21 CFR Part 11 Mapping

Checklist

This matrix is a nexus of 21 CFR Part 11's clauses and Scilife expertise. As a leading SaaS platform, Scilife's QMS harmonizes seamlessly with these mandates, guiding your digital transformation path. This matrix unveils alignment and synergy, where regulations find their match in Scilife's functionalities.

21 CFR Part 11 governs the FDA regulations for electronic signatures and electronic documents. It defines the rules under which electronic records and electronic signatures are trustworthy, reliable, and comply with data integrity principles. It applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted.

Scilife Supporting science. Improving life.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
Subpart B--Electronic Records - Sec. 11.10 Controls for closed systems				
1	11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes	Validation of systems is done as per defined procedure and individual plans are developed for each module.
2	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.	Yes	Scilife application generates accurate and completed copies of records both in human readable and electronic format.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
3	11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Yes	Records are maintained till retention period. Only authorized users can have access to records.
4	11.10 (d)	Limiting system access to authorized individuals.	Yes	Scilife application access is user ID and password controlled. Additional Multi-Factor Authentication (MFA) is also available. Access to system functionality is governed through user access levels.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
5	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.	Yes	Audit trail is available in the application which records all operator entries with user name, date, time and action performed. All record changes in the application are version controlled and the audit trail is 'view only'. Audit trails are retained and are available for review and copy.
6	11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Yes	Application uses operation system checks to enforce sequencing or flow of steps.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
7	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.	Yes	Only authorized users can login into the system using user ID and password. Additionally MFA authentication can be configured.
8	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.	NA	NA
9	11.10 (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.	Yes	Training management procedures are available and training records are maintained. Training module is used for this purpose.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
10	11.10 (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.	Yes	Data and control related procedures and policies are available.
11	11.10 (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.	Yes	Procedural controls are available.
Sec. 11.50 Signature manifestations				

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
12	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.	Yes	System asks for electronic signature for creation, modification or confirmation of records as per module configurations. Each executed electronic signature contains the printed name of the signer, date and time of signature and meaning of the signature.
13	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).	Yes	Electronic signatures are subject to the same controls as electronic records.
Sec. 11.70 Signature/record linking				

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
14	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.	Yes	Electronic signatures are implemented such that signatures cannot be excised, copied or transferred to falsify an electronic record by ordinary means.
Subpart C--Electronic Signatures - Sec. 11.100 General requirements				
15	11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Yes	Electronic signatures are unique to individuals, duplicate credentials cannot be created.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
16	11.100 (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.	Yes	Procedure control is in place.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
17	11.100 (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 signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement. (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.	NA	Usage of Scilife platform by Scilife is to manage internal activities, documentation and their respective e-signatures. The platform is not used to handle, process or submit any GxP data and hence this clause is not applicable for Scilife. However, whenever e-signature is performed a warning message “Be aware that you are now signing an electronic record which is equivalent to a handwritten signature.” is displayed to the users.
Subpart C--Electronic Signatures - Sec. 11.200 Electronic signature components and controls				

18	11.200 (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.	Yes	Electronic signatures consist of two different components i.e. user ID and password for initial signing. For subsequent signing in a continuous session, the system only asks for the password component of the signature. For non-continuous sessions, the system asks for both user ID and password for signing.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
19	11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Yes	Electronic signatures are unique to individuals.
Subpart C--Electronic Signatures - Sec. 11.300 Controls for identification codes/passwords				
20	11.300 (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.	Yes	Electronic signatures are unique to individuals.
21	11.300 (b)	Ensuring that identification codes and passwords are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Yes	Application has configurable password expiry setting, which enforces users to change password when password age has been reached.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
22	11.300 (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.	NA	Tokens, cards or other devices are not used for authorization.
23	11.300 (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.	NA	Unauthorized login attempts are only captured in system logs.

ITEM # & CFR REF.		DESCRIPTION	YES / NO / NA	EXPLANATION
24	11.300 (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.	NA	Tokens, cards or other devices are not used for authorization.