

## Key Highlights

### Most Secure Solution

- AES 256-bit encryption & de-duplication at source
- SSL & OAuth protection

### Flexible Deployment Options

- Public Cloud
- Cloud-in-a-Box Appliance
- Private Cloud/On premise

### Unified Platform

- Secure File Sharing
- Managed Data Mobility
- Secure Endpoint Backup
- End-to-end Encryption
- VPN-free Anywhere Access
- Data Privacy

### Enterprises Control

- Centralized Administration
- AD-based Deployment
- Smart De-duplication
- Remote Wiping

# HIPAA & BAA

**Vaultize provides an enterprise platform for secure file sharing, anywhere access, endpoint data protection and mobility.**

Over the last few years, risk of data loss, security and compliance has grown due to exponential increase in unstructured data (files/emails). More and more data is moving out of corporate network because of proliferation of endpoints (laptops/smartphones/tablets) through workforce mobility and BYOD. There may not exist a standard for file sharing and endpoint backup for Health Insurance Portability and Accountability Act (HIPAA), however, Vaultize helps you comply with HIPAA security and privacy guidelines through the following capabilities:

- **Security of data in-transit and at-rest:** To ensure security and privacy, the data is encrypted using 256-bit encryption at source (on the device itself) before being transferred over the network (while other vendors encrypt the data only at the server). The network communication is performed over Secure Socket Layer (SSL). The data stays encrypted in the storage at the Vaultize Enterprise server (in all deployment options – public cloud, Cloud-in-a-Box Appliance and private cloud). In case of file sharing, the data is decrypted only on the receiving endpoint giving ensuring end-to-end protection of data. Additionally, all communication between your devices and Vaultize servers is protected by OAuth, the technology used by Google, Facebook, Twitter and other popular web services. This means only authorized users and devices can access the servers and eventually only their data.

- **Privacy:** Only the owner of the data is allowed to access his data. Even the administrator of an organization is not allowed to access user data from the centralized admin console. All major operations that affect data require individual user to reconfirm his password. For example, downloading data from other devices or synchronizing with other device requires password. So even if user's device is lost or falls in wrong hands, the data on Vaultize server and other devices is safe.
- **World-class Data Centers (for Public-cloud):** Vaultize servers used in our public-cloud offering are hosted in the world-class infrastructure of Rackspace cloud. Rackspace data centers are compliant with SAS 70 Type II, PCI DSS and ISO 27001 standards. They are also Safe Harbor certified. Rackspace network is Cisco-certified and offers 100% up-time. More than half of Fortune 500 companies host their sites or apps with Rackspace.
- **Data Backup and Recovery:** Vaultize provides policy based unstructured data (files) backup and restore. It provides unlimited versioning and point-in-time copy restore. In public cloud the data chunks are stored in data centers across multiple disaster zones ensuring high-availability and reliability of backed up data.
- **Data Privacy:** With Data Privacy – an option available in Vaultize, the encryption keys are never stored on any infrastructure that is not under enterprise control – ensuring that the customer is in complete control of privacy of data and, ownership of data is retained by the customer. The data is thus completely secure from any unauthorized access while in motion or at rest in the cloud. The ability to access usable data remains solely with the customer as they hold the encryption key. This way, a Vaultize customer can comply with privacy and residency requirements by virtue of keeping the encryption keys within jurisdiction, regardless of the actual physical location of the backup and sharing data.
- **Enterprise Control and Visibility:** Vaultize is built with full enterprise control and visibility for enterprise IT. All features including - anywhere access and sharing capabilities are completely under the control of enterprise IT. That means IT can selectively give access and sharing permissions to users within the organization on the need basis.

Although not required through the HIPAA Privacy Rule, Vaultize can sign a Business Associate Agreement (BAA) for those customers looking to be HIPAA compliant in their file sharing, data protection and mobility requirements. Our Professional Services can also work with our customers or any necessary parties to ensure compliance.

For more information please log on to [www.vaultize.com](http://www.vaultize.com) or reach us at [sales@vaultize.com](mailto:sales@vaultize.com)