HIPAA HANDBOOK

Keeping your backup HIPAA-compliant

The federal Health Insurance Portability and Accountability Act (HIPAA) spells out strict regulations for protecting health information. HIPAA is expansive and can be a challenge to navigate. Use this handbook to learn about some of the most current legal requirements and see how Carbonite protects private patient information and, in turn, your practice.

CARBONITE

Table of contents

INTRODUCTION

U.S. healthcare laws intended to protect patient information (Protected Health Information or PHI) now apply to a broader array of businesses than ever—covering not only healthcare organizations (HCOs), but their Business Associates as well.

Businesses from lawyers and accountants to web hosting firms now find themselves subject to the data privacy and security requirements of HIPAA if they partner with HCOs like yours.

HIPAA requires, among other things, the protection and confidential handling of PHI—protected data which includes names, addresses, birth dates, geographic identifiers, SSN numbers, medical records, and any other information that can be used to identify an individual.

HIPAA violations can result in fines ranging from $100 to $50,000 per occurrence. It pays to comply.

Who is impacted by HIPAA?

Health Plans

Health insurance companies

HMOs

Company health plans

Government programs that pay for health care, such as Medicare, Medicaid, and military and veterans' healthcare programs

Healthcare Providers

Doctors

Clinics

Psychologists

Dentists

Chiropractors

Nursing Homes

Pharmacies

Healthcare Clearinghouses

Entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Business Associates

The Omnibus Rule expanded the definition of a Business Associate to include vendors who "create, receive, maintain, or transmit" PHI on behalf of a Covered Entity like a healthcare organization. Simply put, the intent of the new regulations is to impose the same level of protection on all PHI, regardless of custody.

How does Carbonite comply with HIPAA regulations?

Under the new regulations, Carbonite regards itself as performing the functions of a Business Associate and has enhanced its compliance program to facilitate the ability to maintain a HIPAA-compliant infrastructure.

Wherever necessary, Carbonite will enter into a Business Associate Agreement, providing contractual assurances that we will safeguard PHI. In addition, Carbonite uses vendors that are willing to enter into HIPAA-compliant agreements, assuring that all PHI is protected using the same stringent standards.

Carbonite has designed solutions that comply with the more than 40 privacy and security safeguards required under HIPAA. Outlined on the next few pages are some of the most significant.

Carbonite's Business Associate Agreement is based on the federal standard and provides contractual assurances that we will protect PHI.

ADMINISTRATIVE SAFEGUARDS

Administrative safeguards are administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect PHI and to manage the conduct of the Covered Entity's or Business Associate's workforce in relation to the protection of PHI.

Risk management

What is required?

HIPAA requires Covered Entities and their Business Associates to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to ensure the confidentiality, integrity, and availability of data.

How does Carbonite meet this standard?

√ Real-time monitoring for suspicious activity on its networks.

√ Secure firewall.

√ Formal incident response process to quickly recognize, analyze, and remediate information security threats.

√ Vulnerability management program.

Login monitoring

What is required?

HIPAA compels Covered Entities and their Business Associates to implement procedures for monitoring login attempts and reporting discrepancies.

How does Carbonite meet this standard?

√ Pro and Server administrators can query user logins and activity.

√ User accounts are automatically locked for ten minutes after an incorrect password is entered five times.

Note: Security email correspondence is sent to the customer's email address of record indicating that the user has been temporarily locked out of their account for failure to enter the correct password.

PHYSICAL SAFEGUARDS

Physical safeguards are physical measures, policies, and procedures to protect a Covered Entity's or Business Associate's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Access control and validation procedures

What is required?

HIPAA requires Covered Entities and their Business Associates to implement procedures to control and validate a person's access to facilities based on their role or function—including visitor control and control of access to software programs for testing and revision.

How does Carbonite meet this standard?

- √ Restricted access at Carbonite's facilities, allowing only authorized Carbonite employees, approved visitors, and other authorized third parties to enter.
- √ Several state-of-the-art security controls as a requirement for access.
- √ Restricted access to Carbonite's software programs for testing and revision purposes, allowing only authorized Carbonite personnel to enter.
- √ Visitor access policy stating that data center managers must approve (in advance) and accompany any visitors to the specific internal areas they wish to visit.

Disposal

What is required?

HIPAA requires Covered Entities and their Business Associates to implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

How does Carbonite meet this standard?

√ Data Destruction upon a customer's instruction or subscription termination.

√ Carbonite's Data Destruction process requires all hardware subject to destruction to be authorized for destruction and then logically wiped by authorized individuals.

√ Erasure consists of a full write of the drive with all zeroes (0x00) followed by a full read of the drive to ensure the drive is blank.

√ Erased results are logged by the drive's serial number for future tracking or recordkeeping.

Facility security plan

What is required?

HIPAA requires Covered Entities and their Business Associates to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

How does Carbonite meet this standard?

√ Well-known technologies implementing industry best practices (for example, the use of custom-designed electronic card access control systems, alarm systems, interior and exterior cameras, and 24-hour security).

√ Isolated areas where systems or system components are installed (or stored).

TECHNICAL SAFEGUARDS

Finally, HIPAA mandates technical safeguards for the use of technology and the policies and procedures for its use, to ensure that stored PHI is adequately protected and access is controlled.

Encryption and decryption

What is required?

HIPAA requires Covered Entities and their Business Associates to implement a mechanism to encrypt and decrypt ePHI.

How does Carbonite meet this standard?

√ 128-bit Blowfish encryption while files are still on the customer's computer.

√ Files are transmitted to state-of-the-art data centers using Secure Sockets Layer (SSL) technology.

√ Files are encrypted on our secure servers.

Automatic logoff

What is required?

HIPAA requires Covered Entities and their Business Associates to implement electronic procedures that terminate an electronic session after a pre-determined time of inactivity.

How does Carbonite meet this standard?

√ Automatic logout on Pro and Server solutions after 30 minutes of inactivity.

√ Prohibited access for ten minutes after entering an incorrect password five times.

Note: Security email correspondence is sent to the customer's email address of record, indicating that the user has been temporarily locked out of their account for failure to enter the correct password.

Emergency access procedure

What is required?

HIPAA requires Covered Entities and their Business Associates to establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

How does Carbonite meet this standard?

√ We provide retrievable exact copies of the most recent backup of a customer's data, thereby ensuring data continuity in the event a Covered Entity's on-premise computer experiences an outage.

√ We provide web-based access (via a unique User ID and password) to the customer's backup when the customer's primary computer is experiencing an outage.

√ Synchronization of the data backed up at Carbonite's data centers with a Covered Entity's on-premise computer.

Carbonite will help you ensure that your PHI is always HIPAA-compliant.

Carbonite's Pro and Server solutions are specifically designed to safeguard business data—and both plans meet or exceed every one of the security standards mandated by HIPAA. Visit **www.carbonite.com** to learn more.

You can also call our Sales Team at **877-905-6876** or locate your nearest authorized Carbonite reseller at **www.carbonite.com/partners**.

To obtain Carbonite's Business Associate Agreement, contact the Business Team at **855-227-2249** or **businessteam@carbonite.com**.

BUY NOW

TRY IT FREE