CARBONITE

HIPAA Compliance

Supporting HIPAA compliance with endpoint data protection & security

Are you doing all you can to safeguard personal health information (PHI) and prevent data breaches? Carbonite Endpoint Backup supports compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA) by tightly controlling invaluable PHI and protecting against endpoint data loss. Its comprehensive set of data protection features gives you secure, auditable, and actionable access to PHI on critical devices – anytime, anywhere. An added benefit: an even more productive, effective, and increasingly mobile workforce.

The Costs of Data Breaches

According to a March 2012 report by the Ponemon Institute, data breaches in the healthcare industry increased by 32 percent between 2010 and 2011; the average cost to the organization due to these data breaches grew by 10 percent.

The study also found that 80 percent of healthcare organizations now use mobile devices to collect, store, and/or transmit some form of PHI. According to 49 percent of survey respondents, lost or stolen computers or mobile devices are the primary cause of healthcare data breaches. Perhaps most alarming, half of the healthcare executives surveyed said their organization does nothing to safeguard the data contained on mobile devices.

So what is the true cost of a data breach? Consider this: Eleven class-action lawsuits valued at US$4.24 billion were recently filed against a single healthcare provider who reported the theft of one desktop computer. The computer contained the unencrypted PHI of approximately 4.2 million members of that healthcare provider, bringing the cost of each compromised medical record to rougly US$1,000[1].

Lock Down Your PHI with Secure Endpoint Protection

Ensuring the security of PHI, wherever it resides, is a critical component of HIPAA compliance. Your data is always encrypted – at rest, in transit, even during deduplication.

Files selected for protection are automatically encrypted using government-approved 256-bit AES encryption[3]; in addition, FIPS 140-2 encryption is integrated with all Windows operating systems. Because all data is encrypted on individual users' hard drives (as well as on the server), PHI is not accessible if a PC falls into the wrong hands.

The HIPAA Framework for Data Breach Prevention

To be HIPAA-compliant, healthcare providers must have in place the following safeguards:

- Administrative safeguards – ensure policies, procedures, and infrastructure protect PHI
- Physical safeguards – ensure the data center(s) cannot be physically compromised
- Technical safeguards – access control, encryption, and audit trail

Microsoft Azure Certifications and Attestations

Flexible hosting options include the Microsoft Azure cloud. Azure data centers meet Tier 4 rating requirements and support HIPAA-compliance[2]:

- ISO/IEC 27001:2005
- SAS 70 Type II (moving to SSAE 16/ISAE 3402)
- HIPAA/HITECH
- PCI data security standard
- FISMA
- Various state, federal, and international privacy laws including 95/46/EC (EU data protection directive) and CA SB1386

HIPAA Compliance

Carbonite Endpoint Backup leverages file- and folder-level encryption to protect PHI stored on a device's hard drive. Laptop data is encrypted during storage, and then decrypted when an application file is opened. The encryption is transparent to employees, so there's no need for additional passwords, and data is protected whether the laptop is on or off.

Do your employees copy their PHI files to USB drives, or burn them onto CDs/DVDs? With Carbonite Endpoint Backup, you can control their read and write access , and use policies to lock down a port completely so that unauthorized users can't remove files.

Finally, you can utilize multiple encryption keys across data sets so that if a single key is compromised, only a subset of PHI data is exposed.

Take Control with Centralized Policy Management

Utilize robust management capabilities to define, deploy, enforce, and report on data backup and protection policies.

- **Configure protection policies** – Determine which files will be protected with backup, at-rest encryption, and proactive data deletion, either by file type or directory structure. You can also define how much storage each user is permitted, how often files will be backed up, and under what schedule such backups should occur.
- **Proactive data deletion and tracing policies** – Decide whether the protected files on a lost or stolen device can be wiped on demand, or set a time-based trigger for a device to be wiped remotely if it has not connected to the server. Deter theft and facilitate device recovery with automatic device tracing.

Contact Us

2 Ave de Lafayette
Boston, MA 02111
800-683-4667
DataProtectionSales@carbonite.com

[1] http://www.inforisktoday.com/more-breach-class-action-lawsuits-filed-a-4275

[2] https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

[3] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf