Citrix ShareFile security and compliance

How ShareFile safeguards your data.

Features	Description
Data protection during file transfer	
File transfer	ShareFile employs SSL/TLS protocols to protect client authentication, authorization and file transfers.
High-grade encryption	ShareFile secures files in transit with no less than 128-bit encryption using industry-standard encryption protocols.
File integrity	ShareFile employs a keyed hashed message authentication code (HMAC) to authenticate and ensure the integrity of intra-system communications. ShareFile verifies file size and file hash to ensure integrity.
Link generation	ShareFile download links are uniquely and randomly generated using strong hash-based message authentication codes. ShareFile provides technical countermeasures to protect links from guessing attacks.
Data protection during storage	
Datacenters	ShareFile uses SSAE 16 Type II accredited or ISO 27001 certified datacenters to host the SaaS application and metadata. All files are stored in SSAE 16 Type II (SOC1), SOC2 and ISO 27001 accredited datacenters with high availability and durability ratings.
Encryption	ShareFile stores client files at rest using AES 256-bit encryption, a Federal Information Processing Standards (FIPS) encryption algorithm.
Firewalls	Files are processed using systems protected by securely configured firewalls that effectively limit and control access to network segments.
Redundant storage	Files are stored in replicate with leading Infrastructure-as-a-Service (IaaS) providers that ensure high file durability and availability.
Backup	Files are backed up according to configurable file-retention and versioning settings.
Configurable settings	
Password policy	Clients have the option of configuring password policies, including password history, expiration, and complexity controls such as length, uppercase and lowercase letters, at least one number, and at least one special character.
SAML 2.0 enabled single sign-on	ShareFile supports SAML 2.0 for single sign-on and integrates with most SAML-compatible identity management solutions.
Custom SMTP (mail) settings	ShareFile enables clients to route email messages though their own mail servers. When enabled, all emails sent through ShareFile will be routed through the client's mail server, instead of ShareFile mail servers. Clients may optionally configure the connection to support SSL.

Multi-factor authentication	Clients may set up a multi-factor (or strong) authentication process that requires submission of the account password and a secondary authentication, such as Google Authenticator or SMS/ text message, in order to access the account. ShareFile supports various two-factor and two-step authentication methods including forms and token-based authentication as well as SMS, voice and backup codes.
File retention	Users can choose to automatically delete files a certain number of days after upload to support retention preferences and policies.
File versioning	Users can view different versions of a file uploaded with the same name to ensure that no changes are lost between updates or edits.
Terms and conditions	Terms and conditions can be displayed on the login page, with the option of including a check box on the login screen that must be marked to indicate compliance with the terms before logging in.
FTP/FTPS	By default, file transfers occur over HTTPS (Port 443). Optionally, clients can connect to ShareFile using FTP or FTP over SSL (FTPS connection over port 990), an inherently more secure protocol than FTP. Users can connect to ShareFile directly from an FTP/FTPS program, providing a way for users to upload or download files to or from a secure location while using existing FTP/FTPS programs.
WebDAV support	ShareFile supports WebDAV over SSL. Users can connect with ShareFile through WebDAV over SSL to various clients, allowing interaction with ShareFile files and folders without logging in to the ShareFile website.
OAuth 2.0 support	ShareFile supports the OAuth authentication protocol with client side configurable OAuth expiration.
Account lockout	ShareFile can configure your account to lock for five minutes after five invalid logon attempts to prevent account tampering. This application control is an account preference that can be customized to meet individual compliance needs.
Customized folder permissions	Administrative users can set folder permissions to ensure that employee and client users may only access specific folders. These permissions may be set to propagate to subfolders or apply only to specific subfolders.
Account activity reporting	ShareFile allows administrative users to run and access various reports on activity, usage, storage and permissions. Reports can be run on demand or emailed daily, weekly or monthly.
Email notifications	Users can choose to have customized notifications sent in real time or in a consolidated daily message.
Access log retention	Detailed file-access logs are retained for at least one year.
Mobile device security	
File self-destruct	Users can determine the number of days downloaded files remain on a device before they are automatically removed after a lapse in user login or account access, even if offline.
External applications interaction	Users can control whether downloaded files can be opened outside of the ShareFile application.
Offline access	Downloaded files can be accessed on iOS and Android mobile devices even when offline.
Permissions management	Users can manage permissions and access rights to ShareFile files and folders from a mobile device.
PIN lock or password	Users can choose to require a PIN or password to access files. Files downloaded after the PIN or password is configured are encrypted by the application on the device. Administrative users can require PIN lock or password.
Restrict modified device	Administrative users can enable this feature to restrict other users from using the iPad or iPhone apps on jail-broken devices.
Remote wipe	Users can remotely lock and wipe ShareFile data from a lost or stolen device.
XenMobile MDM/MAM (optional)	Citrix XenMobile can augment device and application security.

Email	
ShareFile Plugin for Microsoft Outlook	With the plugin, email attachments can be replaced with secure ShareFile links to files. Users can also use the plugin to create a 'Request a file' link that allows recipients to securely upload a large file to the user's ShareFile account.
Attachment conversion	ShareFile allows users to send secure links to files and folders up to 10 GB in size, bypassing limitations on attachment size in email systems and preventing email bounce backs.
Customer SMTP configuration	Users can configure ShareFile to send messages through individual mail servers with the option of configuring ShareFile to send messages to a mail server over an SSL encrypted segment (provided the mail server supports SSL connections).
Virtual Data Room (VDR)	
Document watermarking	Customizable dynamic watermarking is available whenever documents are viewed, downloaded or printed to discourage unauthorized distribution of data.
View-only permission	Use "view-only" permissions to ensure that files cannot be downloaded, printed or saved. Access to your documents is available only in ShareFile's web-based viewer.
Enhanced analytics	Administrative users can track how and when files are being accessed, including data on the most active users, recent searches, most-viewed documents and longest-viewed documents.
Document Q&A	Users can submit questions directly to administrative users via the data room. Answer questions privately or provide added clarity with secure public or private questions annotated onto a file. Receive real-time notifications when comments are made, or export the entire question log.
File archiving	
Archiving for financial services	When enabled, ShareFile's archiving feature supports your compliance with federal regulations regarding data retention by retaining all files, links, attachments and versions either uploaded or sent through the ShareFile SMTP email server for a customizable period of at least three years.
ShareFile Cloud for Healthcare	
HIPAA	ShareFile provides multiple technical safeguards to support client compliance obligations under HIPAA. ShareFile supports your HIPAA compliance and will provide and sign a HIPAA Business Associate Agreement upon request.
Audit controls	Clients can use the tools provided within ShareFile to review account activity, such as account usage and access to files and folders, to track disclosures.
Unique users and authentication	ShareFile provides clients the capability to assign individual user accounts based on unique email addresses. Clients are responsible for providing unique accounts and logins to each client.
Encryption	ShareFile handles the encryption and decryption of all files, including those presumed to contain PHI. Clients can, at their discretion, also encrypt files prior to uploading them to their ShareFile account.
Integrity controls	To help ensure that PHI has not been altered or destroyed in transit or at rest, ShareFile verifies file size and uses industry-accepted hashing algorithms to verify file integrity during file transfers.
Physical safeguards	Measures are in place to prevent unauthorized persons from gaining physical access to datacenters and systems, where PHI may be processed or stored. Infrastructure-as-a-Service providers do not have access to unencrypted customer files and do not manage encryption on Citrix's behalf.
Testing and evaluation	To maintain compliance with the HIPAA Security Rule, Citrix engages an independent third party to perform periodic risk assessments and gap analyses.