HIPAA Disaster Backup Plan: Are You Prepared?

The recent hurricane got us thinking: what’s *your* disaster backup plan? The HIPAA Security Rule requires all Covered Entities (CEs) to draft a disaster recovery plan, by service definition, that includes what measures your practice will take in case of a natural disaster. Are you prepared?

**Contingency Plan**
Federal law requires that CEs must implement protocols to safeguard - and ensure access - to electronic Protected Health Information (ePHI), including a contingency plan to secure continued availability to ePHI during emergencies or disasters.

However, ePHI isn’t accessible without use of a data processing application, such as Electronic Health Records (EHR) or Practice Management System software - which means that the data can only be recovered with those systems, and their utilization needs to be included in the contingency plan.

**Data Backup Plan, Methods**

**Most data recovery centers recapture ePHI by using either data backups or replication:**

- **Data backups** are to removable media such as CDs, flash drives, etc - or to storage systems such as dedicated backup appliances. Data backups are typically: taken regularly, duplicated, and stored both on and off site to maintain multiple versions of the data.

- **Data replication** copies ePHI to another site, which might be a host, network, or storage system facility. Data replication can be booked to happen on a certain schedule; or copies of the data can be made while the information is being modified (synchronous mirroring).

**Data Backup Plan, Site Types**

To be successful, disaster recovery depends on utilization of an alternate or secondary site. There are typically three options available:

- **Cold Site**: provides only power, cooling, and networking. Servers, switches and storage hardware must be supplied. If choosing a cold site, you will need to ship any necessary hardware to the site, as well as all backup data.

- **Warm Site**: adds enough servers, switches and storage hardware to support ePHI operations during a disaster. If choosing a warm site, backup data must be transported to the site.
> **Hot Site**: offers warm site hardware, plus continuous mirroring of ePHI to make disaster recovery faster and more efficient.

For all three site types, servers, networking and software systems will need to be reconfigured onsite to support emergency operations.

**Disaster Recovery Plan (DRP)**

In addition to the Data Backup Plan (securing ePHI backup and an alternate site arrangement), you must also implement a disaster recovery and emergency mode operations plan. The data backup plan creates systems to allow for the recovery of all ePHI. The disaster recovery plan establishes protocols needed to make sure ePHI can be restored in case of loss. The emergency mode operation plan provides a method for operations to continue to safeguard ePHI during an emergency.

While HIPAA disaster recovery requirements break these into two separate policies, many HIPAA compliance consultants cover both mandates with an integrated Disaster Recovery Plan (DRP). Any DRP should encompass the following:

> **Disaster Declaration** ePHI might be comprised by a significant disaster, such as a hurricane, that requires a practice to work in an alternate location (which can be costly) - or a smaller threat, such as a power fluctuation. Whether the data threat is large or small, the disaster declaration identifies the decision process to address and the key players involved.

> **Disaster List** Classifying high-probability and high-impact events (such as natural disasters) can support justifying investment in expensive backup systems, alternative site(s) and recovery procedures.

> **Data Backup** The DRP should detail the data backup procedures, including the type of backup system; location(s) of any offsite repositories; and the frequency at which the data is copied. In the case of removable device backups, how the data is shipped to the alternate site (including activation protocols, vendor contact details and instructions on how practice staff would access and/or travel to the alternate site) should be documented.

It should also be demonstrated that any offsite repositories are far enough away from the practice location (and any other backup locations) to ensure safety in the event of a natural disaster impacting the primary site.
> **ePHI Recovery** Ultimately, the whole point of a DRP is to restore ePHI in a safe environment so that a practice can continue treating clients. DRPs should identify all ePHI systems - including your EHR - and all data requirements. It should also identify the procedures to restore these systems, including a recovery priority list and the contact information for staff members familiar with these emergency operations.

**But Wait! There's More...**

In addition to all of these requirements, don’t forget that changes to ePHI applications (such as EMR) can change the DRP! Regular modification and testing are necessary to ensure that you're current and up to date.

"Periodic plan tests and resultant corrections are vital to the continuing success of any disaster recovery. With natural disasters and security breaches occurring more frequently, the need for a practicable DRP is more essential than ever."

**PIMSY **Is Your Backup Plan**

Head spinning yet? It's a lot to take in, much less stay on top of, especially for mental + behavioral health care practices simply trying to keep up with treating clients. **Here's the great news:** **PIMSY is your backup plan!**

Yep, you heard correctly. With PIMSY, your practice data is stored in the **Microsoft Azure Cloud**, automatically backed up and encrypted at multiple locations. Azure (a "hot site") adheres to HIPAA protocols, adding another layer of compliance and security.

While every practice is individually responsible for HIPAA compliance - and no EHR is actually HIPAA compliant - using **PIMSY for your mental health software greatly increases HIPAA compliance and data security.** While you still have to establish a DRP, the mechanics of it are taken care of simply by using PIMSY, and most of the steps listed above are fulfilled - all included in PIMSY’s affordable price.

**CLICK HERE TO SEE HOW PIMSY HELPS YOU STAY HIPAA COMPLIANT**

**Learn More**

For more information about how PIMSY can support your mental / behavioral health agency, contact us: hello@pimsyemr.com - 877.334.8512, ext 1. We're happy to show you how **PIMSY saves time, pays for itself, and helps you meet compliance regulations.**