



**MINISTÈRE DE LA SANTÉ
PUBLIQUE, HYGIÈNE ET
PRÉVOYANCE SOCIALE**

**Secrétariat Général à la Santé
Direction des Laboratoires de Santé**

Document des Spécifications pour un Système Intégré de Gestion de l'Information des Laboratoires (SIGIL) en RDC

Mars 2025

Introduction

Dans le cadre de la modernisation du système de santé de la République Démocratique du Congo (RDC), le Ministère de la Santé Publique, Hygiène et Prévention s'engage à améliorer la qualité des services de laboratoire. Un élément essentiel de cette initiative est la mise en place d'un Système Intégré de Gestion de l'Information de Laboratoire (LIMS) performant. Ce système vise à renforcer les capacités de diagnostic, la surveillance épidémiologique et la prise de décision basée sur des données probantes.

Le présent document expose les spécifications fonctionnelles et non fonctionnelles pour l'acquisition d'un LIMS adapté au contexte congolais. Il servira de guide pour la sélection d'une solution logicielle répondant aux besoins des laboratoires de santé en RDC, tout en s'intégrant harmonieusement dans le paysage numérique national. Les exigences détaillées dans ce document permettront d'assurer la cohérence, l'interopérabilité et la pérennité du système.

1. Contexte et Objectifs

1.1 Contexte

La RDC fait face à des défis sanitaires majeurs, marqués par une forte prévalence des maladies transmissibles et une augmentation des maladies non transmissibles. Les laboratoires de santé jouent un rôle crucial dans la lutte contre ces maladies, mais leur efficacité est souvent limitée notamment par l'absence d'un réseau fonctionnel des laboratoires de santé, l'absence des bases des données des laboratoires à différents niveaux, l'inexistence de mécanisme d'accréditation des laboratoires, l'inexistence des supports d'analyse des données de laboratoire permettant de générer l'information utile à la prise de décision, etc.

1.2 Objectifs

Le développement et la mise en place d'un système intégré de gestion de l'information de laboratoire (SIGIL) vise notamment :

- L'amélioration de la qualité et de l'utilisation des résultats des analyses à travers les demandes de test et les retours des résultats plus rapides, fiables et sécurisés),
- L'amélioration de la disponibilité de l'information de laboratoire (en temps réel) et de la performance collective du réseau des laboratoires,
- La centralisation et la standardisation des données de laboratoire (notamment les données les tests et de performance du réseau).
- Le renforcement de la surveillance épidémiologique, à travers la disponibilité des résultats des analyses dans un délai plus réduit pour une prise de décision rapide.

- L'amélioration de la prise en charge clinique, à travers des résultats de qualité partagé de manière sécurisé et disponible à temps,
- L'optimisation de la gestion des ressources (équipements, réactifs, consommables) et l'amélioration continue du réseau des laboratoires.
- La facilitation de la prise de décision concernant le système de laboratoire et le réseau diagnostic pour plus d'efficacité.
- L'amélioration de la contribution du laboratoire à la prise de décision clinique et de santé publique (incluant la surveillance et la riposte).

2. Exigences Fonctionnelles

Le SIGIL doit répondre aux besoins opérationnels des laboratoires de santé en RDC. Cependant il important de distinguer les deux dimensions suivantes :

- le système d'information de laboratoire (LIS local) et
- le système intégré de gestion de l'information de laboratoire (SIGIL) qui constitue l'étape ultime d'intégration souhaitée des différents LIS ainsi que des autres sous-systèmes tels que le dossier médical électronique, le système électronique de gestion des approvisionnements et des stocks, etc.

