CARBONITE SUPPORTS HIPAA, GLBA AND FERPA COMPLIANCE

At Carbonite, the security, confidentiality and integrity of customer information are at the core of its backup and recovery solutions. To that end, all Carbonite business plans support HIPAA, GLBA and FERPA compliance.

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is a federal law that requires doctors, hospitals, health plan providers, and other healthcare entities to safeguard patients' medical records and other protected health information (PHI).

Failure to comply with this law can result in large fines and, in some cases, even jail time.

As a "Business Associate", Carbonite implements administrative, physical and technical precautions to ensure the security of protected health information.

Additionally, Carbonite has performed a thorough audit documenting the ways in which it meets each specific safeguard.

GLBA (Gramm-Leach Bliley Act)

GLBA is a federal law that controls the way financial institutions – banks, brokerage companies, insurance companies – share a consumer's non-public personal information. This information includes social security numbers, account information, account balances, payment histories, credit card information, incomes, credit scores, etc.

Like HIPAA, failure to comply with this law can result in large fines and, in some cases, jail time.

Carbonite has undergone a rigorous SOC 2 security assessment. And similar to HIPAA, Carbonite supports GLBA compliance by employing administrative, physical and technical controls to ensure the security and confidentiality of information.

FERPA (Family Educational Rights and Privacy Act)

FERPA is a federal law that protects personally identifiable information and education records, and applies to all schools that receive federal funding – typically universities, academies, colleges, seminaries and institutes of technology.

Educational institutions that fail to comply with FERPA may forfeit their federal funding.

While the handling of education records does not legally require the same level of protection as the healthcare and financial industries, Carbonite protects those records with the same level of security.

What other steps does Carbonite take to protect data and support compliance?

All data backed up with Carbonite is encrypted using 128-bit encryption and sent over a secure SSL (Secure Sockets Layer) connection. The data remains encrypted while in transmission and in storage.

For added protection, Carbonite's business plan customers can choose to set up their own 256-bit private key encryption.

Additionally, all Carbonite data centers are guarded by on-site security officers and are physically secure with protective measures that include restricted access using biometric scanners, electronic key cards and PIN codes.

CARBONITE