

Cloud Backup for HIPAA



HIPAA Regulations

HIPAA (Health Insurance Portability and Accountability Act) establishes national standards to protect people's electronic Protected Health Information (ePHI) and requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of ePHI. The new Omnibus Rule of March 2013 broadens the definition of companies that need to comply with HIPAA regulations to include cloud service providers.

Who Must Comply

Those who must comply with HIPAA fall into two categories: Covered Entities (CE) and Business Associates (BA). A Covered Entity includes all health plans, health care clearinghouses, or health care providers who transmit health information in electronic form. A Business Associate is someone who performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involve the use or disclosure of individually identifiable health information. Cloud backup providers are considered a Business Associate.

Business Associate Agreement

Under the new regulations, all Business Associates need to sign a Business Associate Agreement with the Covered Entities. If a cloud backup provider will not sign an agreement, then the Covered Entity should immediately start looking for a new provider. The Business Associate Agreement requires the Business Associate to implement safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PHI, and to ensure that any subcontractor engaged by the business associate in this process agrees to implement similar safeguards.



Cloud Backup Specifics

There are several pieces of the new regulations that apply specifically to cloud backup providers and that should be addressed in the Business Associate Agreement. These are:

- Business associates are now separately and directly liable for compliance with and violations of HIPAA.
- Business associates must review and modify security measures on an ongoing basis.
- If a breach of PHI occurs, the Business Associate must notify the Covered Entity in a predetermine amount of time. The covered entity must then notify the affected individuals, unless it has delegated such responsibilities to a business associate.