Les exigences fonctionnelles sont réparties dans ces deux dimensions et catégorisées de manière suivantes :

Tableau n°1. Exigences fonctionnelles

a. LIS local

ID exigence	Exigence fonctionnelle	Catégorie	Justification (notes explicatives)
F-001	Gestion des patients	Essentielle	Identifiant patient unique, critique pour la traçabilité.
F-002	Gestion des échantillons	Essentielle	Traçabilité indispensable pour toutes analyses.
F-003	Gestion des analyses	Essentielle	Base opérationnelle du laboratoire.
F-004	Gestion des résultats	Essentielle	Clé pour fiabilité des données générées.
F-005	Contrôle qualité	Essentielle	Garantir fiabilité des résultats.
F-006	Gestion des stocks	Essentielle	Indispensable pour la continuité des opérations.
F-008	Sécurité et confidentialité	Essentielle	Obligation légale et éthique.
F-009	Traçabilité	Essentielle	Obligatoire pour audits et conformité.
F-010	Gestion des utilisateurs	Essentielle	Sécurité et gouvernance interne.
F-011	Gestion des workflows	Importante	Optimisation du processus interne.

ID exigence	Exigence fonctionnelle	Catégorie	Justification (notes explicatives)
F-012	Gestion des équipements	Importante	Impact direct sur la qualité des tests.
F-013	Gestion des documents	Importante	Facilite gestion administrative et qualité.
F-016	Gestion des interfaces automatés	Importante	Réduire les risques d'erreurs humaines.
F-018	Personnalisation	Optionnelle	Adaptation selon préférences locales.
F-019	Support multilingue	Importante	Pertinent dans contexte multilingue RDC.
F-020	Audit et traçabilité	Essentielle	Critère obligatoire pour certification et conformité.

Les descriptions et les critères d'acceptation des différentes exigences sont reprises dans le document annexe des exigences.

b. SIGIL (intégration et interopérabilité)

ID exigence	Exigence fonctionnelle	Catégorie	Justification (notes explicatives)
F-014	Intégration avec autres systèmes	Essentielle	Clé pour l'interopérabilité nationale (DHIS2).
F-015	Gestion des alertes	Essentielle	Gestion proactive des risques sanitaires.
F-017	Gestion des référentiels	Essentielle	Standardisation nationale indispensable.

ID exigence	Exigence fonctionnelle	Catégorie	Justification (notes explicatives)
F-021	Gestion des accréditations	Essentielle	Priorité de la DLS pour garantir la qualité.
F-049	Gestion données épidémiologiques	Essentielle	Surveillance et prise de décision stratégique.
F-050	Confidentialité des données	Essentielle	Conformité réglementaire nationale.
F-007	Génération de rapports nationaux	Essentielle	Reporting national centralisé obligatoire.
F-045	Gestion alertes sécurité	Importante	Sécurisation accrue des données.
F-046	Gestion des communications	Importante	Facilite échanges interlaboratoires.
F-048	Gestion résultats externes	Importante	Communication efficace avec les prescripteurs.
F-047	Gestion demandes externes	Importante	Centralisation demandes inter-établissements.
F-031	Indicateurs de performance	Importante	Suivi national et amélioration continue.
F-038	Gestion archives nationales	Importante	Conservation sécurisée et durable.
F-024	Gestion des coûts	Optionnelle	Optimisation financière à terme.
F-025	Gestion facturation	Optionnelle	Gestion financière optimisée.
F-026	Gestion paiements	Optionnelle	Utile mais non critique immédiatement.

3. Exigences Non Fonctionnelles

Le SIGIL doit également respecter des exigences non fonctionnelles pour garantir sa performance, sa fiabilité et sa sécurité. Les principales exigences non fonctionnelles sont les suivantes :

Tableau n°2. Exigences non fonctionnelles

a. LIS (implémentation laboratoire)

