SENAITE LIMS v1.3.2

21 CFR Part 11 Compliance GAP Analysis

2019.10.01

TABLE OF CONTENTS

1. Purpose of this document

The purpose of this document is to guide LIMS developers and implementers through the FDA's 21 CFR Part 11 for lab systems.

Unless otherwise indicated, texts were sourced from US Food and Drug Administration (FDA) in the U.S. Department of Health & Human Services.

This document is a reviewed version of the document publicly posted at bika user's list in September 2014, initially compiled by Perry W. Burton and updated later by Jordi Puiggené[1] .

2. Definitions

21 CFR Part 11	United States Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records. The governing rules and guidance to persons who, in fulfilment of a requirement in a statute or another part of FDA's regulations to maintain records or submit information to FDA, have chosen to maintain the records or submit designated information electronically and, as a result, have become subject to part 11.

1 https://sourceforge.net/p/bika/mailman/attachment/540DDD89.3080706%40bikalabs.com/2/

Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations.

Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act (the PHS Act), even if such records are not specifically identified in Agency regulations (§ 11.1).

The underlying requirements set forth in the Act, PHS Act, and FDA regulations (other than part 11) are referred to in this guidance document as predicate rules.

Electronic Records

Electronic records are "any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system".

Under a narrow interpretation, the FDA considers part 11 to be applicable to the following records or signatures in electronic format (part 11 records or signatures):

Records that are required to be maintained under predicate rule requirements and that are maintained in electronic format in place of paper format.

On the other hand, records (and any associated signatures) that are not required to be retained under predicate rules, but that are nonetheless maintained in electronic format, are not part 11 records.

The agency recommends that a company determine based on the predicate rules; whether specific records are part 11 records and recommends that a company document such decisions.

Records that are required to be maintained under predicate rules, that are maintained in electronic format in addition to paper format, and that are relied on to perform regulated activities.

In some cases, actual business practices may dictate whether you are using electronic records instead of paper records under § 11.2(a).

For example, if a record is required to be maintained under a predicate rule and you use a computer to generate a paper printout of the electronic records, but you nonetheless rely on the electronic record to perform regulated activities, the Agency may consider you to be using the electronic record instead of the paper record.

That is, the Agency may take your business practices into account in determining whether part 11 applies.

Accordingly, the agency recommends that, for each record required to be maintained under predicate rules, you determine in advance whether you plan to rely on the electronic record or paper record to perform regulated activities.

We recommend that you document this decision (e.g., in a Standard Operating Procedure (SOP), or specification document).

Records submitted to FDA, under predicate rules (even if such records are not specifically identified in Agency regulations) in electronic format (assuming the records have been identified in docket number 92S-0251 as the types of submissions the Agency accepts in electronic format).

However, a record that is not itself submitted, but is used in generating a submission, is not a part 11 record unless it is otherwise required to be maintained under a predicate rule and it is maintained in electronic format.

Electronic

Electronic signatures that are intended to be the equivalent of handwritten signatures,

Signature	initials, and other general signings required by predicate rules. Part 11 signatures include electronic signatures that are used, for example, to document the fact that certain events or actions Occurred in accordance with the predicate rule (e.g. approved, reviewed, and verified). An electronic signature is "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature".
Digital signature	A digital signature is "an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified". Digital signatures are required for open systems and as such need higher security levels. Therefore, in addition to electronic signatures, cryptographic methods have to be applied for authentication of the user and integrity of the record.
Biometrics	Biometrics is "a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable". Examples of biometrics include facial recognition, voice recognition and fingerprint scanners. Most of them need specific hardware and software. The biggest problem with such devices is validating that they work reliably for the specified user but not for anyone else.
Audit Trail	A record of events related to a transaction including the original information and any changes to the information used to reconstruct a series of related events that have occurred. It may be composed of manual or computerized records of events and information, or both.
Closed System	A closed system is defined as an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Open System	An open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system. Practically all systems in analytical laboratories are closed systems. With an appropriate security system in place, the laboratory has full control on who will access the system. An open system in a laboratory would be one where the data is stored on a server that is under the control of a 3rd party. Other examples for open systems are websites where everyone has access.
Hybrid systems	Hybrid systems are a combination of electronic records and paper records. They are common systems in analytical laboratories today. Raw data are recorded electronically to reconstruct the analysis but the final results are printed and signed on paper. The FDA does not prohibit hybrid systems but has expressed some concerns about their acceptability.
Meta data	Meta data is important for reconstructing a final report from raw data. In chromatography it includes integration parameters and calibration tables.

