Fondation Mérieux

Lab Book

LabBook v3.6

Technical guide for preparing a LabBook validation file

March 2023

Fondation **Mérieux**

Lutte contre les maladies infectieuses depuis 1967

www.fondation-merieux.org

Table of Contents

Purpose

This document is intended for medical laboratories using the LabBook Laboratory Information System (LIS). It serves as a guide for laboratories to set up a software validation file in accordance with ISO 15189. This guide provides an approach enabling the laboratory to qualify the use of the LabBook tool and ensure its adoption in terms of control, maintenance, and monitoring. The laboratory must also have a procedure for using the LIS, a procedure for degraded mode, and a procedure for assessing skills (which in this case covers the assessment of the teams' skills in managing and using the software).

We recommend watching this training video on the Quality Initiative website:

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 map highlights the interactions between the LabBook software and other laboratory software (middleware, PLC software, external software, etc.).

Finally, conducting a risk analysis is strongly recommended for security purposes.

Settings

Roles

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

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

Analysis reference system

The laboratory must check the settings for analyses and dictionaries before putting LabBook into service. Only the administrator and the biologist can perform this task within LabBook.

Configuring analyses is a critical operation that must be checked and validated before the software is put into service, focusing on the following elements:

- Code
- Designation
- Abbreviation
- Analysis family
- Sample type
- WHONET export

- Label
- Value type
- Usual values
- Unit
- Formula if calculated field

All settings must be validated before commissioning. This validation must be recorded in the laboratory's documentation system along with evidence of the tests performed (e.g., screen shots).

Dictionaries

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

Report templates

Reports must include, but are not limited to, the information specified by ISO 15189. In case of non-compliance, the laboratory must edit the template and complete the missing elements. It may refer to the LabBook reference.

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 that test patient files be created to verify data transmission from recording to report editing. We recommend one test file per analysis actually performed by the laboratory.

During this data transmission phase, it is important to check rounded figures, reference values, and units.

It is also important to validate internally the "cancel and replace" function, which allows you to check that the words "cancel and replace" have been added with the date/time of modification on the corrected report.

The correct execution of the three validations available within LabBook must be checked: administrative, technical, and biological validation.

The LabBook software offers the option to merge and delete files. These two functions must be validated internally before use.

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

Access security

The laboratory must raise awareness of IT security among its users. It is recommended that a user charter be drawn up. In employment contracts or through a specific charter, each laboratory employee must be bound to confidentiality when using the software. The laboratory must also ensure that any fraudulent access to the software is prevented.

Organizational chart

The laboratory shall implement measures to organize IT responsibilities and authorization levels in order to ensure control. It shall appoint an IT manager and a deputy. These appointments may involve internal and/or external personnel, for example the IT manager.

The roles and responsibilities must be clearly defined:

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

Access to the LabBook server

It is essential to keep the LabBook server in a quiet location. If there is no air-conditioned room available, the server must be placed in a room with a low temperature. The server must be connected to an uninterruptible power supply (UPS) to monitor its operation and ensure minimum autonomy. In a multi-user environment, it is advisable to check and set the server's IP address. Restarting the router or making changes to the equipment may cause this IP address to change, making the software inaccessible to users.

User monitoring

Periodic monitoring must be defined based on changes in the IT infrastructure and staff turnover. The manager must periodically check the system users. Inactive user accounts must be deactivated from the system. Everyone must adopt a policy of periodically changing passwords.

Inactivity lockout period

In order to ensure that actions can be attributed to users, it is important to set a lockout or logout period for inactivity, with redirection to the login page. In order to protect data, guarantee system security, and ensure the traceability of actions, the laboratory specifies the lockout procedures in its IT security policy:

- When leaving the workstation;
- Based on a predefined period of inactivity;
- In the event of a change of user.

Data security

The laboratory must develop a procedure for controlling the integrity of information, in particular data backup.

Data integrity tests must be performed at defined intervals, after software modifications, and in the event of a failure (before restarting). These tests must enable the laboratory to ensure that the data is complete, i.e., accurate, legible, original, complete, durable, consistent, available, and uncorrupted. The tests performed and the associated evidence must be kept in the laboratory's QMS.

Backup

Backups prevent data loss in the event of unauthorized access or failure. The person responsible must regularly check at a specified time that the backup has been performed correctly.

Backup type

There is only one type of backup with LabBook: full backup. It includes database files and downloaded files.

Backup media

Backups are performed on removable media connected to the LabBook server. This media allows for restoration in the event of a computer server failure or destruction. The backup is encrypted with a GPG key and secured with a password to prevent any risk of data access. Remember to change the backup media when there is no more space available, or copy the backups to another medium and free up the space. It is recommended that you copy the contents of the backup media to a location remote from the server (not in the same building), so that data can be restored 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 sets the time at which the system performs the automatic backup. Preferably, this should be a time when the system is less busy. Manual backups can be initiated at any time.

Restoration

Data restoration allows the LabBook database to be restored 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 the data is not corrupted after restoration. To do this, reports before and after restoration will be compared. This test must be documented and attached to the laboratory's quality system.

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

Update

New features in 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 for new updates and installs them. The version used is indicated at the bottom of the software pages.

Before updating, the manager must verify that the last backup was performed correctly. In the event of an update involving software changes, it is necessary to verify that there is no retroactivity (in the event of a result being reissued, old reports must not be modified by the new version of the software).

After the update, the software must be revalidated by creating test files and documenting this in a report.

Managing a server failure

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

Before a failure

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

In the event of a failure

- → Inform laboratory staff of the incident and the implementation of the degraded procedure.
- → Start restoring the data using the latest available backup.
- → Check that the restoration is proceeding correctly (number of files; list of users; display of results on the report).

After a failure

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

Staff training

All staff using the LabBook software must be trained in its operation and use. To this end, when the software is installed, future key users of the system are trained. The term "user" should be taken in the broadest sense, including all secretaries, technicians, biologists, and IT staff. At this level, the laboratory must plan to include LabBook training in its staff training program. Training is provided for new users, of course, but also for existing users when major software updates are released. Records of this training must be kept.

Patient traceability

The patient's unique 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 option of entering an internal laboratory patient code. This makes it possible to link the patient's test requests, recall previous reports, and easily track the patient's history within the laboratory. The user first searches for the patient before creating a new one.

Fondation Mérieux

Fighting infectious diseases since 1967

www.fondation—merieux.org