HIPAA: Understanding The Omnibus Rule and Keeping Your Business Compliant

Introduction

U.S. healthcare laws intended to protect patient information (Protected Health Information or PHI) and the myriad of privacy and security implementation safeguards that are required under the new regulatory regime, 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 the Healthcare Information Portability and Accountability Act (HIPAA) if they have HCOs as partners or customers.

It's more important than ever for businesses to ensure they're compliant with HIPAA regulations, as the consequences can be steep. The fines that can result if the privacy and security of PHI are compromised are higher than ever, and the new regulations provide for increased incentive for government enforcement agencies to take action against violators.

This white paper provides a summary overview of what your organization needs to know about the changes resulting from the HIPAA Omnibus Rule. It also outlines how to evaluate secure cloud backup solutions that can facilitate your

© Copyright 2014 Carbonite, Inc. All rights reserved.

CARBONITE™

business' compliance with the complex regulatory requirements so that you can guard against and mitigate the risks posed by governmental and private actions while remaining competitive.

The Evolution of HIPAA

The original HIPAA legislation was passed by the U.S. Congress and signed by President Clinton in 1996. One of HIPAA's central goals was to enable workers to retain their health insurance coverage when changing jobs. To allow for uninterrupted coverage, HCOs needed to be able to exchange patient data and other records. In order for this exchange to occur reliably and efficiently, healthcare records would need to exist in a form that was both consistent and portable, so HIPAA set forth new terminology and Electronic Data Interchange (EDI) code sets for transmitting patient data. Given the inherent risk that transferring confidential healthcare records might result in inadvertent or inappropriate exposure, HIPAA also laid the groundwork for fundamental data security and privacy protections for PHI.

On January 25, 2013, the U.S. Department of Health and Human Services (HHS) issued a final rule (Omnibus Rule) modifying the HIPAA Privacy, Security, Breach Notification and Enforcement Rules. These modifications integrate statutory amendments under the Health Information Technology for Economic and Clinical Health (HITECH) Act. In general, the new rules expand the obligations of physicians and other healthcare providers to protect PHI. However, the most dramatic business change as a result of the Omnibus Rule is the impact on a number of individuals and companies who, as "Business Associates," provide services that bring them in contact with Protected Health Information.

HIPAA requires, among other things, the protection and confidential handling of PHI – defined as information relating to the physical or mental health condition of an individual, the provision of healthcare services, or the payment for the provision of healthcare services to an individual. This definition includes data such as names, addresses, birth dates, geographic identifiers, SSN numbers, medical records, and any other information that identifies, or can be used to identify, an individual.

Covered Entities

HIPAA applies to "Covered Entities" - health plans, healthcare clearing houses, and healthcare providers - that transmit health information electronically. The following are examples of each of type of entity:

Healthcare Provider:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

Health Plan:

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' healthcare programs.

© Copyright 2014 Carbonite, Inc. All rights reserved.

Healthcare Clearinghouse: 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.

Bunsiness Associates

Although HIPAA initially only directly regulated Covered Entities and, indirectly, their vendors who had access to PHI, 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. Simply put, the intent of the new regulations is to impose the same level of protection on all PHI, regardless of in whose custody it resides. In the past, HHS only had direct recourse to Covered Entities; today, each entity that comes in contact with PHI has direct accountability, regardless of how far down the chain of custody that provider may be.

Even prior to the Omnibus Rule, Carbonite managed all PHI mindful of its obligations to its Covered Entity customers, and in compliance with the applicable HIPAA requirements. Under the new regulations, Carbonite regards itself as performing the functions of a Business Associate and has enhanced its compliance program to facilitate our Covered Entity customers' ability to maintain a HIPAA-compliant infrastructure.

Carbonite's Pro and Server Solutions

The security, confidentiality and integrity of customer information are core to the Carbonite solution. As a result, Carbonite was at the forefront of compliance with the regulatory change.

Carbonite's Pro and Server solutions are designed to meet the privacy and security safeguards, and the notification requirements, of HIPAA. At Carbonite, we understand that finding the right cloud backup solution is particularly important in the healthcare industry because it is intensely regulated, with numerous compliance requirements at the federal, state and local level. With the potential for reputational damage and steep financial and other penalties for non-compliance, it is critical to choose the right backup solution and trusted partner to facilitate HIPAA compliance.

Business Associate Agreement

For Covered Entities that use Carbonite to back up PHI, Carbonite will enter into a Business Associate Agreement in order to provide contractual assurances that we will appropriately safeguard your PHI. In addition, as required under the Omnibus Rule, Carbonite only uses subcontractors that are willing to enter into HIPAA-compliant agreements in order to assure that all PHI, regardless of the custodian, is protected using the same stringent standards.

To obtain Carbonite's Business Associate Agreement, contact the Business Team today:

1-855-CARB-BIZ (1-855-227-2249)
businessteam@carbonite.com

Carbonite's Subcontractors/Partners

Each of Carbonite's subcontractors or partners has entered into a contract with us that assures that each has implemented all of the required administrative, physical and technical safeguards required under the HIPAA Privacy and Security Rules. Further, each has made available the third party audits that attest to their compliance. As a result, Carbonite is able to leverage the resources of these partners to enhance its ability to facilitate HIPAA compliance for our Covered Entity customers.

© Copyright 2014 Carbonite, Inc. All rights reserved.

