

## HIPAA Compliance Checklist, Part 2: Data Disaster Recovery Plan

Saturday, 28 June 2008

Earlier, we talked about the HIPAA requirement for a data backup plan, and features to look for when choosing a data backup vendor. If you missed that post, you can find it here: [Part 1: Backup HIPAA Data Offsite](#).

But there's a lot more you need to be thinking about in terms of HIPAA compliance, including a data disaster recovery plan, because HIPAA requires that you "establish (and implement as needed) procedures to restore any loss of data."

[Read More...](#)

Earlier, we talked about the HIPAA requirement for a data backup plan, and features to look for when choosing a data backup vendor. If you missed that post, you can find it here: [Part 1: Backup HIPAA Data Offsite](#).

But there's a lot more you need to be thinking about in terms of HIPAA compliance, including a data disaster recovery plan, because HIPAA requires that you "establish (and implement as needed) procedures to restore any loss of data."

You're already in the process of choosing a provider for your data backup plan. That provider should also support your disaster recovery planning efforts by providing effective and timely data recovery solutions. We suggest that you have the following on your backup vendor shopping list:

- Support should include both localized disasters (typically equipment failure) and site or regional disasters, which could be things like fire, flood, hurricanes, or natural events.

- We've mentioned this before, but it bears repeating -Your data should be stored offsite in two geographically separate data centers. In the event that your business location is destroyed, that data should be easily retrievable as soon as you have identified a temporary location and have acquired equipment. And for maximum safety, those data centers should be located thousands of miles apart. This drastically decreases the likelihood that a regional disaster will affect both data centers at the same time.

- Some data backup companies will provide an onsite virtual server in the form of a NAS device, at no additional cost to you. It can function as a failover server if your disaster is equipment related (and it usually will be). That way, you'll have almost no downtime while waiting for replacement equipment. A NAS device also provides you with an additional, onsite copy of your data, quickly retrievable if you need it.

If you're searching for a data backup and disaster recovery vendor that can deliver all the features you need, go to the comparison chart at [Compare Online Backup](#) to see how Granite Mountain stacks up against the competition. Then complete our [Fast Quote Form](#) or call us at [to find out how we can support your HIPAA compliance efforts](#).

Next in our HIPAA Compliance Checklist series:

[Part 3: Emergency Mode Operation Plan](#)

[Part 4: Physical Safeguards for HIPAA Compliance](#)

[Part 5: Technical Safeguards](#)