Labstep for 21 CFR Part 11 Compliance

Title 21 CFR Part 11 of the Code of Federal Regulations contains the regulations concerning electronic records and electronic signatures as formulated by the US Food and Drug Administration (FDA).

Since the compliant adherence to 21 CFR Part 11 is not only dependent on the software system, but also on procedural controls (e.g. document control, SOPs, training etc.) within an organization which uses electronic records, a software cannot be certified to be compliant (and any software vendor claiming a 21 CFR Part 11-compliance is incorrect!). It is, however, possible for software vendors to offer a system which meets the technical requirements for electronic records set by the FDA in a compliant set-up.

This document gives a brief overview of technical features which fulfill the requirements of 21 CFR Part 11 and facilitate its implementation within an organization. This document does not give detailed information on 21 CFR Part 11, nor does it provide legal advice for full compliance.

The full text of 21 CFR Part 11 can be found on the FDA website:

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11

The following outline below summarizes the sections of the 21 CFR part 11 regulations which are relevant to electronic systems, also pointing out the Labstep implementation to meet these technical requirements.

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:

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

Labstep implementation: According to the FDA classification above, Labstep is a closed system because the use of the electronic lab notebook requires a login and password which are both unique to the Labstep-system.

- **Confidentiality**: All records are by default only available to the authors, and authors can share them with other users within the closed system. Sharing rules and access rights can be set up within an organization to further increase confidentiality.
- **Authenticity**: All records have only one unique/original author that cannot be changed during the entire lifecycle of a document
- **Integrity**: Every single record as well as changes to a record are tracked in a full audit trail and obtain a timestamp provided by the server-system which cannot be manipulated by users. The deletion of documents is possible after authorization, and can be further controlled by organizational policy.

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 copy of the electronic records.

- Labstep implementation: Access to records in the closed system can be granted to any individual or organization, and PDFs of records can be exported anytime. In both implementations, third parties can review records, authors, time stamps, audit trails and electronic signatures.

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

- Labstep implementation: In the cloud version, records are stored for three years beyond the subscription period unless explicitly being deleted by the user. Thus, Labstep complies with the standard “records retention period” of 21 CFR Part 11. On local server installations, retrieval throughout the records retention period is within the responsibility of the hosting organization.

Limiting system access to authorized individuals

- Labstep implementation: Access to Labstep requires authentication via a unique username and password. Access to records can be controlled, granted and revoked anytime by the organization which controls and owns these records.

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.

- Labstep implementation: All records and record changes are provided with a system-created time-stamp and recorded in an activity log which cannot be manipulated by any user of Labstep. Deletion of records can be controlled and prohibited by organizational access rights and permissions.

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate

- Labstep implementation: If an organization requires the sequence check of steps and events, they can implement these using steps in their protocols in Labstep, as well as completing entire protocols in the workflow overview of an experiment record.

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

- Labstep implementation: Additional to the login, every user can be assigned administrative roles within an organization. Read/edit access to records as well as the possibility to sign can be managed for every member of the organization individually, allowing to enforce authority checks even within nested and branched organizational structures.

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

- Labstep implementation: A login is required from every device from which records are accessed and IP addresses of the device are stored for every session.

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks

- Labstep implementation: The Labstep product development team is well trained on the field of software design, implementation of cryptographic methods and regulations. Labstep team members who are not familiar with the system and the requirements are being provided with manuals and training.

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.

- This feature is beyond the scope of the software system provided by Labstep and falls under the responsibility of the user. However, Labstep can provide guidelines and training to ensure compliance.

Use of appropriate controls over systems documentation including:

- Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
- Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Section 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.

Labstep implementation: This section does not apply to Labstep because Labstep is a 'closed system' according to FDA definition.

Section 11.50 Signature Manifestations

Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- **The printed name of the signer;**
- **The date and time when the signature was executed;**
- **The meaning (such as review, approval, responsibility, or authorship) associated with the signature**

Labstep implementation: Labstep provides a digital signature which indicates the printed name of the signer, a time-stamp for the signature and the meaning of the signature.

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).

- Labstep implementation: Digital signatures in Labstep as well as their authors and time-stamps are forever recorded in the activity log and can only be altered by persons with the appropriate authority. Digital signatures are displayed in the review section of each experiment entry, and are exported as well during a PDF export.

Section 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.

- Labstep implementation: By being electronically linked to each record, electronic signatures in Labstep can not be excised, copied or transferred to another record.

Subpart C - Electronic Signatures
Section 11.100 General requirements

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

- Labstep implementation: Any combination of username and password in Labstep is unique. Since electronic signatures are linked to the username/password combination, they can be used only by one individual per signature.

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.

- Labstep implementation: Organizations can enforce Two Factor Authentication for all Electronic Signatures. If enabled users will be asked to enter an authentication code before being able to sign.

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.

- **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.**
- **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.**
- The submission of certifications to the FDA is beyond the scope of the software system provided by Labstep and falls under the responsibility of the user.

Section 11.200 Electronic signature components and controls

Electronic signatures that are not based upon biometrics shall:

- **Employ at least two distinct identification components such as an identification code and password.**
- **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.**
- **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.**
- **Be used only by their genuine owners;**
- **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**

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

- Labstep implementation: The first check whether a signature is executed by the authorized individual is provided by the system-login, which is unique for each individual user of Labstep. The second check is at the point of signing and is implemented using the Time-based One-time Password Algorithm linked to a specific device held by the user. (Note: Organizations must enable the Two-Factor Authentication feature to enforce this second check).

Section 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:

Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

- Labstep implementation: The user name/password combination which is required to authenticate to the system is unique for each individual user of Labstep.

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.

- This feature is beyond the scope of the software system provided by Labstep. A regular password change has to be governed by organizational policies.

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 feature is beyond the scope of the software system provided by Labstep. Labstep does not natively require access tokens, but can provide consulting on how to implement token safeguards.

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.

- Labstep implementation: Labstep has implemented security features that report suspicious behaviour. Unauthorized use can further be detected and prevented by monitoring and restricting IP addresses for system access.

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.

- This feature is beyond the scope of the software system provided by Labstep. However, Labstep can provide guidelines and training to ensure compliance.