ID Exigence	Exigence Non Fonctionnelle	Catégorie	Notes explicatives
NF-001	Disponibilité locale ≥99%	Essentielle	Continuité des opérations locales
NF-004	Mode hors-ligne local	Essentielle	Infrastructures locales limitées en RDC
NF-005	Sauvegarde et récupération locale	Essentielle	Protection des données locales
NF-006	Maintenance locale simplifiée	Importante	Facilite autonomie locale
NF-007	Formation continue locale	Essentielle	Adoption immédiate utilisateurs
NF-020	Support technique local permanent	Essentielle	Assistance immédiate utilisateurs
NF-018	Interface utilisateur personnalisable locale	Optionnelle	Adaptation aux préférences locales
NF-008	Documentation utilisateurs complète	Importante	Renforce autonomie locale
NF-019	Compatibilité multi-plateforme locale	Optionnelle	Souhaitable pour flexibilité

b. SIGIL (Intégration et interopérabilité)

ID Exigence	Exigence Non Fonctionnelle	Catégorie	Notes explicatives
NF-002	Sécurité des données (Authentification forte, chiffrement AES-256)	Essentielle	Obligation réglementaire
NF-003	Conformité normes sécurité (RGPD, HIPAA)	Essentielle	Respect cadre légal international
NF-009	Traçabilité et audit	Essentielle	Obligation réglementaire
NF-004	Synchronisation automatique	Essentielle	Consolidation des données nationales
NF-005	Sauvegarde nationale régulière	Essentielle	Prévention pertes de données
NF-010	Sécurisation avancée nationale	Essentielle	Protection données sensibles nationales
NF-012	Interopérabilité HL7 FHIR	Essentielle	Norme nationale adoptée
NF-013	Redondance système central	Importante	Renforce disponibilité centrale
NF-014	Scalabilité du système	Importante	Extension progressive prévue
NF-019	Compatibilité multiplateforme	Optionnelle	Flexibilité accrue
NF-015	Interface utilisateur nationale personnalisable	Optionnelle	Adaptation possible selon besoin
NF-003	Gestion de la conformité aux normes sécurité	Essentielle	Respect réglementation stricte
NF-011	Redondance système national	Importante	Réduction risques techniques
NF-012	Interopérabilité renforcée (HL7 FHIR national)	Essentielle	Standard adopté par ANICNS

ID Exigence	Exigence Non Fonctionnelle	Catégorie	Notes explicatives
NF-013	Infrastructure redondante nationale	Importante	Augmente disponibilité système
NF-014	Tableau analytique avancé centralisé	Optionnelle	Analyses avancées à terme
NF-022	Audit centralisé et traçabilité complète	Essentielle	Conformité aux normes réglementaires
NF-021	Gestion accréditations nationales (ISO 15189)	Essentielle	Priorité stratégique de la DLS
NF-016	Tableau de bord analytique national	Importante	Outil de décision utile
NF-023	Surveillance centralisée des KPI	Importante	Suivi performance nationale
NF-017	Gestion sécurisée des équipements	Importante	Fiabilité des équipements
NF-023	Gestion des documents et archives centralisées	Importante	Obligations légales

4. Spécifications Techniques

4.1 Architecture du Système

- **Architecture logicielle :**

Le SIGIL doit être conçu selon une architecture modulaire et flexible, de type n-tiers, pour faciliter l'évolution et la maintenance. Les composants principaux incluent :

- **Interface utilisateur :** Accessible via un navigateur web (compatible avec Chrome, Firefox et Edge) pour une utilisation sur différents appareils (ordinateurs, tablettes). Privilégier une interface intuitive avec des menus clairs, des icônes explicites et une navigation simple.
- **Serveur d'application :** Hébergeant la logique métier du SIGIL, développé avec des technologies robustes comme Java ou Python, et capable de gérer un grand nombre de requêtes simultanées.
- **Serveur de base de données :** Utilisant une base de données relationnelle (PostgreSQL, MySQL) pour stocker les données de manière sécurisée et performante. La base de données doit être hébergée sur un serveur dédié et sécurisé, avec des sauvegardes régulières et un système de restauration en cas de panne.

