nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
Office: +1.617.520.4120

HOW NCRYPTED CLOUD ENSURES HIPAA COMPLIANCE

Background

This white paper outlines how nCrypted Cloud is the industry leading solution to ensure HIPAA/HITECH regulatory compliance when using cloud-based file storage and sharing facilities such as Dropbox.

Specifically, this white paper details:

- How nCrypted Cloud ensures HIPAA/HITECH compliance.
- Why nCrypted Cloud is superior to all of the other competitive products.

Executive Summary

nCrypted Cloud enables covered entities and business associates to confidently maintain HIPAA/HITECH regulatory compliance when using cloud-based file storage and sharing technologies in the delivery of health care services.

nCrypted Cloud provides all the privacy and security safeguards to meet, and in many instances exceed, HIPAA/HITECH requirements.

nCrypted Cloud offers the most comprehensive and effective solution in the marketplace. nCrypted Cloud is the only solution that persistently encrypts ePHI (electronic personal health information) at rest on mobile devices and traditional personal computers. nCrypted Cloud also delivers superior security controls to ensure minimum necessary access is maintained at desired levels.

Cloud-based file storage and sharing – Level Setting

Cloud-based file storage and sharing is the underlying technology to access, synchronize, and share documents or files anywhere, anytime, with anyone, and from any device. Numerous cloud-based storage providers exist, however, the most prominent and the market leader is Dropbox.

Cloud-based sharing of ePHI is an emerging approach to improve collaboration between health care providers, patients, carriers, and business associates. Cloud-based file storage and sharing is an innovative technology that can be used to deliver more efficient health care services, improve health care outcomes, and reduce healthcare administrative costs.

HIPAA/HITECH Privacy and Security Compliance Requirements Overview

HIPAA/HITECH regulations have three major components: privacy, security, and breach notification.

The privacy component requires covered entities and related parties to limit access to ePHI to the minimum necessary and provide accounting of who accessed their ePHI if demanded by individuals.

The security component proscribes and details the required and addressable security safeguards necessary to protect ePHI.

Finally, a breach notification component that requires health care entities and related parties to notify individuals and government agencies if a privacy breach occurs.

How nCrypted Cloud Ensures HIPAA/HITECH Compliance

nCrypted Cloud security safeguards effectively and efficiently addresses all of the components of HIPAA/HITECH to ensure or exceed compliance.

nCrypted Cloud Ensures Privacy HIPAA Compliance

nCrypted Cloud's consumer and data-centric design ensures ePHI privacy requirements are met, since only explicitly authorized individuals can access ePHI whether it is stored in the cloud, on a mobile device, or on a traditional personal computer.

Also, nCrypted Cloud provides fine-grained privacy access controls such as read, print, or edit privileges, termination date triggers, and water marking at both the folder and document level. These security controls ensure access to ePHI can be maintained at the desired minimum necessary levels.

Finally, nCrypted Cloud provides all the indispensable audit trails, documenting who accesses ePHI, what they exactly did, when they did it, and where they did it. This provides all the necessary event data to provide an accounting of access activity to ePHI if demanded by an individual.

nCrypted Cloud Ensures Security HIPAA Compliance

nCrypted Cloud uniquely provides all the required and addressable security safeguards to meet, and in many instances

nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
Office: +1.617.520.4120

exceed, the HIPAA Security Rule requirements when using cloud-based storage and sharing technologies.

Specifically, nCrypted Cloud ensures:

- ePHI is encrypted at all times, whenever and wherever it goes, using industrial strength encryption algorithms. This means ePHI is persistently encrypted at rest on cloud storage servers and on any mobile devices and traditional personal computers. ePHI is also encrypted while being transmitted over the Internet.
- Only authorized individuals can access ePHI.
- Individuals are uniquely identified.
- Access to ePHI is protected by strong passwords.
- Access events to ePHI is captured and logged for monitoring and reporting purposes.
    - Who, what, when, and where
- Access to ePHI is terminated at the individual, folder, or document level when it is no longer needed.
- Notifications or alerts are sent to individuals or work group members when a change to ePHI records or files occurs.

nCrypted Cloud also gives health care entities or business associates the administrative capabilities to securely manage cloud-based file storage and sharing activities, including means to:

- Recover data for business continuity or forensic purposes.
- Prevent data loss.
- Back up and recover files or documents.

Finally, nCrypted Cloud provides a high availability (HA), secured, and hardened computer-processing infrastructure to ensure business continuity and data processing recovery in case of a disaster.

How nCrypted Cloud Protect Entities from Breach Notification Requirements

HIPAA regulations do not require breach notifications to individuals or government agencies if the ePHI information breached was encrypted.

Because nCrypted Cloud provides persistent encryption at all times (i.e. during transmissions and at rest on servers, traditional computers, and mobile devices), covered entities and related parties are not exposed to breach notifications requirements, related expenses, and potential fines.

How nCrypted Cloud Does It Better Then Competitors

nCrypted Cloud technology and its capabilities are superior to that of any other competitive product. While many competitive products make similar claims, nCrypted Cloud is the only one that offers a complete and comprehensive solution. nCrypted Cloud's ground breaking, unique technology and set of features include:

- Persistent encryption at all times and in all places.
    - While other competitive products only encrypt files and documents in transit and on their servers, nCrypted Cloud encrypts all files and documents on mobile devices (i.e. smart phones, tablets) as well as traditional computers (i.e. laptops, PCs).
- Feature rich privacy controls at the document or file level.
    - nCrypted Cloud delivers the most features to control the privacy of the documents or files including: read once only, access expiration date, print, view, edit privileges, and many more privacy control features.
- Extensive event logging and auditing capabilities.
    - nCrypted Cloud captures and records all individual activity to every document, file, or folder. It also provides a facility for the enterprise and workforce members to monitor activity, detect inappropriate use, and provide a book of record for forensic purposes.

Conclusion

nCrypted Cloud delivers a ground breaking cloud file storage and collaboration security solution that meets, and in many instances exceeds, HIPAA Privacy and Security requirements.

nCrypted-Cloud's consumer-centric design, data-centric security architecture, enterprise strength encryption, and auditing features make it the undisputed leader in the marketplace.