Predicate rule Predicate rule as referred in 21 CFR Part 11 are the 21 CFR Food and Drugs regulations (besides 21 CFR Part 11). They are basically promulgated under the authority of the Food, Drug and Cosmetic Act or under the authority of the Public Health Service Act.

3. 21 CFR Part 11 Requirements

SENAITE LIMS complies

Partially compliant or requires customization

Inconsistencies or “Not applicable”

3.1. Electronic Signatures

UR #	Requirement	Comment
UR-1	Electronic signatures must be unique to each individual. Each user must have a unique Full Name. Each user must have a unique user id.	Every single user with access to the system have a unique ID. The system has the ability to prevent an inactivated (not deleted) user id from being reused. **Proposal**: add a validator for user first name and second name fields to ensure each user have a unique Full Name.
UR-2	The system must verify that an individual has the authority to electronically sign a record before allowing them to do so.	Only authorized users have system access. They can only do the actions (creation, modification, transitions) against electronic records based on the roles and groups they belong to. All transitions are logged with a timestamp and the unique user id who performed that action.
UR-3	The system will not allow electronic signatures to be reused or reassigned to anyone other than the original owner.	Laboratory and Client users cannot be removed, rather cancelled. Thus, their unique information (user id and fingerprint) cannot be reused.
UR-4	The meaning of the signature (author, reviewer, or approver) must be displayed a. at the point of signing; b. on the human readable copy of the associated record (screen or printed; c. on the electronic copy of the associated record.	SENAITE displays the signature of verifiers (and lab managers if necessary) for the results contained on results report, with job title and contact details. Reviewing and Approving is a one-step operation in SENAITE, called Verification, and is carried out by users authorized as Verifier or Lab Manager. Clients get to see results on-line but they may also receive it per email etc. in a

UR #	Requirement	Comment
		follow-up Publication step carried out by Publisher or Lab manager users. a. A results report preview is displayed before being published, or saved to the database, and includes the signature and its key. b. The results report pdf and the printed version contains the meaning of the signature/s. c. PDF is stored as is, including signatures.
UR-5	Maintain electronic records and linked signatures for the life of the electronic record.	SENAITE always maintain the electronic records. Removal of electronic records is not allowed, rather their transition to a cancelled status. Transactions done to any given electronic record are always linked to the user responsible of that change, along with a time stamp and other relevant information. The transition of an electronic record to a pre-verified/pre-publish state is not possible. The record must be retracted/invalidated by the lab manager, after which a new fresh copy of that Analysis Request is generated and both Analysis Requests (Invalidated and Retest) are linked for traceability purposes. The 'retracted'/'invalidated' Analysis Request is not removed from the system, as well as all the information associated to it. The transition is recorded in the audit trail.
UR-6	Electronic signature shall be able to show the signer's full printed name, to show the time and date of execution.	Signatory full name and transition datetime are always displayed.
UR-7	Electronic signature are non-removable, non-modifiable and an integral part of the electronic records.	Refer to UR-4 and UR-5. Compliant
UR-8	At a minimum, Electronic signatures employ two distinct components e.g. user ID & password.	Username and password are needed for user authentication before being able to take any allowed action (based on the roles and groups it belongs to) within the system, involving the modification of electronic records.
UR-9	The system shall be able to require at least one electronic signature component to be re-applied during a series of signings in a single controlled session	For a specific results preview screen, more than one results report layout can be displayed. For each one, a different pdf will be generated. The signature of the current user will be embedded in all of them. **Proposal**: Always prompt for user password on report preview after the button Email/Save being pressed. The reports will only be

