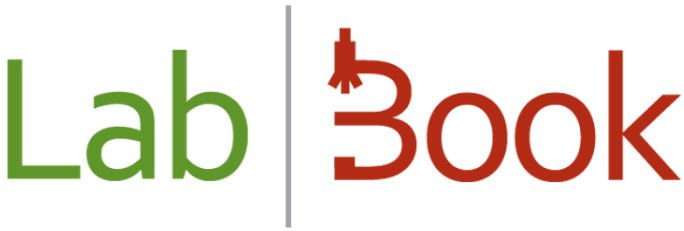
Technical guide for the development of a validation procedure for the SIL LabBook in medical laboratories



March 2023

Table of contents

1. Object

This document is intended for medical laboratories using the LabBook Laboratory Information System (LIS). It is a guide for setting up a software validation procedure by the laboratory according to the ISO15189 standard. This guide provides an approach that allows the laboratory to qualify the use of the LabBook tool and to ensure its appropriation in terms of control, maintenance and monitoring. The laboratory must also have a procedure for using the LIS, a procedure in degraded mode and a procedure for evaluating skills (which covers here the evaluation of the skills of teams on the management and use of the software).

It is recommended that you watch this training video on the Quality Initiative website: (in French)

https://www.initiative-qualite.org/webcast/comment-valider-un-logiciel-de-laboratoire/

The laboratory can define a map of the information systems that communicate with the LabBook software. This mapping allows you to highlight the interactions of the LabBook software with other laboratory software (middleware, PLC software, software external to the laboratory, etc.)

Finally, a risk analysis is highly recommended in terms of security.

2. Setting

a. Roles

The laboratory creates user accounts by assigning a role in the LabBook software. The access rights in the software are predefined. LabBook offers 10 different roles and each has specific rights: biologist, technician, advanced technician, quality technician, secretary, advanced secretary, prescriber, quality specialist and stock manager. The administrator role (root) is dedicated to the IT manager.

If the laboratory uses IT service providers to manage the software, they are considered as critical suppliers and must be subject to a confidentiality clause. A contract must also be established between the two parties involved.

b. Benchmark of analyses

The laboratory must check the settings of the analyses and dictionaries before using LabBook. Only the administrator and the biologist can perform this work within LabBook.

The analysis setup is a critical operation that should be checked and validated before the software is put into operation, focusing on the following elements:

- Code
- Designation
- Abbreviation
- Analysis family

- Type of sampling
- Export WHONET
- Wording
- Type of value
- Usual values
- Unit
- Formula if field calculated

All settings must be validated before being put into service. This validation must be recorded in the laboratory's documentation system with proof of the tests carried out (e.g. screen copies).

c. Dictionaries

In addition to analyses, checking the choice lists is an important task before the LIS is started. The dictionary is a collection of reference data needed to link variables to their possible value types. Several parameters can be linked to a single dictionary.

d. Reporting templates

The reports shall include, but not be limited to, the information specified in ISO 15189. In case of failure, the laboratory must edit the template and complete the missing elements. It can refer to the LabBook referent.

e. Validation tests

Validation tests must be performed before the software is put into production and after any changes to the repository, dictionary and report templates, software failure or software update.

It is recommended to make test patient files, this allows to check the transmission of data from the registration to the report of the result. We recommend one test file per analysis actually performed by the laboratory.

In this phase of data transmission, it is important to check rounding, reference values and units.

It is also important to validate internally the "cancel and replace" function which allows you to check the addition of the "cancel and replace" label with the date/time of modification on the corrected report.

The proper execution of the three validations available in LabBook must be controlled: administrative, technical and biological validation.

LabBook software offers the possibility of merging folders and deleting folders. These two functions must be validated internally before use.

All of these tests performed must be recorded within the quality management system (QMS) with associated evidence.

3. Access security

The laboratory must make its users aware of computer security. The definition of a user charter is recommended. In the work contracts or through a specific charter, each employee of the laboratory must be held to confidentiality when using the software. The laboratory must also make sure to prevent any fraudulent access to the software.

a. Organization chart

The laboratory shall put in place measures to organize IT responsibilities and clearance levels to ensure control. It appoints an IT manager and a deputy. These appointments may involve internal and/or external persons, for example the IT manager.

