CITRIX ShareFile

Citrix ShareFile and Title 21 CFR Part 11

How ShareFile helps you address federal guidelines for electronic records and signatures

By Manny Landron, Senior Manager, Security and Compliance
Citrix ShareFile

What is Title 21 Code of Federal Regulations (CFR) Part 11?

Title 21 CFR Part 11 is a Food and Drug Administration (FDA) guideline on electronic records and signatures that defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable and equivalent to paper records.

Does ShareFile meet the technical requirements of Title 21 CFR Part 11 for a compliant system?

Yes, ShareFile meets the technical requirements outlined in Title 21 CFR Part 11 for a compliant system.

What are the specific technical requirements?

Discerning invalid or altered records.

ShareFile performs file-integrity checking to ensure that the file you upload is the file we store. ShareFile also provides users with the ability to configure file versioning to track changes to files.

Generating accurate and complete records.

ShareFile performs integrity checking to ensure the accuracy and completeness of uploaded files. Files are protected in transit using SSL/TLS encrypted segments so that no one can intercept the file and modify it in transit.

Protecting records throughout the record-retention period.

ShareFile provides users with the ability to configure file-retention policies, and provides the requisite security controls necessary to protect uploaded files throughout the file-retention period.

Generating a cumulative audit trail through the record-retention period that contains date and time of operator entries with the description of actions taken.

ShareFile supports audit trails with reporting and versioning. ShareFile records file access and account activity and provides the customer with the capability to generate audit-trail reports on demand in various formats, including PDF.

Using authority checks to limit access to the system to authorized individuals.

ShareFile requires authentication via either username and password or identity management systems; users may also choose to require multi-factor authentication to further protect an account. The service manages authorization based on the access control lists that enforce the degree of privilege a user maintains over a file. All files are uploaded and downloaded using SSL/TLS protocols with a minimum of 128-bit encryption and a maximum of AES 256-bit encryption in transit (depending on the

user's browser settings). Files are encrypted at rest using AES 256, an encryption algorithm approved by the Federal Information Processing Standards (FIPS).

Limiting access to system functions to authorized users and using checks to determine the validity of the source of data input.

ShareFile performs file-integrity checking to ensure that the file you upload is the file we store. Administrative users are provided with the ability to provision and de-provision users and grant granular permissions to specific users for specific functions using a role-based approach.

Limiting data input to authorized sources.

As mentioned above, administrative users are provided with the ability to provision and de-provision users and grant permissions to specific users for specific functions. Customers should train and educate their employees and clients to use ShareFile in a compliant manner.

Establishing and adhering to written policy that governs use of electronic signatures.

ShareFile supports the use of electronic signature and protects file integrity regardless of service provider. Users are responsible for using ShareFile in a compliant manner.

ShareFile partners with RightSignature to provide the capability to send documents for signature directly from a ShareFile account. Users may digitally sign files using any digital signature utility and ShareFile will preserve the integrity of the file and the digital signature.

Protecting transmission of data from point of creation to receipt.

As mentioned above, all data is protected in transit. All files are uploaded and downloaded using SSL/TLS protocols with a minimum of 128-bit encryption and a

maximum of AES 256-bit encryption in transit (depending on the user's browser settings). Files encrypted at rest using AES 256, an encryption algorithm approved by the Federal Information Processing Standards (FIPS).

Does ShareFile meet the administrative or procedural requirements of Title 21 CFR Part 11?

ShareFile meets all of the technical requirements necessary for customers to achieve Title 21 CFR Part 11 compliance. This does not mean that by simply using ShareFile you are Title 21 CFR Part 11 compliant. Because your compliance is a shared responsibility, we can meet the technical requirements for your compliance, but you must also implement relevant procedural and administrative safeguards and configure the application in a compliant manner.

What procedural and administrative steps do I need to take to meet Title 21 compliance when using ShareFile?

ShareFile gives you the tools to be compliant, but they must be used correctly. One example is that ShareFile allows you to restrict users on the account to limited access to certain files. However, if you do not choose to set up the granular permissions to appropriately restrict user access, you may not be compliant.

How can I set up ShareFile in order to be compliant?

The best way is to work with your account manager. Your account manager will be happy to provide training, assist with account setup and ensure that you understand how to set up granular permissions and other safeguards. If you need a quick answer about setting up these safeguards, you can also call our customer support line at 1-800-441-3453 and speak with a support representative.