Carbonite Endpoint and HIPAA

How our endpoint backup solution supports compliance with federal legislation

Carbonite Endpoint supports compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA) by preventing unauthorized access to protected health information (PHI) and preventing accidental or malicious deletion of patient medical records.

Security for PHI

A key component of HIPAA is ensuring the security of electronic medical records (EMR), no matter where they reside. Carbonite Endpoint uses 256-bit AES encryption for data at rest on a protected device, and Transport Layer Security (TLS) for sending data over the wire. Our endpoint protection also performs global deduplication of data, ensuring that patient data never exists in a decrypted state: not while at rest on the hard drive, not while in transit and not during the global client-side deduplication process. The encryption is transparent to employees, so there's no need for additional passwords, and data remains protected whether the laptop is on or off. Carbonite Endpoint also lets you use multiple encryption keys across data sets so that if a single key is compromised, only a subset of PHI is affected.

Hidden threats

Many healthcare organizations are unaware of the risks employees introduce unintentionally when they copy EMR to thumb drives or burn them onto CDs or DVDs. Carbonite Endpoint helps you control read and write access, and create policies to lock down a port completely so that unauthorized users can't remove files.

Central management

Carbonite Endpoint helps system administrators define, deploy and manage data backup and protection policies remotely. Working within the administrative dashboard, the solution lets you determine which files are backed up, how frequently, what time of day and how long they're retained before being purged.

Microsoft Azure certifications and attestations

Azure data centers meet Tier 4 rating requirements and support HIPAA compliance[1]:

- 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

[1] www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

Administrators can also trigger security features if a device containing PHI is lost or stolen. With Carbonite Endpoint, an IT admin can remotely delete all protected data on a lost or stolen laptop by an administrative command, or via a poison pill, which can be scheduled via policy. Carbonite Endpoint also lets you delete files when a hacker tries to crack the administrative passcode. With Carbonite, files remain protected while the user is on unprotected Wi-Fi networks. Anyone trying to access the laptop will not be able to open any files since they won't have the correct encryption keys. Carbonite Endpoint also facilitates device recovery with automatic device tracking.

Contact Us

Phone: 877-542-8637
Email: DataProtectionSales@carbonite.com