UR #	Requirement	Comment
		published / sent / recorded if the credentials are correct. This procedure is enough to prove proof of person identity and prevent unauthorized access/actions.
UR-10	The system shall be able to require all electronic signature components to be re-applied when a series of signings are not in a single controlled session.	**Proposal**: Prompt for password confirmation at every signing (proof of person identity). Refer to UR-9
UR-11	The System shall maintain an Electronic Signature activity log in the audit trail. The log shall track the history of all Electronic Signatures activities applied to each record. This should also include the any previously entered data in the event a record is reset, data re-entered and a signature reapplied and will not obliterate the journal of previously entered data.	SENAITE keeps track of edits done for every single electronic record anytime, storing the following information: Electronic Record version, modification date time, actor's user id and fullname, remote IP address, type of action performed and diff of changes.
UR-12	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.	SENAITE embeds digitalized handwritten signatures in results reports (pdf) by default. Results reports can be revoked, but the files generated are always stored and cannot be edited or removed. These files are always stored as BLOBs in the database, along with a time stamp and the user who generated them.
UR-13	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.	Theis requires the elaboration of a document procedure that can be verified and validated. Not applicable, but the document can be maintained with version control in SENAITE. **Proposal**: When a user logins for the first time to the system, the system displays the policy document and asks the user to adhere. The user will only be able to login if accepts.

3.2. Audit Trails

UR #	Requirement	Comment
UR-14	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.	The audit trail of any given electronic record can be accessed by adding '/log' at the end of the record's unique URL. All data can be retrieved in JSON format thanks to SENAITE's RESTFul API. Also, data can also be exported to CSV/Excel format easily. Only users with suitable privileges have access

UR #	Requirement	Comment
		to all this information.
UR-15	11.10(e) - Use of secure, computer generated, time-stamped audit trails with a source IP address to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record the changes that will not obscure previously recorded information. The audit trail is to be retained (archived) for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. “The system administrator should not be able to ‘switch off’ the audit trail function without higher authorisation. Recovery of the audit trail in human readable form from archived storage must also be possible. The system should be capable of detecting invalid electronic records prior to data access. The system must be capable of audit trailing all GMP data in such a way that the original value is not overwritten and the change is linked through time/date and user ID to the modifier.” Audit Trail additional information from 21 CFR Part 11 guidance states: "The Agency intends to exercise enforcement discretion regarding specific Part 11 requirements related to computer-generated, time-stamped audit trails (§ 11.10 (e), (k)(2) and any corresponding requirement in §11.30)". "Persons must still comply with all applicable predicate rule requirements related to documentation of, for example, date (e.g., § 58.130(e)), time, or sequencing of events, as well as any requirements for ensuring that changes to records do not obscure previous entries". "We recommend that you base your decision on whether to apply audit trails, or other appropriate measures, on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on product quality and safety and record integrity". "Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal	SENAITE keeps track of edits done for every single electronic record anytime, storing the following information: Electronic Record version, modification date time, actor's user id and fullname, remote IP address, type of action performed and diff of changes. SENAITE does not keep log of the accessions and pages visited during a user session, but the data can be recovered from NGINX and ZEO's log files (see below). Audit trail, as well as electronic records cannot be removed and are stored forever. Disabling the audit trail function cannot be done by the system administration, cause is managed at code-level. Unauthorized attempts to log into SENAITE and the pages visited by authenticated users, along with their IP addesses can be recovered from NGINX and ZEO log files. These logs are plain text files stored in the server itself. OS keeps track of all the activity done within the server and all this information is stored in .log files inside /var/log directory. All these files can only be accessed by the system administrator and are bound to the organization's System Infrastructure security and recovery policies Refer to UR-11 for compliance regarding to log of electronic records edits. **Proposal**: - Keep track of the pages visited by a logged in user within an active session. - For some transitions (e.g retractions, rejections, etc.) or edition of some fields, show a pop-up with a compulsory field for the user to enter the reason of the transition and keep track in the audit log.

