Fondation Mérieux

LabBook

LabBook v3.6

Dossier de validation du SIL

Qualifier et maîtriser LabBook selon la norme ISO 15189

V3.0

Octobre 2026

Table des matières

1. Objet et public 3
2. Présenter le système 4
2.1 Cartographie 4
2.2 Analyse de risques 4
3. Paramétrage 5
3.1 Rôles et habilitations 5
3.2 Référentiel des analyses 5
3.3 Dictionnaires 6
3.4 Modèles de comptes rendus 6
4. Tests de validation 7
5. Sécurité d'accès et traçabilité 8
5.1 Organisation 8
5.2 Accès au serveur 8
5.3 Utilisateurs 8
5.4 Verrouillage sur inactivité 8
5.5 Journal d'audit (nouveau en 3.6) 8
6. Sécurité des données 10
6.1 Sauvegarde 10
6.2 Restauration 10
6.3 Tests d'intégrité 10
7. Mises à jour et gestion des changements 11
8. Gestion d'une panne du serveur 12
9. Formation du personnel 13
10. Traçabilité du patient 14
Annexe — Historique du document 15

1. Objet et public

Ce guide aide un **laboratoire de biologie médicale** utilisateur de LabBook à constituer son **dossier de validation du SIL**, selon la norme **ISO 15189**. Le laboratoire y démontre qu'il **qualifie** l'outil et qu'il en **maîtrise** le contrôle, la maintenance et le suivi.

Public	Responsable qualité, biologiste responsable, responsable informatique
Livrables	Dossier de validation, procédure d'utilisation du SIL, procédure de fonctionnement en mode dégradé, procédure d'évaluation des compétences
Ressources	Vidéo de l'Initiative Qualité : https://www.initiative-qualite.org/webcast/comment-valider-un-logiciel-de-laboratoire/

Contenu type du dossier de validation :

#	Partie	§ de ce guide
1	Présentation : version de LabBook, cartographie des systèmes, analyse de risques	2
2	Paramétrage vérifié : rôles, référentiel, dictionnaires, modèles	3
3	Tests de validation et preuves	4
4	Sécurité d'accès et traçabilité	5
5	Sécurité des données : sauvegarde, restauration, intégrité	6
6	Mises à jour et gestion des changements	7
7	Gestion des pannes : mode dégradé	8
8	Formation et compétences	9

2. Présenter le système

2.1 Cartographie

Décrivez les systèmes qui communiquent avec LabBook :

- automates, via **LabBook Connect** ;
- tablettes **LabBook Lite** ;
- exports **DHIS2** et **WHONET** ;
- **API** (DPI, facturation) ;
- envoi des résultats par **email ou WhatsApp**.

Exemple de cartographie :

Système	Sens	Données	Moyen
GeneXpert (via Dx System)	Automate → LabBook	Résultats de charge virale	LabBook Connect, ASTM, port 12345
Tablette LabBook Lite (centre de santé)	Lite → LabBook	Patients, dossiers, résultats	HTTPS, synchronisation manuelle
DHIS2 national	LabBook → DHIS2	Données agrégées hebdomadaires	Automatisme, API DHIS2
Messagerie (Mailjet)	LabBook → patient	Compte rendu PDF protégé	Méthode d'envoi

2.2 Analyse de risques

L'analyse de risques est **vivement conseillée** en matière de sécurité. *Exemples de risques à évaluer :*

Risque	Mesure de maîtrise
Panne du serveur	Sauvegarde quotidienne, poste de secours, procédure en mode dégradé
Erreur de paramétrage d'une analyse	Validation du référentiel, dossiers tests
Accès non autorisé	Comptes nominatifs, rôles, déconnexion automatique, journal d'audit
Erreur de transfert depuis un automate	Vérification du mapping, contrôle des premiers résultats
Perte du mot de passe de la clé de sauvegarde	Double conservation, sous enveloppe scellée

3. Paramétrage

3.1 Rôles et habilitations

Chaque compte utilisateur reçoit un **rôle**. LabBook 3.6.28 propose 15 types de rôle :

- 12 rôles configurables : administrateur, biologiste, technicien, technicien avancé, technicien qualiticien, secrétaire, secrétaire avancé, préleveur, prescripteur, qualiticien, gestionnaire de stock, laboratoire ;
- 3 rôles particuliers : API, agent (LabBook Lite), personnel (sans connexion).

Depuis la 3.5, les **droits** de chaque rôle peuvent être ajustés, et des rôles dérivés créés (guide D1, § 5).

À documenter :

- la matrice des droits **réellement appliquée** dans le laboratoire. Partez de la matrice par défaut (document *Rôles et droits LabBook 3.6.28*) et notez les écarts ;
- la liste des utilisateurs et de leur rôle, **revue périodiquement**.

