Agaram TECHNOLOGIES

How Logilab SDMS helps Laboratories to enable 21 CFR Part 11 Compliance

White Paper

Part 3

V. Raghavan

Agaram Technologies Private Limited

12 – Dec - 2020

TABLE OF CONTENTS

Logilab SDMS solution for 21 CFR Part 11 Compliance requirements

Nature of Logilab SDMS and its applicability for 21 CFR Part 11

Logilab SDMS is a closed system. 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.

Hence the following subparts are applicable.

SUBPART B – ELECTRONIC RECORDS §11.10 CONTROLS FOR CLOSED SYSTEMS

SUBPART B – ELECTRONIC RECORDS §11.30 CONTROLS FOR CLOSED SYSTEMS

SUBPART B – ELECTRONIC RECORDS §11.50 SIGNATURE MANIFESTATIONS

SUBPART B – ELECTRONIC RECORDS §11.70 SIGNATURE/RECORD LINKING

SUBPART C – ELECTRONIC SIGNATURES §11.100 GENERAL REQUIREMENTS

SUBPART C – ELECTRONIC SIGNATURES §11.200 ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS

SUBPART C – ELECTRONIC SIGNATURES §11.300 CONTROLS FOR IDENTIFICATION CODES/PASSWORDS

Let us see one-by-one in the next few pages.

1. Subpart B – Electronic Records §11.10 Controls for Closed Systems

Section: §11.10 (a)

Section Requirements:

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

Logilab SDMS Approach:

Product is tested and released for customers. It is also validated against operational qualification tests which are performed during implementation with relevant documentation to justify the same. The product can discern invalid and altered records by the automatic versioning.

Section: §11.10(b)

Section Requirements:

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.

Logilab SDMS Approach

Data can be downloaded for copying, reviewing and printing by users with appropriate privileges. The original data will reside within the system in electronic format for any verification.

Section: §11.10(c)

Section Requirements:

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

Logilab SDMS Approach

Data within the system is protected from un-authorized access or modification by applying security and access control measures. Data or records within the system can be accurately retrieved throughout the records retention period

Section: §11.10(d)

Section Requirements:

Limiting system access to authorized individuals.

Logilab SDMS Approach

Logilab SDMS system is only accessible through valid “username” and “password” which gives access to only authorized users.

Section: §11.10(e)

Section Requirements:

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 of at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Logilab SDMS Approach

System generates audit trail of user(s) login, log-off, user actions that create, edit, (records cannot be deleted in Logilab SDMS). System audit trails are automatic and cannot be intervened or modified by users. User audit trails are available at relevant areas of application that authenticates the action by way of requesting a user name, password, pre-defined reason and a comment. The audit trail records consist of user name, Logilab client ID, action performed, change in data if any along with server date/time stamp. The audit trail is a non-editable, searchable, printable, and exportable for review. Since no data can be deleted within the system and the system has a built-in versioning capability, old or previous versions of data does not get obscured.

Section: §11.10(f)

Section Requirements:

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

Logilab SDMS Approach

System has validations in place that allows only valid sequence of operations can be performed. Also, there is no sequence or operation available within the system to modify any electronic records after it has been captured.

Section: §11.10(g)

Section Requirements:

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.

Logilab SDMS Approach

Anonymous access to the system is not allowed. Only authorized user can access the system, provide input and perform operations. No record can be altered after capture.

Section: §11.10(h)

Section Requirements:

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

Logilab SDMS Approach

System works in automated fashion to fetch data generated by instruments and it checks for source of data and its validity before being uploaded to server. Any change in source data like creation, editing, deleting is detected by the system and audit trailed.

Section: §11.10(i)

Section Requirements:

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

Logilab SDMS Approach

Logilab administrators and end-users are adequately trained to use the system for the intended purpose. Since Logilab SDMS is an automated system, end-user simply does not need to have any special skills to use the system, other than login to the system and view the data captured.

Section: §11.10(j)

Section Requirements:

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.

Logilab SDMS Approach

Whenever electronic signatures are to be executed, system prompts for user name, password, pre-defined reason, comments. This mandatory process conveys the literal meaning. The implications of the action about to be taken are also displayed such that it takes cognizance of the person performing such action.

Section: §11.10(k)(1)

Section Requirements:

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.

Logilab SDMS Approach

System related documentation (guides) which are provided along with the product. It is the responsibility of the user organization to develop policies as well as Standard Operating Procedures (SOP) regarding controlled access to system, user and manuals.

Section: §11.10(k)(2)

Section Requirements:

Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Logilab SDMS Approach

System documentations are version controlled and the document history will be maintained in each of the system document. The Release notes will have all the details of the released product version.