HIPAA Safeguards

The HIPAA Privacy Rule establishes the safeguards required to protect the privacy of PHI, while the HIPAA Security Rule sets national standards for the security of electronic protected health information (ePHI). HHS enforces these Rules and the detailed administrative, physical and technical safeguards that Business Associates must implement to ensure compliance.

Carbonite conducted a thorough audit and risk assessment in order to document the ways in which it meets each safeguard. Below are a few examples of how Carbonite complies with the more than 40 privacy and security safeguards required under HIPAA.

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.

Here are some examples of Administrative Safeguards:

Risk Management

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.

Carbonite Meets This Standard By:

- Performing periodic network penetration testing.
- Having implemented a proprietary intrusion detection solution.
- Monitoring [on a real-time basis] for suspicious activity on its networks.
- Maintaining a secure firewall.
- Following a formal incident response process to quickly recognize, analyze, and remediate information security threats.
- Running a vulnerability management program.

Log-in Monitoring

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

Carbonite Meets This Standard By:

- Allowing Pro and Server administrators to query user logins and activity.
- Automatically locking user accounts 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.

© Copyright 2014 Carbonite, Inc. All rights reserved.

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.

Here are some examples of Physical Safeguards:

Access Control and Validation Procedures

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.

Carbonite Meets This Standard By:

- Restricting access to Carbonite's facilities to authorized Carbonite employees, approved visitors and other third parties.
- Having implemented several state-of-the-art security controls, including biometric identification, as a requirement for access.
- Restricting access to Carbonite's software programs for testing and revision purposes to authorized Carbonite personnel only.
- Maintaining a visitor access policy stating that data center managers must approve, in advance, and accompany any visitors for the specific internal areas they wish to visit.

Disposal

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.

Carbonite Meets This Standard By:

- Enacting the Data Destruction process described below 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. The erasure consists of a full write of the drive with all zeroes (0x00) followed by a full read of the drive to ensure that the drive is blank. These erase results are logged by the drive's serial number for future tracking or recordkeeping.

Facility Security Plan

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.

Carbonite Meets This Standard By:

- Implementing well-known technologies and following industry best practices, for example, custom designed electronic card access control systems, alarm systems, interior and exterior cameras, 24-hour security and biometric controls.
- Isolating areas where systems, or system components, are installed or stored from general office and public areas.

© Copyright 2014 Carbonite, Inc. All rights reserved.

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.

Here are some examples of technical Safeguards:

Encryption and Decryption

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

Carbonite Meets This Standard By:

- Encrypting files with 128-bit Blowfish encryption while still on the customer's computer.
- Transmitting files to state-of-the-art data centers using Secure Socket Layer (SSL) technology.
- Keeping files encrypted on our secure servers.

Automatic Logoff

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

Carbonite Meets This Standard By:

- Automatically logging out Pro and Server customers after 30 minutes of inactivity.
- Prohibiting 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

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

Carbonite Meets This Standard By:

- Providing retrievable exact copies of the most recent back up of a customer's data, thereby ensuring data continuity in the event a Covered Entity's on-premise computer experiences an outage.
- Providing 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.
- Synchronizing the data backed up at Carbonite's data centers with Covered Entity's on-premise computer.

© Copyright 2014 Carbonite, Inc. All rights reserved.

Partner

Carbonite is a trusted partner for your small business clients who need a HIPAA-compliant cloud backup solution. Carbonite protects computers, encrypts data, stores data in highly-secure data centers, and provides easy access (to authorized personnel) and restoration of data in the event data is lost.

1) **Carbonite's Pro and Server solutions:**
   - Facilitate the confidentiality, integrity, and availability of electronic protected health information.
   - Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
   - Protect against any reasonably anticipated uses or disclosures of PHI.
2) **Carbonite will provide and sign a businees assocaite agreement**

To obtain Carbonite's Business Associate Agreement contact the Business Team today:

1-855-CARB-BIZ (1-855-227-2249)

businessteam@carbonite.com

Business Plans & Pricing

All Carbonite business plans support HIPAA compliance

Workstation Backup

For businesses that need to protect unlimited computers

PRO BASIC

250 GB CLOUD STORAGE
to share between an unlimited # of:
- Computers & laptops
- NAS devices & external hard drives

PRO PRIME

500 GB CLOUD STORAGE
to share between an unlimited # of:
- Computers & laptops
- NAS devices & external hard drives
- Windows file servers

Server Backup

For businesses that need hybrid, local, live applications

SERVER BASIC

250 GB CLOUD STORAGE
to share between an unlimited # of:
- Servers (physical & virtual), databases, live applications, Hyper-V environments
- NAS devices & external hard drives

SERVER PRIME

500 GB CLOUD STORAGE
to share between an unlimited # of:
- Servers (physical & virtual), databases, live applications, Hyper-V environments
- NAS devices & external hard drives

Complete Business Backup

Combines our automatic workstation backup with robust server backup

SERVER PRO BUNDLE

500 GB CLOUD STORAGE
to share between an unlimited # of:
- Servers (physical & virtual), databases, live applications, Hyper-V environments
- NAS devices & external hard drives
- Windows file servers
- Computers & laptops

+ ADD STORAGE

100 GB

STORAGE PACK

© Copyright 2014 Carbonite, Inc. All rights reserved.

CARBONITE™