UR #	Requirement	Comment
	operation". Audit trail is a requirement of some FDA predicate rules, for example 21 CFR Part 58 (GLP). Others don't specifically mention audit trail but require changes to data to be recorded, for example 21 CFR Part 211 (drug cGMP) states in Paragraph 194b: "Complete records shall be maintained of any modification of an established method employed in testing. Such records shall include the reason for the modification and data to verify that the modification produced results that are at least as accurate and reliable for the material being tested as the established method". If the audit trail is not generated by the computer it should be generated manually, as a minimum. A record's integrity is a basic requirement of regulations and users of computer systems must be able to demonstrate this, especially for critical records. #3 above mentions "other appropriate measures". This means you can use other techniques to demonstrate record integrity, for example to demonstrate file integrity through hash values. #4 is important as it talks about manual interaction with the system. It is difficult to demonstrate record integrity if users sit in front of a computer and can change data on the screen if there is no electronic audit trail. This becomes really critical if a change of such data can have an impact on critical records, for example, accuracy of product test results. In this case the system should have a built-in electronic audit trail and the function should be validated. This is one example where discretion would not be exercised "as explained in this guidance".	

3.3. Control and Identification and Password

UR #	Requirement	Comment
UR-16	Password use must expire after a predetermined length of time.	SENAITE: Password auto-expire feature. By default 90d OS: Adhere to security policies from organization's System Administration dept.
UR-17	The system must require the password to contain a combination of at least 6 characters with at least one letter and one number.	Plone's Password Strength add-on can be installed in SENAITE LIMS. https://plone.org/products/passwordstrength
UR-18	The system must prevent the reuse of the specified number of previous passwords	**Proposal**: Add a field in SENAITE Setup to set the max number of previous password reuses allowed. Add a validator including the above rule in the user's edit form.
UR-19	The system must force users to immediately change their passwords after initial issuance or after their passwords have been reset.	Standard SENAITE / Plone
UR-20	The system must allow the user to change their password if they feel it has been compromised.	Standard SENAITE / Plone
UR-21	User passwords can only be reset by the System Administrator after account has been locked out or user has forgotten their password.	Authorised user with admin privileges may set this to the default policy
UR-22	User's account must be locked out if three consecutive failed logon attempts occur.	Plone's Login Lockout add-on can be installed in SENAITE LIMS. https://plone.org/products/loginlockout/
UR-23	If account is locked out the system must send an account locked out message to the System Administrator immediately.	Plone's Login Lockout add-on. Refer to UR-22
UR-24	The system must use 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. Verification of users, Administrators, Application managers, 'super users', etc. and their access to various functionalities of the program will be validated. The administrator of the system should have the capability to add or delete access, or increase or decrease the level of functionality to the database for users.	Plone's LDAP add-on. https://plone.org/products/ploneldap SENAITE allows admin to define user groups, roles with different permissions. admin can even set specific permissions for every single electronic record and state.
UR-25	Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Standard SENAITE / Plone

3.4. Data Retention

UR #	Requirement	Comment
UR-26	The system data must be able to be periodically backed up	Plone's collective.recipe.backup add-on https://plone.org/products/collective.recipe.backup
UR-27	The system data must be able to be restored	Plone's collective.recipe.backup add-on https://plone.org/products/collective.recipe.backup
UR-28	The data files are protected against intentional or accidental modification or deletion. The protection of records to enable their accurate and ready retrieval throughout the records retention period. Restrict deletion of records to administrator access level. This deletion should be audit trailed and this should include backup. The system must be capable of secure backup & recovery to durable media.	Records cannot be deleted, only de-activated or cancelled. Database access, its eventual/accidental deletion, backups and restore procedures depends on the security policies established by the systems dept.
UR-29	Electronic records will need to be able to be restored at any time during the designated retention of the record	Apart from restoring incremental backups, individual records can be rolled back by authorized users, but not always be restored completely due to transition state and DB integrity constraints.
UR-30	The data files are written to a highly secure database, directory or to an unalterable media	Use of a Database with security. Zope DB is a highly secure database. The security of the directory and media used depends on the security policies established by the systems department.

