FILECLOUD

FDA 21 CFR Part 11 Requirements - FileCloud Checklist

Discover how FileCloud can support FDA 21 CFR Part 11 requirements for electronic records and signatures.

FileCloud is an enterprise grade file sharing and content governance solution that offers controlled data sharing and collaboration tools for healthcare, life sciences, and pharmaceutical organizations. Read our checklist to learn how FileCloud can support FDA requirements for electronic record and signature security.

Title 21 Chapter I Subchapter A Part 11 (86 FR 68830, Dec. 3, 2021)

Subpart B - Electronic Records		FileCloud Support
Scope	This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.	FileCloud provides services in line with a shared responsibility model, in which FileCloud is responsible for the application, and has a shared responsibility with Amazon Web Services for the underlying infrastructure, within the scope of provided services. The customer is responsible for data, applications, and configurations beyond the scope of provided services. Requirements entirely outside of service scope are marked as "N/A."

§ 11.10 Controls for closed systems		FileCloud Support
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:		Access controls, authentication mechanisms, encryption for data at rest and in transit, immutable audit logs, acitivity logs, custom reports, antivirus scanning, Content Disarm & Reconstruction (CDR) integration, SIEM integration, Signority e-signature integration, workflow automation, retention policies, content classification, Data Leak Protection (DLP) rules, Digital Rights Management (DRM), etc.
a.	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Audit logs, Live Document Audit Trail
b.	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	User activity logs, which can be viewed and filtered through the FileCloud Admin dashboard (Audit Logs) and exported as CSV files. Signority has a live audit trail within the platfor for each document as well as an audit trail that arrives with the completed (signed) document in pdf format.
c.	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Retention policies (Enterprise Advanced)
d.	Limiting system access to authorized individuals.	Role Based Access Controls, Two-factor Authentication (2FA), Single Sign-on (SSO) integration, AD/LDAP integration, Granular permissions, Session & Device management

Title 21 Chapter I Subchapter A Part 11 (86 FR 68830, Dec. 3, 2021)

	§ 11.10 Controls for closed systems	FileCloud Support
e.	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Comprehensive audit logs that cannot be altered or overwritten.
f.	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Workflow automation
g.	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Password-based login & password strength requirement policies, Role Based Access Controls (RBAC), Two-factor Authentication (2FA), Single Sign-on (SSO) integration, AD/LDAP integration, Granular permissions, FileCloud Signority e-signature
h.	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Antivirus scanning is available by default, with the option of integrating other services. Everfox Content Disarm and Reconstruction (CDR) is also available as an integration to provide file scanning for embedded threats.
i.	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	N/A
j.	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Global, user, and group policies, along with custom Terms of Service (ToS), notifications, and other in-app messages can support this requirement. Email and SMS authentication can be used to verify the recipient before they are allowed to sign. With Digital Signatures, a digital certificate is then applied to the document to seal it when finalized to ensure integrity of document making any future changes immediately detectable.

Title 21 Chapter I Subchapter A Part 11 (86 FR 68830, Dec. 3, 2021)

§ 11.10 Controls for closed systems		FileCloud Support
k.	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	N/A

§ 11.30 Controls for open systems	FileCloud Support
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. **Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.**	Access controls, authentication mechanisms, encryption for data at rest and in transit, immutable audit logs, acitivity logs, custom reports, antivirus scanning, Content Disarm & Reconstruction (CDR) integration, SIEM integration, Signority e-signature integration, workflow automation, retention policies, content classification, Data Leak Protection (DLP) rules, Digital Rights Management (DRM), etc.

§ 11.50 Signature manifestations		FileCloud Support
a.	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Signority offers an option to enable "Regulatory Information" on the signature tag. Regulatory information captures 1) the printed name of the signer and 2) the date and time the signature was executed. The meaning associated with the signature is not currently captured. The Globally Unique Identifier (GUID) of the document is included.
b.	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Signority captures and stores the above information as part of the signature graphic. Once the signature is complete, the details, including the GUID and the associated regulatory information, cannot be modified or changed. Signatures are tracked in a dashboard, and all FileCloud controls apply to files sent for signature through Signority when used as an integration (rather than a standalone application).

Title 21 Chapter I Subchapter A Part 11 (86 FR 68830, Dec. 3, 2021)

§ 11.70 Signature/record linking.	FileCloud Support
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	In Signority, enabling "Regulatory Information" on the signature tag displays the GUID that is associated with the GUID of the document - this information is part of the digital signature. The secured seal, inherent to Signority's audit trail, is tamper-proof and digitally encrypted. If the audit trail document is altered or edited in third-party software, the seal will immediately break, rendering it invalid.

Subpart C - Electronic Signatures		FileCloud Support
Scope	Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.	FileCloud provides services in line with a shared responsibility model, in which FileCloud is responsible for underlying infrastructure within the scope of provided services. The customer is responsible for data, applications, and configurations beyond the scope of provided services. Requirements entirely outside of service scope are marked as "N/A."

§ 11.100 General requirements		FileCloud Support
a.	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Signority enables senders to ensure each signature is unique to one individual by setting up multi factor authentication and not allowing other signers to sign on their behalf without a pin code that is sent direct to the signers phone number or email. The audit trail also captures the IP address of the signer to ensure accountability and compliance.
b.	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Multi factor authentication with SMS or email pin code is used to verify the identify of the individual before allowed access to the document for signing.

Title 21 Chapter I Subchapter A Part 11 (86 FR 68830, Dec. 3, 2021)

§ 11.100 General requirements		FileCloud Support
c.	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	This agreement is completed from the perspective of the organization planning to collect and use esignatures.

§ 11.200 Electronic signature components and controls		FileCloud Support
a.	Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	Signority uses a two-factor identification method. Each individual is identified using a valid email address and must confirm access by entering a time-sensitive PIN code sent to their email or phone number. This process verifies the individual's control over their email and or phone.

Title 21 Chapter I Subchapter A Part 11 (86 FR 68830, Dec. 3, 2021)

§ 11.200 Electronic signature components and controls		FileCloud Support
b.	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Signority does not use biometric-base authentication. Instead, we rely on email and phone number authentication methods.

§ 11.300 Controls for identification codes/passwords		FileCloud Support
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:		N/A
a.	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	N/A
b.	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	N/A
c.	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	N/A
d.	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	N/A
e.	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	N/A

Interested in learning more about FDA and GMP (Good Manufacturing Practice) regulation?
Read our GxP Compliance - Healthcare and Life Sciences White Paper →

About Us

FileCloud is a hyper-secure file sharing, collaboration, and governance solution that provides industry-leading tools for compliance, data leak protection, data retention, and digital rights management. Workflow automation and granular control of content sharing are fully integrated into the complete feature stack.

The FileCloud platform offers powerful file sharing, sync, and mobile access capabilities on public, private, and hybrid clouds. Headquartered in New York, New York, USA, FileCloud is deployed by top Global 1000 enterprises, educational institutions, government organizations, and managed service providers, with over one million users worldwide.

1M+
USERS

3000+
ENTERPRISES

100+
RESELLERS

90+
COUNTRIES

125 Park Avenue FL 25
New York, NY 10017-5550

Fax: +1 (866) 824-9584

https://www.filecloud.com

Copyright Notice