recovery planning process. Most organizations actively back up critical data, but is your strategy sound and complete? What data files are getting backed up? How often are they getting backed up? Where is the backed-up data stored? These are all questions that need to be asked. You should also perform restoration testing of data from backup media on a regular basis to ensure the data recovery process can be completed in a timely manner.

Before you develop a disaster recovery plan, you must identify the resources you'll need during a recovery effort. For example, an alternate location may be necessary if the primary location is unavailable. Server hardware, devices, and other equipment may be difficult to procure in a timely manner should the primary hardware become irreparably damaged. As a result, you may need to implement an emergency procurement process.

In addition, you might need to obtain backup tapes from a commercial storage facility. Backup software and spare hardware, such as tape drives, may be necessary for successful and timely data restoration. You'll need to determine connectivity needs during a recovery effort, and there may be key IT staff (primary contacts for a particular system) who need to be available to configure the temporary server after it's brought online. Once these resources are identified, development of the plan can begin.

Clearly, there's a lot to consider. But even though it may seem like a daunting task, being methodical in developing your disaster recovery plan can help you implement a practical and achievable course of contingent action.

Kevin Villanueva leads the firm's information security and infrastructure practice. He has over 14 years of experience in information technology, with particular focus on disaster recovery planning and IT security. He can be reached at (206) 302-6542 or kevin.villanueva@mossadams.com.

Reprinted with permission from the Oregon Healthcare News. To learn more about the Oregon Healthcare News visit orhcnews.com.