USING CARBONITE TO ASSIST WITH HIPAA COMPLIANCE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rules apply to protected patient health information in electronic formats. This information must be protected with appropriate security measures to guard against unauthorized access during transmission over an electronic communication network.

Carbonite Business **provides critical data security protection without compromising patient privacy and can assist customers with HIPAA compliance efforts:**

- **Offsite Backup for Disaster Recovery**: Carbonite online backup is a key component in any disaster recovery plan as protection against hardware failure, theft, virus attack, deletion and natural disaster.
- **Encryption**: All customer data that is sent to Carbonite servers is encrypted before transit with 128-bit Blowfish encryption, then sent to Carbonite data centers using an SSL connection. While at the data centers, all backed up data remains encrypted.
- **Secure Data Centers**: Carbonite's data centers are physically secure with protective measures that restrict personal access using biometric scanners, electronic key cards, and PIN codes. Additionally, the location is guarded by onsite security officers 24 hours a day, 365 days a year.
- **Private Encryption Key Option**: Carbonite provides users with the option of managing their own private encryption key, storing their data in such a way that no one, not even the Carbonite technical support staff, has access to customer data. If you choose this option, your backed up files cannot be decrypted without your unique encryption key. Only someone who can supply the correct encryption key will be able to access your backed up files.*
- **Written Information Security Program**: Carbonite, as required by the HIPAA Security rule, has a Written Information Security Program, including a written contingency plan for responding to system emergencies.
- **Business Associates**: A business associate agreement is not required with Carbonite. These agreements are between covered entities where there is a reasonable probability that protected health information can be accessed. The self-managed encryption key specifically blocks Carbonite from accessing backed up data.

For more information on using Carbonite to remain in compliance with government regulations, including HIPAA, please contact your Carbonite Authorized Reseller.

**Customers who choose to manage the sole copy of their encryption key will not be able to use features such as Anytime Anywhere Access and Courier Recovery.*

CARBONITE™