2 Subpart B – Electronic Records §11.30 Controls for Closed Systems

Section: §11.30

Section Requirements:

Controls for Open Systems

Logilab SDMS Approach

Logilab SDMS is a closed system

3 Subpart B – Electronic Records §11.50 Signature Manifestations

Section: §11.50(a)(13)

Section Requirements:

Signed electronic records shall contain information associated with the signing that clearly indicates all 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.

Logilab SDMS Approach

System documentations are version controlled and the document history will be maintained in each of the system document. The Release notes will have all the details of the released product version.

Section: §11.50(b)

Section Requirements:

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).

Logilab SDMS Approach

Whenever an E-signature is applied to an electronic record, it appears as an electronically signed as part of the electronic record in the user display.

4 Subpart B – Electronic Records §11.70 Signature / Record Linking

Section: §11.70

Section Requirements:

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.

Logilab SDMS Approach

Logilab SDMS does not have any provision to remove or modify an e-signature applied to an electronic record. It is always linked to specific record on which the signature was applied.

5 Subpart C – Electronic Signatures §11.100 General Requirements

Section: §11.100(a)

Section Requirements:

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

Logilab SDMS Approach

Each individual in the organization will have their unique user ID and password, which cannot be reused or reassigned to any other user.

Section: §11.100(b)

Section Requirements:

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.

Logilab SDMS Approach

This activity is beyond the scope of Agaram's Project Implementation. It is the responsibility of the organization to establish policies and procedures to verify the identity of the individuals who are authorized to use the electronic signature.

Section: §11.100(c), §11.100(c)(1), §11.100(c)(2)

Section Requirements:

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), 5600 Fishers Lane, 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.

Logilab SDMS Approach

Each organization is required to notify the FDA in writing of their intention to use electronic signatures. It is the responsibility of the organization to perform this notification.

6 Subpart C – Electronic Signatures §11.200 Electronic Signature Components and Controls

Section: §11.200(a)(1)

Section Requirements:

Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

Logilab SDMS Approach

Every user is verified based on 2 different distinct components (1) username and (2) password before the user can apply a e-signature for the electronic record in Logilab SDMS.

Section: §11.200(a)(1)(ii)

Section Requirements:

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.

Logilab SDMS Approach

For every e-signature applied the user has to enter all the signature components within Logilab SDMS system.

Section: §11.200(a)(2)

Section Requirements:

Electronic signatures that are not based upon biometrics shall: Be used only by their genuine owners; and

Logilab SDMS Approach

User with valid username and password only can access the system and apply e-signature.

Section: §11.200(a)(3)

Section Requirements:

Electronic signatures that are not based upon biometrics shall: 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.

Logilab SDMS Approach

It is the sole responsibility of the organizations to instruct all the employees to adhere to the process of using their own credentials and not to use others in a strict manner. This cannot be enforced by the Logilab SDMS if passwords are shared by individual users. However, when such attempts are made with mistakes will be audit trailed by the system.
Section: §11.200(b)

Section Requirements:

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

Logilab SDMS Approach

Biometrics is not used by the system

7 Subpart C – Electronic Signatures §11.300 Controls for Identification Codes/Passwords

Section: §11.300(a)

Section Requirements:

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.

Logilab SDMS Approach

System allows only unique combinations of user name and password. No two users can have either the user name or password as the same.

Section: §11.300(b)

Section Requirements:

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

Logilab SDMS Approach

Option to setup Password ageing is available under Logilab SDMS password policies.

Section: §11.300(c)

Section Requirements:

Following loss management procedures to electronically de-authorize 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.

Logilab SDMS Approach

When loss of password or compromise is reported, such user's passwords can be reset by the administrator. In the event of employees leaving the organization their user accounts can be retired. Also, temporary de-activation and activation of specific users is possible.

Section: §11.300(d)

Section Requirements:

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.

Logilab SDMS Approach

System is fully integrated with security policies that prevent any form of undetected or unauthorized access to the application. Any such attempt is audit trailed and such user's accounts are automatically locked after a preset failed number of attempts.

Section: §11.300(e)

Section Requirements:

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.

Logilab SDMS Approach

This is not applicable as there are no devices that bear or generate identification code or password information.

In **Part 1**, we have understood the fundamental concepts of 21 CFR Part 11 and its principles as applicable to Computerized systems

In **Part 2**, we have understood the overview of Logilab SDMS and its importance in 21 CFR Part 11 as applicable to Computerized systems

In **Part 3**, we looked into how Logilab SDMS fulfils the requirements of 21 CFR Part 11.

(Concluded)