TECHNICAL OVERVIEW

Eusoft.Lab LIMS & FDA CFR 21 Part 11

-

How Eusoft.Lab LIMS facilitates
the compliance to FDA Title 21 CFR Part 11

eusoft
more than a LIMS

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).

This document gives a brief overview of technical features of Eusoft.Lab as cloud-based LIMS Software as a Service (SaaS) which fulfils the requirements of 21 CFR Part 11 and facilitate its implementation within an organization.

21 CFR Part 11 Subpart B - Electronic Records

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

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Altered Record Detection	If records can be altered by tools outside the System, the System shall detect and trace all the actions performed on records by pre-authorized operators (even at the highest level of access, such as System Administrator).	Eusoft.Lab database are not reachable as per Microsoft Azure logical security features. [1]
Invalid Record Detection	The system must be able to detect invalid records (such as invalid fields left blank that should contain data, values outside of limits, ASCII characters in numeric-only fields, and incorrect file formats, etc.).	Eusoft.Lab validates each single input data in accordance with predefined rules. The system notices the user with dedicated alert/warning messages.

[1] **For On Premise installation:** The Business Owner and Customer IT department are responsible for the logical security of the data.

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.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Record Inspectability	The System allows to generate accurate and complete copies of electronic record in both human readable printouts and standard electronic format (e.g. PDF, MS Word, MS Excel, etc.) suitable for inspection, review and copying by the Regulatory agency.	Reports are available in every application functionality for each Electronic Record. Eusoft.Lab can export data in different standard electronic formats (PDF, RTF, CSV, MS Excel, etc.).

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

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Backup	Regular backups of all relevant data should be done. Backup data should be stored in a separate and secure location. Integrity and accuracy of backup data should be checked during or on completion of the backup process.	Microsoft Azure Cloud backup technology automatically creates full backups every week, differential backups every 12 hours and transaction log backups every 5-10 minutes. See Microsoft Azure GxP Guidelines (July 2020) for full Microsoft references.(2)
Restore	The availability to restore the data should be checked during the validation and monitored periodically.	Eusoft plans, tests and documents the own Restore procedure in the Business Continuity Protocol. The restore policies and procedures in place for Microsoft Azure are detailed in Microsoft Azure Procedures as per Microsoft Azure GxP Guidelines (July 2020). (2)
Data Retention	Data should be secured by both physical and electronic means against damage. The System shall allow to store electronic records to enable their accurate and ready retrieval throughout the records retention period.	The Customer is responsible for determining the recordkeeping requirements based on internal policies and regulatory requirements. Data Retention topic managed by Microsoft is detailed in section 3.2.10 “Data retention” of Microsoft Azure GxP Guidelines (July 2020).(3)
Archiving	In case the data are archived offline (i.e. not immediately available to users), data shall be periodically checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	Data Archiving can be managed by Eusoft Technical team. The Historical data can be retrieved by a read only instance in Eusoft.Lab.

(2) **For On Premise installation:** The Customer is responsible for the Backup and restore processes which will be verified during the Validation activities.

(3) **For On Premise installation:** The customer must put in place dedicated procedures to address the Data Retention process in accordance with a dedicated Risk Assessment.

11.10(d) Limiting system access to authorized individuals.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Access Control	The System shall restrict logical access to pre-authorized users.	Eusoft.Lab manages different access criteria like: • Local user set directly in LIMS, using the username assigned by the administrator and the password chosen by the operator; • Using company Active Directory users and rules.

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 that required for the subject electronic records and shall be available for agency review and copying.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Audit Trail	The system shall ensure the irrefutable recording of the identity of operators entering or confirming data through the Audit trail, which shall record all actions that create, change or delete electronic records with relative metadata. Audit trail shall be created automatically by the System without any user action. Audit trail shall include time and date relative to the action performed on the record. The alteration to data shall permit the reading of the original information, i.e. audit trail shall not overwrite record changes on previously stored information. In case the reason of change or deletion of GMP-relevant data is required to be documented, the System shall force user to enter reason.	All the activities performed within the Eusoft.Lab system are stored in a system log, which keeps track of: • Date and time of the transaction; • Operator who performed the operation; • Description of the operation carried out; • Information on the data preceding the change; • The system log is also subject or access verification, only allowed for specifically enabled users. The system log functionality provides reports to copy the audit train in a standard form. The information logged in the audit trail cannot be deleted or changed by any user.
Temporal Reference	Temporal reference shall be equal for all users, otherwise The System shall automatically synchronize all workstations. Temporal reference cannot be changed by the user.	Eusoft.Lab is a web application so all temporal references are managed by the application server and cannot be changed by the users.

