Barracuda

Solutions Brief

HIPAA Compliance With Barracuda Backup

Overview

The healthcare industry relies on critical data to provide effective patient care. This sensitive data must be easily accessible by healthcare providers, while kept safe from inappropriate parties and accidental loss. It also needs to be able to be quickly recovered in case of server failure or even a disaster.

Barracuda Backup secures data while ensuring its availability to appropriate parties. In addition, Barracuda Backup aids organizations in meeting compliance with the Health Insurance Portability and Accountability Act (HIPAA). This is a must-have for any healthcare provider, health plan, and clearing house that electronically maintains or transmits health information pertaining to individuals in the United States.

What is the Health Insurance Portability and Accountability Act (HIPAA)?

HIPAA is the primary U.S. law governing the protection of patients' health information. Signed into law in 1996, HIPAA has since been supplemented and clarified by the Health Information Technology for Economic and Clinical Health (HITECH) Act and various Health and Human Services (HHS) regulations, including the 2013 Omnibus Rule. HIPAA's Security Rule requires organizations to safeguard protected health information (PHI). The Privacy Rule regulates whether and how organizations may use or disclose PHI. Subpart D mandates that organizations notify patients whose PHI has been subject to a data breach or security incident or has been impermissibly used or disclosed.

Originally, HIPAA's requirements were targeted at Covered Entities—health plans, healthcare clearinghouses, and healthcare providers that transmit any health information electronically. However, many of the law's provisions, including the Security Rule, apply equally to Business Associates: organizations that create, receive, maintain, or transmit PHI on behalf of Covered Entities. As such, providers of IT services must secure any PHI held in the cloud on behalf of Covered Entities and ensure the confidentiality of PHI in the cloud.

Additionally, each Covered Entity is required to enter into a Business Associate Agreement (BAA) with its Business Associates. A BAA is a legal agreement in which a Business Associate makes various commitments regarding the security and privacy of PHI held on the Covered Entity's behalf.

How can Barracuda help organizations with HIPAA-related requirements?

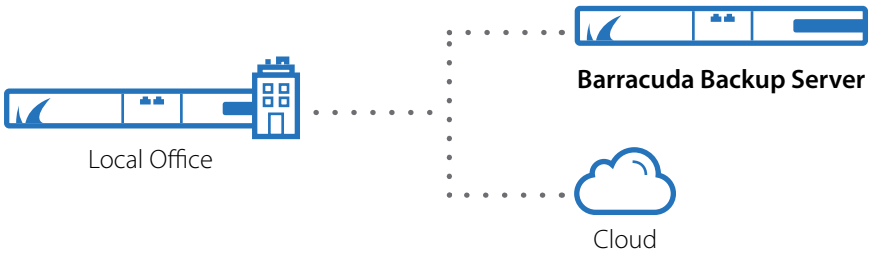
Listed are some basic requirements that may need to be addressed

Requirement: Healthcare providers need to have a data backup and disaster recovery plan.

Section 164.308 states that providers need to "establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information" and "establish (and implement as needed) procedures to restore any loss of data." Healthcare providers should provide ways to protect their servers both locally for quick recovery, but also have a copy of the protected data stored offsite for redundancy in case of disaster.

Solution

Barracuda Backup protects a wide range of physical and virtual environments. With Barracuda, healthcare providers are able to deploy a local appliance for fast local backups and restores. Source-based and global deduplication on the local appliance reduce storage footprints to meet retention needs. With the Barracuda solution, there is no need to worry about per-server or application licenses. Barracuda Backup is a comprehensive solution that provides a complete site license. Organizations can protect all of their servers and applications at one affordable price. Organizations can choose to replicate to another Barracuda appliance or to the Barracuda Cloud. This replication technology gives organizations the capability to simultaneously backup and replicate protected data, limiting time to recovery.



Requirement: Healthcare providers need to keep patient information secure.

There are many security requirements in HIPAA. Subpart C, the Security Rule, requires that organizations protect against any reasonably anticipated threats or hazards to the security of PHI and lists safeguards that organizations must implement. For example, section 164.312(a)(1) mandates that Covered Entities implement access controls over their PHI, and 164.308(a)(1) requires the implementation of audit logs to allow organizations to review records of information system activity.