Si des prestataires informatiques interviennent sur LabBook, ce sont des **fournisseurs critiques** : contrat et clause de confidentialité.

3.2 Référentiel des analyses

Le paramétrage des analyses est une **opération critique**. Seuls l'administrateur et le biologiste (et le technicien avancé, par défaut) peuvent le modifier.

Pour **chaque analyse réalisée** par le laboratoire, vérifiez :

Bloc	Points à vérifier
Analyse	Code, désignation, abréviation, famille, type de prélèvement, cotation, export WHONET
Variables	Libellé, type de résultat, valeurs usuelles, unité et précision, formule si champ calculé, présence sur le compte rendu

Exemple de fiche de vérification :

Analyse	Élément	Attendu	Constaté	Conforme	Visa / date
B004 Créatininémie	Unité	µmol/L	µmol/L	Oui	AB, 12/10
B004 Créatininémie	Valeurs usuelles (F adulte)	45 – 90	45 – 90	Oui	AB, 12/10
VGM	Formule	`$_3*10/$_1`	`$_3*10/$_1`	Oui	AB, 12/10

3.3 Dictionnaires

Vérifiez les **listes de choix** utilisées par les variables : libellés et codes. Vérifiez aussi la liaison au type de résultat (guide D1, § 7.3).

3.4 Modèles de comptes rendus

Le compte rendu doit comporter les informations exigées par l'ISO 15189. En cas de manque, adaptez le modèle (guide D3) et faites-le valider.

4. Tests de validation

Quand faire les tests :

- avant la **mise en production** ;
- après toute **modification** du référentiel, des dictionnaires ou des modèles ;
- après une **panne** ;
- après une **mise à jour** de LabBook.

Méthode : créez des **dossiers patients tests**, idéalement **un par analyse réalisée**. Suivez chaque dossier de l'enregistrement jusqu'à l'édition du compte rendu.

Contrôle	Comment
Transmission des données	Les valeurs saisies se retrouvent à l'identique sur le compte rendu
Arrondis, unités, valeurs de référence	Comparez au référentiel ; testez une valeur hors normes (signal et mise en forme)
Formules	Calculez à la main un résultat calculé
Validations	Administrative (A), technique (T) et biologique (B) : statuts et droits
« Annule et remplace »	Rééditez un compte rendu validé : mention et date de modification présentes
Fusion de dossiers patients	Testez la fusion sur deux patients tests (guide D1, § 11.2)
Suppression de dossier	Testez-la sur un dossier test, avec le rôle qui en a le droit
Envoi des résultats (3.6)	Envoi à une adresse de test ; consentement respecté ; PDF protégé si activé
Interfaces	Automates, Lite, DHIS2 : comparez les données reçues et envoyées
Droits	Pour chaque rôle utilisé, vérifiez qu'il voit ce qu'il doit voir, et seulement cela

Preuves : copies d'écran, comptes rendus PDF, fiches de vérification datées et signées. Conservez-les dans le système de management de la qualité.

5. Sécurité d'accès et traçabilité

5.1 Organisation

- Nommez un **responsable informatique** et un **suppléant**, internes ou externes.
- Définissez précisément leurs fonctions : gestion du référentiel, gestion des utilisateurs, installation des mises à jour, vérification des sauvegardes, gestion du matériel (ordinateurs, imprimantes, onduleur).

5.2 Accès au serveur

- Serveur dans un local **peu fréquenté**, frais (climatisé si possible), sur **onduleur**.
- En multiposte, **fixez l'adresse IP** du serveur (guide E3).
- Appliquez les mesures de sécurisation (guide E2) : HTTPS, changement des mots de passe par défaut, chiffrement du disque.

5.3 Utilisateurs

- Sensibilisez le personnel : **charte informatique**, clause de **confidentialité** dans les contrats.
- **Un compte nominatif par personne**, jamais de compte partagé.
- Revue périodique des comptes ; **désactivation** des comptes inactifs ; changement périodique des mots de passe.

5.4 Verrouillage sur inactivité

Fixez le délai de **déconnexion automatique** (guide D1, § 3.2) et décrivez dans la politique de sécurité les règles de verrouillage :

- au moment de quitter son poste ;
- après un temps d'inactivité défini ;
- à chaque changement d'utilisateur.

5.5 Journal d'audit (nouveau en 3.6)

Le **journal d'audit** enregistre automatiquement les actions sensibles : connexions réussies ou échouées, opérations sur les utilisateurs, les dossiers et les paramètres. Il indique pour chacune la date (UTC), l'utilisateur, son rôle et l'adresse IP. C'est un élément de preuve majeur pour l'**imputabilité** des actions.

À documenter :

- l'activation du journal (préférence *Audit trail activé*) ;

- sa durée de conservation en base (12 mois par défaut) ;
- l'archivage automatique mensuel et le lieu de conservation des archives ;
- la fréquence de **revue** du journal. *Exemple : chaque mois, recherche des connexions en ECHEC et des modifications de paramètres.*

Voir le guide D1, § 11.1.

