Ensuring HIPAA and HITECH Compliance With Wasabi

Table of Contents

Executive Overview

Wasabi is an affordable and fast cloud storage service. Healthcare organizations can use Wasabi hot cloud storage for a variety of purposes including primary storage for application data and content, secondary storage for backup or disaster recovery, and archival storage for long-term data and record retention. The U.S. Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) impose strict requirements on how electronic health information is stored and protected.

Healthcare providers, insurers and clearinghouses can use Wasabi to store and maintain electronic health records (EHRs) in accordance with the HIPAA and HITECH regulations. Wasabi uses security best practices and technologies to ensure the physical security of its facilities and to maintain the privacy and integrity of electronic data and digital records. In addition the Wasabi service passed a thorough HIPAA/HITECH audit performed by Schellman & Company, a leading provider of attestation and compliance services.

This white paper provides an overview of the HIPAA and HITECH statutes and explains how Wasabi helps healthcare IT organizations comply with government regulations for safeguarding Protected Health Information (PHI).

Introduction – HIPAA and HITECH Overview

HIPAA was enacted in 1996 to improve the efficiency and effectiveness of the U.S. healthcare system. The HIPAA mandate includes a Privacy Rule to protect patient confidentiality and a Security Rule to safeguard IT systems and infrastructure. HIPAA laws apply to all healthcare providers, plans and clearinghouses that conduct certain healthcare transactions electronically.

The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of individually identifiable health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. It also grants patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The HIPAA Security Rule establishes national standards to protect electronic personal health information. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI.

The HITECH Act of 2009 expanded the original HIPAA law and introduced financial incentives to stimulate the adoption of health information technology. The HITECH statute extends HIPAA privacy and security requirements, strengthens the enforcement of HIPAA rules, and requires healthcare providers to notify patients if their protected information is breached.

HIPAA Data Privacy and Security Implications

HIPAA imposes specific technical and administrative requirements for healthcare IT planners, InfoSec organizations and compliance officers. Healthcare IT organizations must put strong security systems and practices in place to protect access to confidential data and to safeguard the integrity of electronic health records throughout their lifecycle. IT organizations must ensure EHRs are not deleted, corrupted, tampered with, or stolen. HIPAA privacy and security rules apply to data maintained on-premises, in a hosted facility (colocation center), or in the cloud.

The U.S. Federal Government and the U.S. Department of Health and Human Services (HHS) do not require or recognize HIPAA audits or other certifications. The onus is on each healthcare organization to ensure its IT systems and practices comply with HIPAA data privacy and security requirements.

Wasabi Hot Cloud Storage Overview

Wasabi hot cloud storage is affordable, fast and reliable cloud object storage for any purpose. Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi hot cloud storage is easy to understand and implement, and cost-effective to scale. One product, with predictable and straightforward pricing, supports virtually every cloud storage application.

Healthcare organizations can use Wasabi for:

- Low-cost primary storage for on-premises or cloud-based applications
- Economical secondary storage for backup, disaster recovery in the cloud, or data migration initiatives
- Affordable and reliable archival storage for long-term data retention

Wasabi hot cloud storage is ideal for a wide variety of healthcare applications including:

- Electronic records (EHR, EMR, EPR, CPOE)
- Medical imaging (PACS, RIS, VNA)
- Healthcare IoT applications
- Drug, device and treatment R&D

Ensuring HIPAA Compliance With Wasabi

Healthcare organizations can use Wasabi to store and maintain electronic healthcare records in accordance with HIPAA/HITECH regulations. The Wasabi cloud storage service is engineered to ensure the privacy and integrity of PHI. The service is built and managed according to security best practices and standards, with HIPAA patient privacy and data security requirements in mind.

Wasabi's security architecture, systems and practices have been evaluated for HIPAA/HITECH compliance by Schellman & Company, an independent CPA. After a thorough audit, the firm issued an attestation report confirming Wasabi complies with HIPAA security and privacy rules for protected health information. Wasabi enters into HIPAA business associate agreements (BAAs) with HIPAA-covered entities (hospitals, insurers, etc.)

