FDA CFR 21 Part 11

How Papercurve helps you meet the regulations

papercurve

Table of Contents

A message from the CTO

Papercurve was built from the ground up to help fast-growing life sciences companies maintain compliance. The Food and Drug Administration has outlined guidance about how companies should implement and maintain electronic records and signatures – known as FDA CFR 21 part 11. This document details how Papercurve meets or exceeds all aspects of the regulation.

Thank you.

Antonio Salumbides
Chief Technology Officer

Electronic Records

Controls for closed systems

Papercurve is a controlled system which by the FDA's definition means an "environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system."

Papercurve is validated during the quality assurance process to ensure that content is displayed in a reliable and consistent manner. Content cannot be altered without an auditable history. For example, previous versions of a document are stored and available to other users.

Papercurve institutes a pre-defined order of sequencing of steps and events in order to enforce compliance. The sequencing mechanism is core to the platform, automatic, and independent of users. These sequencing rules govern each step of the approval process. An administrator has access to the audit log to validate operational checks.

In the event that the FDA requests a copy of any document, users with the appropriate permissions can download the file in its original format - PDF, Word, PowerPoint or Excel and submit it to the Agency.

Use of authority checks

The Papercurve platform by default ensures that only authorized users can use the system, electronically sign an approval, alter records and perform other operations. Roles are created as groupings of permissions and each user is given a role that controls their individual permissions. In order to further limit a user's access, we have another layer that is the library permissions system. This allows administrators to lock users into only seeing specific groupings of content.

Use of device checks

Papercurve will not accept connections, and therefore will not accept commands or data, from unauthenticated sources.

We further limit connections where the IP address of a request does not meet our security standards and firewall rules. Our environments are hardened environments, Papercurve will only communicate over HTTPS/Secured TCP, which prevents a third party from modifying data being transmitted.

We optionally provide Two-factor authentication (2FA) to ensure that any change in IP address between requests is subject to a second device authentication.

Records Retention

Papercurve retains every copy of every file ever uploaded to the platform. No files are permanently deleted from the platform unless requested by the client. In the Papercurve user interface, there is an option to “delete” a file, depending on the user’s permission level. Files that are “deleted” in the platform are retained and made available upon request.

When a customer ends their contract with Papercurve and is no longer using the platform, all versions of all files will be made available to the client as part of the offboarding process.

Limiting access to authorized individuals

The Papercuve platform controls access to only authorized individuals. Administrators invite users to the platform on a per-person basis.

Granular controls to content allow each user to be granted or denied access to approved content “libraries”, which are collections of content. For un-approved content, the author invites a user to collaborate or approve the content on an as-needed basis.

Audit Trail

Users with “admin” permissions have access to the “Activity Log” which is secured with the user’s login and password. The Activity Log is a time-stamped audit trail of

most user actions in the Papercurve platform. There are 2 types of Activity Log records – Document and User.

User records include any new user, edit of user details, change in role, deactivation of account, who made the change to the user, and date stamp when the change was made.

Document records include adding, editing, deleting, renaming and uploading new versions of a document, along with a date stamp, a document ID and the person who performed the action. All review and approval actions are also stored in the Activity Log. This includes adding and removing reviewers, submitting your approval, approving with changes, or requesting a new version.

The Activity Log is an independent, computer-generated audit trail that cannot be altered. It can be downloaded in CSV (Comma Separated Values) format between any date range.

Training

The Customer Success team provides training to all users as part of the onboarding process to ensure the customer understands the platform and key functionality. As you hire new team members, the Papercurve Customer Success team will provide training to ensure familiarity with the platform. Periodically the Customer Success team will provide your team with refresher training and updates to the platform as required.

Documentation

Papercurve has a self-serve knowledge base at https://help.papercurve.com with articles and videos about functionality and best practices. Papercurve maintains a process to keep documentation current with production environments. There is a time-stamped audit trail of when an article is updated, and which Papercurve employee made the change.

Controls for open systems

Papercurve does not allow users to access or modify any electronic records without a username and password. As such, there are no additional procedures or controls with respect to open systems.

Signature manifestations

The Activity Log contains the information required by FDA CFR 21 part 11 including:

- The name of the signer
- The date and time when the signature was executed
- The meaning (approve, approve with changes or submit new version)
- The document identified including title and document ID to uniquely identify the document, including the document version number

Signature record linking

Electronic signatures are linked to electronic records using the document ID and cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means.

Electronic Signatures

Each electronic signature is unique to the individual and tied to their user ID. The identity of the individual is tied to the email address associated with the user ID.

Electronic signatures in Papercurve contain the following components to identify a user:

- A unique ID for the user (not visible in the user interface)
- Email address (identification code)
- Password

When a user submits their electronic signature, their identity is verified with the user's password.

Controls for logins and passwords

Papercurve does not allow more than one user with the same email address to be in the same Workspace to maintain uniqueness.

Only users with the "Admin" role can change the email address of a user. This change is stored in the Activity Log and made available during an audit.

The Papercurve platform and technology checks password minimums, strength insurance, password length and prevents the reuse of a configurable number of prior passwords. In addition to organizational procedures, the Papercurve platform and technology checks password minimums, strength insurance, password length and prevents the reuse of a configurable number of prior passwords. In order to establish a preference, please contact our customer success representative in order to establish this configuration process.

Your role in maintaining CFR 21 part 11 compliance

There are parts of the CFR 21 part 11 regulation that are beyond the scope of the software. Maintaining compliance is a partnership and we all have a role to play. Here are your key responsibilities in staying compliant.

1. Ensure employees have the training and experience to perform their assigned tasks.

2. 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.

3. Papercurve User IDs are associated with email addresses in the platform. It is the role of the client to correctly verify the identity of the individual and control access to an email address.

4. Ensure each user is given the appropriate level of access to the Papercurve platform.

5. In the event that an employee's corporate email or a device with access to corporate email is compromised, contact support@papercurve.com to temporarily deactivate a user until the breach is resolved.

6. When an employee leaves the company, ensure a user with an "admin" role deactivates the terminated user's Papercurve account, or contact support@papercurve.com for assistance.

Appendix

FDA Code of Federal Regulations Title 21

PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

---

https://ecfr.federalregister.gov/current/title-21/chapter-I/subchapter-A/part-11

Contents

Subpart A – General Provisions

§11.1 Scope.

(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.

(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.

[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004; 79 FR 71253, 71291, Dec. 1, 2014; 80 FR 71253, June 19, 2015; 80 FR 56144, 56336, Sept. 17, 2015; 80 FR 74352, 74547, 74667, Nov. 27, 2015; 81 FR 20170, Apr. 6, 2016; 81 FR 34218, May 27, 2016]

§11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) ***Act*** means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) ***Agency*** means the Food and Drug Administration.

(3) ***Biometrics*** means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) ***Closed system*** means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) ***Digital signature*** means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) ***Electronic record*** means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) ***Electronic signature*** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) ***Handwritten signature*** means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) ***Open system*** means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B – Electronic Records

§11.10 Controls for closed systems.

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:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(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.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(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.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(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.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(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.

(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.

(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.

§11.30 Controls for open systems.

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.

§11.50 Signature manifestations.

(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.

(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).

§11.70 Signature/record linking.

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.

Subpart C – Electronic Signatures

§11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(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.

(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.

§11.200 Electronic signature components and controls.

(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.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

§11.300 Controls for identification codes/passwords.

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:

(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.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).(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.

(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.

(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.