6. Sécurité des données

Élaborez une **procédure de maîtrise de l'intégrité des informations**. Les données doivent être exactes, lisibles, originales, complètes, durables, cohérentes, disponibles et non corrompues.

6.1 Sauvegarde

Élément	Ce que fait LabBook	À documenter
Type	Sauvegarde **totale** : base de données et documents	—
Support	Média amovible branché sur le serveur ; archive **chiffrée** (GPG) par une clé protégée par mot de passe	Supports utilisés, rotation, copie hors du bâtiment
Fréquence	Sauvegarde **automatique quotidienne** à l'heure choisie, plus des sauvegardes manuelles à tout moment	Heure choisie, période creuse
Surveillance	Statut sur la page d'accueil ; **alerte** si la dernière sauvegarde réussie date de plus de 24 h	Responsable, fréquence de vérification, registre

6.2 Restauration

Réalisez des **tests de restauration** réguliers, sur un poste de test. Comparez des comptes rendus **avant et après** restauration et documentez le test (guide E4, § 8).

6.3 Tests d'intégrité

À intervalles définis, après une modification du logiciel et après une panne (avant la remise en route) : contrôlez un échantillon de dossiers, de comptes rendus et de résultats. Conservez les preuves.

7. Mises à jour et gestion des changements

- Les nouveautés sont publiées sur **www.lab-book.org** et dans le **journal des modifications** (Changelog) du dépôt GitHub. Elles sont aussi annoncées dans la communauté LinkedIn : https://www.linkedin.com/groups/9052040/.
- La **version** en service est affichée en bas de chaque page (ex. *Version : 3.6.28*).

Avant la mise à jour :

- lisez les changements de la version et évaluez leur impact (fonctions, droits, modèles) ;
- vérifiez la dernière sauvegarde.

Après la mise à jour :

- vérifiez la **non-rétroactivité** : un ancien compte rendu réédité n'est pas modifié par la nouvelle version ;
- **revalidez** avec des dossiers tests, en ciblant les fonctions modifiées ;
- consignez le tout dans un rapport.

Exemple de fiche de changement :

Version	Date	Changements notables	Tests réalisés	Résultat	Visa
3.6.27 → 3.6.28	24/10/2026	Sécurité : certificats racines (certifi)	Connexion, demande, validation, CR, envoi email	Conforme	Resp. info

8. Gestion d'une panne du serveur

Avant une panne :

- rédigez et diffusez la **procédure en mode dégradé** : registre papier, fiches de résultats, ressaisie ultérieure ;
- disposez si possible d'un **ordinateur de secours** sur lequel LabBook est installé, dans la même version ;
- vérifiez chaque jour les sauvegardes.

Pendant la panne :

- informez le personnel et appliquez la procédure dégradée ;
- restaurez la **dernière sauvegarde** sur le poste de secours (guide E4) ;
- vérifiez la restauration : nombre de dossiers, utilisateurs, affichage des comptes rendus.

Après la panne :

- faites un **test de validation** du système restauré ;
- reconfigurez le réseau et vérifiez l'accès depuis les postes (guide E3) ;
- vérifiez les sauvegardes sur le nouveau serveur ;
- ressaisissez les dossiers traités en mode dégradé et tracez cette ressaisie.

9. Formation du personnel

- **Tout le personnel** qui utilise LabBook est formé : secrétaires, préleveurs, techniciens, biologistes, qualiticiens, informaticiens.
- Prévoyez une formation **à l'installation**, pour chaque **nouvel arrivant** et à chaque **mise à jour majeure**.
- Intégrez LabBook au **plan de formation** et à l'**évaluation des compétences**.
- Conservez les preuves de formation. Les guides par rôle (B1 à B7) et le module **LabBook E-learning** du serveur servent de supports.

10. Traçabilité du patient

- L'**identifiant unique** du patient (code LabBook) est différent du numéro d'ordre du registre du laboratoire. Le laboratoire peut aussi renseigner un **code patient interne**.
- Cet identifiant relie toutes les demandes du patient, permet les **antériorités** sur le compte rendu et l'**historique** du patient.
- **Règle à faire appliquer : toujours rechercher le patient avant d'en créer un nouveau.** Les doublons sont corrigés par la **fusion** de dossiers (guide D1, § 11.2), elle-même tracée.

Annexe — Historique du document

Version	Date	LabBook	Modifications
3.0	10/2026	3.6.28	Mise à jour 3.6 : 15 rôles et droits configurables, journal d'audit, envoi des résultats, interfaces (Connect, Lite, DHIS2, API). Ajout d'exemples de cartographie, d'analyse de risques, de fiche de vérification et de fiche de changement ; plan type du dossier
—	03/2023	3.3	Version précédente