mozyenterprise®

Mozy and HIPAA Security

The MozyEnterprise® advantage

Simple

Seamlessly manage backup, sync, and mobile access for multi-user and server environments from a single web-based console.

Secure

Your data is safe with military-grade encryption, world-class data centers, and EMC—a company built to last.

Affordable

Keep costs low with no hardware to purchase and minimal overhead required.

Contact Mozy

corporatesales@mozy.com
866.950.6699
www.mozy.com/enterprise

We can help you comply with the HIPAA Security and Privacy Rules

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that stores protected health information must ensure that all of the required physical, network, and process security measures are in place and followed. As a provider of HIPAA-compliant backup services that safeguard protected health information, we ensure that your data is protected in a way that complies with HIPAA regulations.

We view compliance as critical and also take steps to protect against anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information. We protect the interests of our customers and business by operating a holistic program focused on theconfidentiality, availability, and integrity of data.

Within our Information Security Management System (ISMS), we incorporate a combination of technical, administrative, and physical controls to safeguard personal information consistent with the industry standards and laws that are applicable to our customers. The principles behind each of these standards are for the data owner to retain control of sensitive data and ensure that only authorized parties can view that data.

Our software and services ensure that the appropriate safeguards are in place so that the protected health information you work with and store remains confidential and secure, as required by HIPAA. With MozyEnterprise, the HIPAA Security settings ensure that the requirements in the HIPAA Security Rule—including those for encryption, password restrictions, and data storage—are in place.

Encryption

- **Encryption key:** We require you set up a corporate encryption key (c-key) or personal encryption key, which is known only by you.
- **Encryption of data during backup:** During the backup process, all files are first secured with a personal 256-bit AES key encryption key and then transferred to our data center via a secure SSL connection.
- **Encryption of data at rest:** As required by HIPAA, your backed up data remains encrypted while stored at rest in our data center.

Password requirements

- **Length and complexity:** Passwords must be comprised of a minimum number of alphanumeric and special characters. Additionally, password validation is time- and logic-sensitive and requires manual updates.
- **Lockout:** Failed login attempts will automatically trigger account lockouts on an IP and user level.

Offsite backup

- **Physical security:** Our data centers are protected by gated perimeter access, 24x7x365 onsite staffed security and technicians, electronic card key access, and strategically placed security cameras inside and outside the building.
- **Remote/offsite backup:** Our service provides an automated remote or offsite backup and is a key component in any disaster recovery plan as protection against hardware failure, theft, virus attack, deletion, and natural disaster.
- **U.S. data centers only:** As required by HIPAA, we send and store all data from a HIPAA-compliant account to our U.S. data centers only.

Other items

- **Logical access:** Backed up data may be accessed via the password-protected, web-based administrative console by supplying a valid encryption key.
- **Written contingency plan:** The HIPAA Security Rule requires that covered entities have a written contingency plan for responding to system emergencies, including a detailed plan concerning the data backup and recovery process in the event of a disaster.

Note: There is no standard HIPAA certificate of compliance for backup software and services. For more information about HIPAA and HIPAA compliance, contact your legal counsel or refer to the HIPAA section of the U.S. Department of Health and Human Services' website.