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

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Operational Check	The System must have operational checks in order to enforce permitted sequencing of steps and events, by allowing the execution of one step only after the execution of the previous one.	The entire life cycle of Electronic Record managed by Eusoft.Lab is governed by specific workflow predefined and configurable in the system. Unauthorized actions are not permitted and reported to the users.

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.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Authority Check	The System must restrict use of the function according to pre-configured user profiles that are maintained. Any changes to the roles should be authorized and tracked.	The segregation of duties is managed by a dedicated user and profile module in Eusoft.Lab Roles and privileges modification is permitted only to the users granted by the assigned roles. Any change to the roles is recorded in audit trail.
Automatic Log Off	The System shall include a log off mechanism after a pre-defined period of user inactivity, or a mechanism where user ID entry is required after inactivity period. This feature must not be modifiable by users.	Eusoft.Lab manages the session expiration and requires the user credential to log on again.

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.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Device Check	Device checks are procedures implemented to verify the validity and reliability of data input sources or operational instruction in electronic systems.	Eusoft.Lab in Cloud as SaaS doesn't need any terminal. In case data is acquired by external source (e.g. from instrument), the system validates each acquisition.

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.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Signer Information	Signed electronic record shall contain the printed name (name and surname) of the signer.	Eusoft.Lab database stores the printed name of each signer.
Time Stamp	Signed electronic record shall contain the date and time when the signature was executed.	Eusoft.Lab keep track of date and time of the electronic signature.
Signature Meaning	Signed electronic record shall contain the meaning of the signature.	Eusoft.Lab keeps track of the meaning (reason) of the signature. The meaning of the signature is given by the functionality used: • when a user registers a sample, Eusoft.Lab automatically put the electronic signature as SampleUserAcceptance; • when an analyst saves the result of a test, Eusoft.Lab automatically put the electronic signature as SampleTestExecutor; • when a user supervises a sample Eusoft.Lab automatically put the electronic signature as SampleSupervisor. The functionality can be configured to meet user needs.

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).

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Display & Print Evidence	Printed copies of electronically compiled and electronically signed documents should be traceable via printed links to the original electronic transaction.	The Electronic Signature, Signature meaning and time stamp can be showed in each report set to report e signature information.

11.70 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.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Signature Record linking	The System shall prevent from signatures deleting, copying or transferring through system or external functions at any ordinary means.	Eusoft.Lab links electronic signature to the respective electronic record. Each change to the electronic record is managed as a revision with the respective electronic signature.

21 CFR Part 11 Subpart C - Electronic Signatures

Sections:

- 11.100 General Requirements;
- 11.200 Electronic signature components and controls;
- 11.300 Control for identification code/passwords.

TOPIC	DESCRIPTION	EUSOFT.LAB TOPIC MANAGEMENT
Signature Management	A procedure shall be defined where electronic signatures assignment and removal are rigorously managed.	Electronic signature removal is not permitted. Each modification of the electronic record is recoded in Audit Trail.
Unique Electronic Signature	The System shall ensure that each electronic signature shall be unique to one individual and shall not be re-used by, or re-assigned to anyone else.	Electronic signature is managed by Eusoft.Lab internal unique user id (not the username). This ID is automatically calculated and cannot be re-used or re-assigned.
Single Step Singing Modality	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.	Electronic signature can be applied to multiple records. Eusoft.Lab record the same signature details to all record at the same time.

eusoft

more than a lims

FIND OUT WHAT WE CAN DO FOR YOU