Duties and responsibilities must be precisely defined:

- Management of the analysis repository;
- User management
- Installation of updates
- Verification of backups
- Management of computer equipment (computer, printer, UPS, etc.)

b. Access to the LabBook server

It is essential to keep the LabBook server in a place with little traffic. In the absence of an air-conditioned room, the server must be placed in a room with low temperature. The server must be connected to an inverter to control its operation and to have a minimum autonomy. In a multi-station environment, it is advisable to check and fix the IP address of the server. Restarting the router or making changes to the equipment may cause the IP address to change and make the software inaccessible to users.

c. User tracking

Periodic monitoring must be defined according to the evolution of the computer equipment and the movement of personnel. A periodic verification of the users of the system must be carried out by the manager. Inactive user accounts must be deactivated from the system. A periodic change of passwords must be adopted by all.

d. Inactivity lockout time

In order to guarantee the accountability of actions to users, it is important to define a time limit for locking or disconnection on inactivity with a redirection to the connection page. In order to protect the data, to guarantee the security of the system and to ensure the traceability of the actions, the laboratory indicates in its IT security policy the locking methods:

- When leaving the workplace;
- According to a predefined time of inactivity ;
- In case of change of user.

4. Data security

The laboratory must develop a procedure to control the integrity of information, including data backup.

Data integrity tests must be performed at defined intervals, after software modifications and in case of failure (before restarting). These tests should ensure that the laboratory has data integrity, i.e., accuracy, readability, originality, completeness, durability, consistency, availability and noncorruption. The tests performed and associated evidence must be maintained in the laboratory's QMS.

a. Backup

Backup prevents loss of data in case of unauthorized access or failure. The person responsible must check regularly at a specified time to ensure that the backup has been carried out correctly.

- Type of backup

There is only one type of backup with LabBook: the total backup. It considers both the database files and the downloaded files.

- Backup media

Backups are made on a removable media connected to the LabBook server. This media allows you to restore the data in case of failure/destruction of the computer server. The backup is encrypted with a GPG key and secured with a password to avoid any risk of access to the data. It is important to remember to change the backup media when there is no more space or to copy the backups to another media and free up the space. It is recommended to copy the contents of the backup media to a location distant from the server (not in the same building), thus allowing the restoration of the data even after an event affecting the integrity of the laboratory itself).

- Backup frequency

The system performs regular automatic backups at a specified time. The laboratory defines the time when the system performs the automatic backup. Preferably a time is specified when the system is less used. Manual backups can be started at any time.

b. Catering

Data restoration allows you to restore the LabBook database to its state at a specific date and time. Restoration tests must be performed to verify the quality and effectiveness of the backup. The goal here is to check that after the restoration, the data is not corrupted. To do this, before and after restoration reports will be compared. This test should be documented and included in the laboratory's quality system.

See the LabBook restoration manual: https://www.lab-book.org/ressources

c. Update

New LabBook updates are published on the website www.lab-book.org and announced in the LinkedIn community: https://www.linkedin.com/groups/9052040/.

The laboratory regularly checks the availability of new updates and proceeds with the installation. The version used is mentioned at the bottom of the software pages.

Before an update, the person in charge must check that the last backup was correctly executed. In case of an update with software evolution, it is necessary to check the absence of non-retroactivity (in case of re-editing a result, the old reports must not be modified by the new software version).

After the upgrade, the software must be revalidated by making test files and documenting it in a report.

5. Management of a server failure

It is important to use a risk analysis to anticipate possible failures in order to minimize their impact.

Before a breakdown

- Write and distribute the procedure for operating in degraded mode.
- It is recommended that you have a computer (backup) with the required technical specifications on which LabBook is installed.
- Verify that the backups are running at the specified time. It is these backups that will allow the database to be restored. It is important to have regular and functional backups.
- Have an up-to-date version of LabBook.

In case of a breakdown

- Inform laboratory personnel of the incident and the implementation of the degraded procedure.
- Start the data recovery with the last available backup.
- Verify that the restoration process is running smoothly (number of files; list of users; display of results on the report).

After a breakdown

- Perform a validation test on this new version of the software.
- Configure the network and check the server access (if multi-station installation).
- Verify that the backups are running correctly on this new computer.

6. Staff training

All personnel using the LabBook software must be trained in its operation and use. In this sense, during the installation of the software, the future reference users of the system are trained. The term "user" must be taken in the broadest sense, including all secretaries, technicians, biologists and members of the IT department. At this level, the laboratory must plan to include training on LabBook in its staff training plan. Training is of course provided for new users, but also for old users when major versions of the software are updated. The traceability of these training sessions must be kept.

7. Patient traceability

The unique patient identifier is different from the order number in the laboratory register. When registering a new patient, a unique identifier is assigned to each patient by the system, the user also has the possibility to enter an internal patient code in the laboratory. This allows the user to link the patient's analysis requests, to recall the history on the report and to easily follow the patient's history within the laboratory. The user first searches for the patient before creating a new one.