LabArchives and 21 CFR Part 11

Background and Introduction

21 CFR Part 11 contains the regulations of the US Food and Drug Administration with regard to electronic records and electronic signatures.

This document was prepared by LabArchives to describe some of the controls, features, and security precautions that are built into LabArchives and how using the LabArchives platform may facilitate your implementation of certain sections of 21 CFR Part 11. Because compliance with 21 CFR Part 11 involves much more than the simple installation of a data management system, however, this paper is not intended to be a comprehensive document on compliance, nor any guarantee that using LabArchives will ensure compliance. It is recommended that those who need to comply with 21 CFR Part 11 seek legal advice in order to ensure full compliance.

Requirements of 21 CFR Part 11


There are several sections of this regulatory code that will be of particular interest to those adopting an electronic document management platform. These are summarized below, along with commentary about the role of LabArchives as part of an overall methodology of compliance.

Subpart B – Electronic Records

Section 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.

LabArchives’ Response: LabArchives offers a secure, accurate, and reliable platform for the storage of electronic data. LabArchives stores all versions of all data, including recording of the IP address of the computer from which it was entered, and a date and time stamp obtained from the National Institute of Standards and Technology (NIST). In fact, it is not possible for users to delete any data, and modifications are all recorded with the above identification technology.
(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.

**LabArchives’ Response:** LabArchives provides the ability to provide access to any authorized individual, enabling a representative of the agency to review all records. By providing access to all, or a selected part, of a LabArchives Notebook, the agency will be able to view records, complete with all versions and date, time, user name, and IP address. LabArchives also provides the ability to download records into HTML or PDF documents.

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

**LabArchives’ Response:** LabArchives records, when using our “Cloud” version, are stored for a minimum of three years beyond the subscription period, which complies with the standard “records retention period” for 21 CFR Part 11. For local installations it is, of course, the responsibility of company management to make provision to retain all data for the prescribed time period.

(d) Limiting system access to authorized individuals.

**LabArchives’ Response:** LabArchives requires user authentication via user name and password; it also records the IP address for every entry. It is, of course, incumbent on company management to issue such login credentials to authorized individuals, and to remove said credentials when required.

(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.

**LabArchives’ Response:** As described above, LabArchives generates a date and time stamp from an independent, trusted third party (National Institute of Standards and Technology) for each and every entry made in the system, whether creating or modifying records. There is no option to actually delete a record (the delete feature simply moves the record to a “Deleted” folder where it remains intact). Thus, the “audit” trail is permanent and a byproduct of using the LabArchives platform.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

**LabArchives’ Response:** First, a note that the "as appropriate" phrase at the end of the sentence indicates this is not a requirement for ALL companies wishing to comply with 21 CFR Part 11, but rather only those having a pre-defined sequence of events that operators must follow in order to comply with an FDA regulation or other cGMPs, and which must be memorialized as records. These operational requirements are beyond the scope of LabArchives.

(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.

**LabArchives’ Response:** LabArchives includes a descending level of user, including “Owner,” “Administrator,” “User,” and “Guest.” Rights to specific information within Notebooks can be controlled by the Owner or Administrator, restricting access and/or limiting it to the ability to read only. Electronically signing a record is limited as well, and all information, including user, date and time, and IP address, are recorded at that time. Further modification to said data is not allowed following electronic signature.

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

**LabArchives’ Response:** LabArchives requires terminal login and records the IP address of the computer from which each Entry is made.

(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.

**LabArchives’ Response:** LabArchives offers web-based education sessions to provide your staff with training on using our platform.

(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.

**LabArchives’ Response:** This is the responsibility of the company.

(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.

**LabArchives’ Response:** These relate in most respects to controls and procedures put in place by the company and are outside the realm of LabArchives’ direct control.

---

**Sec. 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.

**LabArchives’ Response:** Not applicable to LabArchives.

---

**Section 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).

**LabArchives’ Response:** LabArchives includes a “Signature” feature that provides users with the ability to electronically sign any Page in a Notebook. LabArchives records the name of the signer (using their LabArchives credentials), as well as the date and time using a trusted third party (National Institute of Standards and Technology). Only certain users are authorized to sign. At present, there is a single meaning for a signature; if required, LabArchives can be adapted to include other meanings, including review, approval, responsibility and/or authorship.

---

**Sec. 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.

LabArchives’ Response: Signatures in LabArchives are, by nature, electronic. They are, therefore, irrevocably linked to the Page(s) that have been signed. Signatures, once executed, cannot be excised, copy, or transferred.

Subpart C--Electronic Signatures
Sec. 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.

LabArchives’ Response: LabArchives will not allow two users to use the same identification, rendering signatures unique. Management of the company must adopt a policy of forbidding user names from being reassigned.

(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.

LabArchives’ Response: This should be company policy.

(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), 12420 Parklawn Drive, RM 3007 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.

LabArchives’ Response: Organizations that must comply with 21 CFR Part 11 must submit a certification to the FDA.

Sec. 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.

LabArchives’ Response: At present, LabArchives does not directly support any biometric devices, although many such tools can function independently of the LabArchives platform. For example, a fingerprint reader can be used as the login mechanism for the user name and password.

To log in to LabArchives, the user must have both an authorized name and password.

Sec. 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.

LabArchives’ Response: LabArchives does not allow two users to have the same identification code. The unique “key” for LabArchives is the e-mail address.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). This is b, not c

**LabArchives’ Response:** LabArchives does not require regular password changes; this should be instituted as an organization policy.

(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. This is c, not d

**LabArchives’ Response:** This paragraph relates to access devices and is outside the scope of LabArchives.

(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. This is d, not e

**LabArchives’ Response:** LabArchives includes certain security features that prevent unauthorized break in attempts through “phishing” by “locking out” users that incorrectly attempt to log in multiple times. Additionally, by capturing the IP address of each user, system administrators can use this as an additional method to detect unauthorized use.

(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.

**LabArchives’ Response:** This should be company policy.