MediBackup HIPPA Compliance

The introduction to HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets the guidelines for how a person's protected health information is treated and safeguarded. Specifically, it spells out the rules for acquiring, modification, sharing, disclosure, transmission and protection of customer data by the specter of organizations engaged in providing healthcare and insurance services. Titled "covered entities", these participants are required to abide by the law of non-disclosure of customers' health data and facilitate its secure safekeeping and transmission. According to the law, the covered entity, which could be a health provider, pharmacy, insurance company, rehabilitation institution and other related parties are fully accountable for the integrity of information entrusted to it. The following requirements apply under the HIPAA legislation:

- **Privacy and confidentiality**
  Protected health information should not be disclosed to unauthorized parties without consent of the bearer. This includes non-disclosure to employers, third-party individuals or organizations not directly involved in providing medical, insurance services, etc. to the owner of the data.
- **Availability**
  The law stipulates that the copy of relevant information be provided to the bearer upon his/her request. The bearer has the right to edit and update the associated health records with the collaboration of the covered entity when necessary. The covered entity is also responsible for long-term storage and archival of the person's health data.
- **Protection**
  The law imposes rigorous restrictions on how the information is acquired, stored and transmitted. Regarding electronic data management which is prevalent today, it states that the covered entity must implement modern authentication and encryption mechanisms to prevent inappropriate viewing or eavesdropping.

Leveraging Amazon S3 as a HIPAA-compliant storage platform

The Amazon S3 platform offers a cost-efficient alternative to store your customers' digital records. All incoming data is automatically duplicated across several distinct locations to provide high durability and availability of customer data. The implemented encryption algorithms protect the confidentiality of in-transit (inbound and outbound) and "at-rest" (resident) data as required by the HIPAA provision. The industry-grade authentication helps delegate specific access control permissions to different user and administrator accounts.

Outsourcing HIPAA compliance

Instituting and enforcing HIPAA compliance is a demanding endeavor for small companies and private firms operating on a tight budget or possessing limited IT resources. Due to a variety of technical and

organizational constraints such as steep hardware costs, the level of technical expertise and the amount of expended time and effort, mandatory HIPAA compliance could be a deal breaker for the new entrants or at least an important consideration factor for seasoned players.

Delegating the task of protecting customers' data to the world's leading cloud storage provider can be a boon in this situation as it removes the technical variable from the equation.

For healthcare and insurance providers that do not wish or cannot afford to deploy costly onsite HIPAA-compliant infrastructures, offloading data to the HIPAA-certified cloud platform can replace or complement local storage solutions.

Another decisive win for the cloud storage is that it can be used to relocate massive amounts of locally residing historical records and archival data off the covered entity's hard drives, NAS and tape devices over the Internet to the protected vault, thus vacating additional room for more immediate storage needs and decreasing the cost of ownership.

The additional benefit of cloud storage is universal accessibility – cloud-based data can be shared with other authorized and intended recipients such as a fellow medical practitioner or the original owner of the information with ease and convenience. This is another HIPAA requirement that is effortlessly met with the advent of cloud technologies.

MediBackup Backup to meet your HIPAA challenge

In accordance to HIPAA, covered entities are obliged to assure their customers' data is highly available and can be recovered in case the disaster affects its main storage repository. This type of redundancy is generally achieved through data backups which are placed at a geographically disperse location.

MediBackup backup solutions utilize Amazon's proven AWS platform to store customer data. The software is deployed within seconds and helps to seamlessly backup customers' data, transfer it to the cloud, and retrieve it any time it's needed. The HIPAA requirements are addressed across every stage of the cloud backup transaction:

- *On transit:*
  any data sent to the cloud is automatically encrypted using the hardened SSL protocols which eliminate the possibility of an outsider gaining access to it.
- *At rest:*
  the information residing on the Amazon S3 cloud space is protected with the client side encryption up to 256 bit in strength and can incorporate over a dozen of industry-grade encryption algorithms (available options are: AES 128-256 bit, DES 64 bit, RC2 40-128 bit and 3DES 112-168 bit). Only the end user/covered entity owns the decryption key, which assures the integrity and privacy of data stored on the Amazon-run cloud.

At no point does MediBackup or any other unauthorized party have access to the customer data. All data transfers take place directly between the customer and Amazon S3, transparently to Medibackup which partakes to facilitate the exchange of the scrambled data only.

Final word

MediBackup data backup solutions facilitate transparent and secure aggregation, transmission, storage and retrieval of customer backup data from the local source to the Amazon cloud infrastructure, ensuring HIPAA compliance throughout any stage of the process.