Solution:

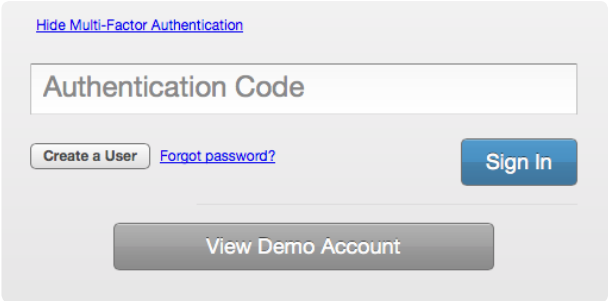
Barracuda Backup helps organizations meet these requirements with encryption, user access control, and complete audit logs.

- Encryption: When data is replicated to the Barracuda Cloud or another appliance, it is encrypted in-flight and at rest with a 256-bit AES algorithm. This offers additional security to data transferred to and stored at remote sites.
- Secure Access: Secure user access is critical for Barracuda and its customers. Barracuda Backup offers a secure and intuitive interface for accessing user data for recovery.

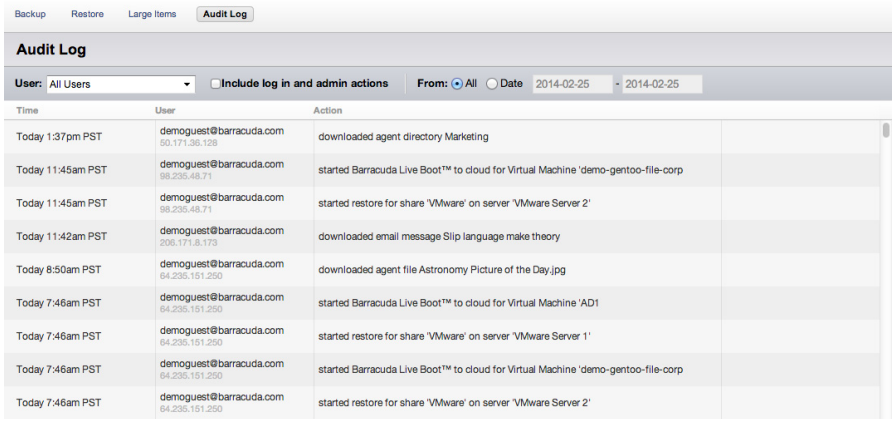
Security safeguards include:

- The ability of IT administrators to enable IP restrictions for authentication to the Barracuda web interface, limiting the locations of access to add an additional level of verification.
- Multi-factor authentication for users managing the Barracuda appliance from the Barracuda Control Center.

Administrators accessing Barracuda Cloud Control will need to enter their credentials into the website and enter a generated key that can be accessed on an Android, Apple, BlackBerry, or Windows device.



Additionally, after authentication, administrators are able to access the audit logs that keep track of every change, authentication, and restore that has been done on the appliance. These logs are stored securely in the cloud and retained for the life of the appliance. Organizations are able to search the logs based on authentication, date, and user.



Business Associate Agreements (BAA)

Organizations storing PHI in offsite storage locations must follow sections 164.502 and 164.504 of HIPAA, requiring Covered Entities to sign Business Associate Agreements with their Business Associates. Customers subject to HIPAA requirements may store PHI through a number of cloud services.

Customers can store their customers' PHI in the Barracuda cloud securely. Barracuda would be considered a Business Associate of the organization. If a customer is not using the Barracuda Cloud for offsite storage, then Barracuda is not storing PHI on behalf of the customer and is not a HIPAA Business Associate of that customer. To the extent that Barracuda is a Business Associate under HIPAA regulations, Barracuda complies with any applicable requirements in HIPAA and the HITECH Act. If a customer stores PHI in the Barracuda cloud, the customer is required under HIPAA to sign a Business Associate Agreement with Barracuda. Customers who store PHI in the Barracuda cloud must contact Barracuda and request a copy of Barracuda's standard Business Associate Agreement.

If a customer is a Business Associate of a different organization and the customer stores PHI in the Barracuda cloud, then under HIPAA, Barracuda is a subcontractor of the customer. In these cases, when requesting a copy of Barracuda's standard Business Associate Agreement, the customer must specifically request the version that reflects Barracuda's status as a subcontractor of the customer.

Barracuda's standard Business Associate Agreement has been updated in response to the 2013 Final Rule.

Conclusion

Healthcare organizations must comply with ever-changing rules and regulations and data protection will always be part of them. Storing, securing, and recovering data can be a complex process, but Barracuda makes it simple. Barracuda offers an easy to use end-to-end solution that includes integrated storage, unlimited agents, and offsite replication—all at an affordable cost. Security and compliance are important components of Barracuda solutions. Barracuda Backup helps healthcare organizations meet regulatory requirements by soundly addressing HIPAA requirements for data protection and recovery.