Wasabi takes a "defense-in-depth" approach, employing multiple layers of security for ultimate protection in accordance with HIPAA security guidelines. Wasabi ensures the physical security of its data centers; institutes strong authentication and authorization controls for all its cloud compute, storage and networking infrastructure; and encrypts data at rest and in transit to safeguard confidential patient information.

Physical Security

The Wasabi service is hosted in premier Tier IV data center facilities that are highly secure, fully redundant, and certified for SOC 2 and ISO 27001 compliance. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility—both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

Wasabi employs advanced network security elements, including firewalls and other boundary protection devices to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to Wasabi infrastructure and services.

Data Privacy and Security

Wasabi supports a comprehensive set of data privacy and security capabilities to prevent unauthorized disclosure of electronic health records. Strong user authentication features tightly control access to stored data. Access control lists (ACLs) and administratively defined policies selectively grant permissions to users or groups of users.

Wasabi encrypts data at rest and data in transit to prevent record leakage. All data stored on Wasabi is encrypted by default to protect data at rest. And all communications with Wasabi are transmitted using HTTPS to protect data in transit.

Data Durability and Protection

Wasabi hot cloud storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s object durability, protecting data against hardware failures and media errors. In addition, Wasabi supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

An immutable object cannot be deleted or modified by anyone—including Wasabi. Wasabi data immutability protects the integrity of data, mitigating the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware.

Data Ownership and Disclosure

The Wasabi Storage Platform Terms of Use Agreement grants the healthcare organization exclusive ownership and control of stored data. Under the terms of the agreement the subscriber (the healthcare organization) maintains ownership of all subscriber data. All data stored on Wasabi remains the exclusive and confidential property of the subscriber.

Customer Responsibilities

Wasabi customers typically interface with the Wasabi service using third-party file management applications and backup tools. To ensure HIPAA compliance, IT personnel must ensure the storage management tools and applications they use are configured to take advantage of Wasabi security features. For example, HTTPS must be enabled to encrypt data in transit. In addition, customers must encrypt all content and data prior to uploading it to Wasabi.

IT organizations must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure. The Wasabi storage service is typically employed as part of a larger public or hybrid cloud IT implementation that includes multiple compute, storage and networking components.

Additional Considerations

Healthcare organizations may also need to comply with individual state laws governing data privacy and security. State health information privacy and consent laws and policies vary widely across the country, and in some cases are more stringent than the HIPAA/HITECH statutes.

Conclusion

HIPAA imposes stringent data privacy and security requirements for healthcare organizations. HHS does not provide formal HIPAA certification mechanisms, so the onus is on every organization to ensure its IT systems and practices are compliant.

Wasabi's cloud storage service ensures the privacy and integrity of electronic health records and protected health information, helping IT organizations comply with the HIPAA and HITECH statutes. Wasabi ensures the physical security of its data centers, employs strong authentication and authorization controls to safeguard infrastructure and services, and encrypts data at rest and in transit to prevent unauthorized record disclosure.

Wasabi is typically used in conjunction with other compute, storage and networking platforms and services. IT organizations must implement strong security systems and practices across all on-premises and cloud-based infrastructure to fully protect electronic health records.

Additional Information

For additional information about HIPAA and Wasabi consult the following resources:

- U.S. Department of Health and Human Services website
- U.S. HealthIT website
- Wasabi HIPAA solution page

About Wasabi

Wasabi is the hot cloud storage company delivering low-cost, fast, and reliable cloud storage. Wasabi is 80% cheaper and 6x faster than Amazon S3, with 100% data immutability protection and no data egress fees.

Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi is on a mission to commoditize the storage industry. Wasabi is a privately held company based in Boston, MA.

Tel 1-844-WASABI-1
Email info@wasabi.com

hot cloud storage

www.wasabi.com