FILECLOUD

FDA Compliance — Title 21, Chapter 1, Part 11

white paper

Title 21, Chapter 1 is a set of regulations established by the Food and Drug Administration (FDA) Department of Health and Human Services (DHHS). Part 11 specifically addresses electronic records and signatures. These regulations are codified by the Electronic Code of Federal Regulations (eCFR).

FDA Compliance

In the United States, the Food and Drug Administration is responsible for regulating food, drugs, and medical devices that are produced for the consumer market.

Production involves the creation and transmission of massive amounts of information via product proposals, preliminary market research, laboratory research datasets, summaries, and figures, production cycle maps, internal and external communications, marketing strategies, and distribution contracts, among other data.

In response to the rapid increase of digital records, the FDA has established Title 21, Chapter 1, Part 11. These regulatory requirements are published by the Electronic Code of Federal Regulations. The entire set of regulations pertaining to digital documents and signatures is often referred to as eCFR Title 21, Part 11.

FileCloud is a hyper-secure Content Collaboration Platform (CCP) that comes with advanced data governance tools to support compliance with eCFR Title 21, Part 11.

These include powerful features such as:

- Easy to use Admin and User Interface
- Granular File and Folder Permissions
- Role-Based Access Controls (RBAC)
- Comprehensive Audit Trails and Activity Reporting
- Metadata Management
- Content Classification
- Data Leak Prevention
- Workflow Automation
- Digital Rights Management (DRM), * integrated Compliance Center

FileCloud also offers multiple deployment options, either on-premises in your private server (FileCloud Server), with a third party, public cloud provider like AWS or Azure (FileCloud Online), or as a hybrid model. Integrate FileCloud with your existing Active Directory, SIEM, or SSO solutions and leverage the built-in and admin-enabled security tools, including two-factor authentication and 256-bit AES encryption.

Scope of e-CFR Title 21 Part 11

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) 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.

(c) 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.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with §11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

FileCloud is recognized as a 2018, '19, '20 and '21 Gartner Peer Insights Customers' Choice for Content Collaboration Platforms

By 2022, 50% of midsize and large organizations in mature regional markets will use a content collaboration (previously known as Enterprise Sharing and Sync - EFSS) platform to implement document workflows and improve collaboration and productivity.

(f) This part does not apply to records required to be established or maintained by §§1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(g) This part does not apply to electronic signatures obtained under §101.11(d) of this chapter.

(h) This part does not apply to electronic signatures obtained under §101.8(d) of this chapter.

(i) This part does not apply to records required to be established or maintained by part 117 of this chapter. Records that satisfy the requirements of part 117 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(j) This part does not apply to records required to be established or maintained by part 507 of this chapter. Records that satisfy the requirements of part 507 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(k) This part does not apply to records required to be established or maintained by part 112 of this chapter. Records that satisfy the requirements of part 112 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(l) This part does not apply to records required to be established or maintained by subpart L of part 1 of this chapter. Records that satisfy the requirements of subpart L of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(m) This part does not apply to records required to be established or maintained by subpart M of part 1 of this chapter. Records that satisfy the requirements of subpart M of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(n) This part does not apply to records required to be established or maintained by subpart O of part 1 of this chapter. Records that satisfy the requirements of subpart O of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(o) This part does not apply to records required to be established or maintained by part 121 of this chapter. Records that satisfy the requirements of part 121 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

21 CFR Requirement and Reference

Ref. No.	Details	FileCloud
	Sec. 11.10 Controls for closed systems.	
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	✓
11.10 (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.	N/A
11.10 (c)	Identify and mitProtection of records to enable their accurate and ready retrieval throughout the records retention period.igate risk associated with unidentified wireless access points connected to the network.	✓
11.10 (d)	Limiting system access to authorized individuals.	✓
11.10 (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 required for the subject electronic records and shall be available for agency review and copying.	✓

11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	N/A
11.10 (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.	✓
11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	N/A
11.10 (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
11.10 (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.	N/A
11.10 (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.	✓

Sec. 11.50 Signature manifestations.		
11.50(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.	N/A
11.50(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).	N/A

Sec. 11.100 General requirements.		
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	N/A
11.100(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.	N/A

11.100(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 submitted in paper form and signed with a traditional handwritten signature to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (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.	N/A

Sec. 11.200 Electronic signature components and controls.		
11.200 (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 the collaboration of two or more individuals.	N/A
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A

Sec. 11.300 Controls for identification codes/passwords.		
11.300 (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.	✓
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	✓
11.300 (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
11.300 (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.	✓
11.300 (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

About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.

1M+
USERS

3000+
ENTERPRISES

100+
RESELLERS

90+
COUNTRIES

13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

support@filecloud.com
https://www.filecloud.com

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
REUTERS
US Army Corps of Engineers
NASA
COLUMBUS REGIONAL HEALTH
TOYOTA
Deloitte.

Copyright Notice