3.5. Security

UR #	Requirement	Comment
UR-31	Security procedures and controls shall be designed and implemented to include: 1. System access shall be limited to authorized individuals. - (Physical access) 2. Operational system checks shall enforce the proper sequencing of steps in a process (as appropriate).	Requires of a documented procedure that can be verified and validated. Depends on the security policies established by the systems dept.
UR-32	Authority checks shall ensure that only authorized individuals can:	Requires of a documented procedure that can be verified and validated. Depends on the security

UR #	Requirement	Comment
	1. Use the system. (Logical access) 2. Access the operation or computer system input or output device. 3. Alter a record. 4. Perform the specified operation. Limiting system access to authorized individuals. System access through multi-tiered user access levels. Restrict access to various functions of the system to authorize individuals who have been assigned the appropriate permissions.	policies established by the systems dept. Standard SENAITE / Plone SENAITE itself applies authorization roles in-line with the corresponding user group's tasks data access requirements, e.g. clients, data clerks, samplers, analysts, verifiers, lab managers.
UR-33	Device or terminal checks shall determine validity of the source of input or operation (as appropriate).	Relies on user authentication, roles, groups and user-specific permissions the user is bound to.

3.6. Personnel Qualification

UR #	Requirement	Comment
UR-34	Determination that the following persons have the education, training, and experience to perform their assigned tasks: 1. Developer(s) of the computerized system. 2. Maintainer(s) of the computerized system. 3. User(s) of the computerized system. A determination is documented that people who develop, maintain, or use electronic record/electronic signature systems have the education, training and experience to perform their assigned tasks. Training of users of the system will be documented in individual training records, as well as their level of access.	This requires a documented procedure that can be verified and validated. This document must be bound to the security policies established by the organization's systems department. **Proposal**: Training of users and keep track of in individual training records requires the development of an HR and Skills Lab Management add-on. An integrate with 3d-party corporative software can also be considered.

3.7. System Documentation Controls

UR #	Requirement	Comment
UR-35	Establishment and use of appropriate controls over systems documentation including: 1. Adequate controls over the documentation for	Documented procedure that can be verified and validated. This document must be bound to the security policies established by the org's systems

UR #	Requirement	Comment
	system operation and maintenance, to include: a. Distribution of documentation. b. Access to documentation. c. Use of documentation.	department. Several add-ons are available for Plone 4.3.x (and thus, for SENAITE too), that offer full document management, version and granular access control.
UR-36	Revision and change control procedures to maintain an audit trail that documents the time-sequenced development and modification of the systems documentation.	Documented procedure that can be verified and validated. This document must be bound to the security policies established by the org's systems department. Several add-ons are available for Plone 4.3.x (and thus, for SENAITE too), that offer full document management, version and granular access control.

3.8. Control of System Management and Configuration

UR #	Requirement	Comments
UR-37	The system must be validated to cGMP and 21CFR Part 11 requirements prior to being put into use in a Production environment. Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records. The system should be capable of detecting invalid electronic records prior to data access. The system must be capable of audit trailing all GMP data in such a way that the original value is not overwritten and the change is linked through time/date and user ID to the modifier.	Documented procedure that can be verified and validated. **Proposal**: Validation of 21 CFR Part 11 requirements on test/pre-production instances before the deployment to production.
UR-38	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. The system will be constructed such that the next step in the workflow process will not be permitted until all the (minimum) required information is entered by the user. Similarly, if a follow-up has lapsed, the system administrator will be informed	A transitions workflow with constraints, e.g. user's authorisation, applies to all records. Moreover, every record has specific state-bound view/access/edit permissions of its own. Data entry validators are also applied to compulsory field and specific-data-type fields.