- **Architecture matérielle :**

- **Serveurs :** Serveurs robustes avec une capacité de stockage et de traitement suffisante pour gérer les données des laboratoires. Privilégier des serveurs avec une redondance pour assurer une haute disponibilité du système. Envisager des solutions d'alimentation de secours (onduleurs, générateurs) pour pallier les coupures d'électricité fréquentes en RDC.

Critère technique	Qualification recommandée pour le serveur LIS/SIGIL
Type de serveur	Serveur dédié ou Cloud hybride
Processeur	Processeur multicœur (≥ 8 cœurs physiques, Intel Xeon ou équivalent)
Mémoire RAM	Minimum 32 Go (recommandé ≥ 64 Go pour évolutivité)
Stockage principal	SSD (disques à état solide) ≥ 2 To
Stockage sauvegarde	Solution RAID (niveau 1 ou 5) pour redondance et sécurité
Réseau	Carte réseau Gigabit Ethernet (≥1Gbps)
Redondance	Redondance matérielle complète recommandée (alimentation, disque, réseau)
Haute disponibilité	Clustering ou virtualisation pour assurer disponibilité ≥ 99.9%

Critère technique	Qualification recommandée pour le serveur LIS/SIGIL
Sauvegarde électrique	Onduleurs professionnels avec autonomie ≥ 2 heures, complétés idéalement par générateur électrique (groupe électrogène)

- **Postes de travail** : Ordinateurs de bureau ou portables pour les utilisateurs, avec des configurations minimales (processeur, mémoire vive, espace disque) définies en fonction des besoins.
- **Imprimantes** : Imprimantes laser pour l'impression des étiquettes, des rapports et des documents. Choisir des imprimantes robustes et faciles à entretenir, avec une disponibilité des consommables en RDC.
- **Scanners** : Scanners de documents pour la numérisation des documents et des résultats d'analyse.
- **Architecture réseau** :
 - Le SIGIL doit pouvoir fonctionner sur un réseau local (LAN) au sein du laboratoire et être accessible à distance via un réseau étendu (WAN) sécurisé (VPN).
 - Utiliser le protocole TCP/IP pour la communication entre les différents composants du système.
 - Mettre en place un pare-feu et un système de détection d'intrusion pour protéger le réseau contre les accès non autorisés.
- **Déploiement** :
Le déploiement du SIGIL en RDC sera structuré selon une approche hybride afin d'optimiser la disponibilité, la sécurité et la facilité de maintenance en fonction des réalités opérationnelles des laboratoires. Il consistera à une combinaison d'approche dont le déploiement sur site et le déploiement dans le cloud.

■ **Déploiement sur site (on-premise) :**

Cette approche convient aux laboratoires dotés d'une infrastructure informatique locale solide, incluant des serveurs dédiés, un réseau fiable et une alimentation électrique stable avec solutions de secours (onduleurs, générateurs).

Avantages principaux :

- Contrôle total des données et des systèmes.
- Indépendance vis-à-vis d'une connexion Internet permanente.

■ **Déploiement dans le Cloud :**

Cette solution est recommandée pour les laboratoires ne disposant pas d'infrastructures adéquates ou de ressources techniques permanentes sur site.

Avantages principaux :

- Maintenance centralisée simplifiée.
- Sécurité et haute disponibilité garanties ($\geq 99.9\%$).
- Accès facilité à partir de divers emplacements géographiques.

- Déploiement Hybride (recommandé) :

Combinaison optimale du déploiement local et cloud en fonction des capacités spécifiques de chaque laboratoire. Cette approche permet une synchronisation sécurisée entre les sites locaux et le cloud, garantissant ainsi une meilleure disponibilité, flexibilité et sécurité.

4.2 Interface Utilisateur

- **Principes généraux** : L'interface utilisateur doit être conçue selon les principes d'ergonomie et d'accessibilité, en tenant compte des besoins des utilisateurs congolais.
 - Utiliser une terminologie claire, concise et adaptée au contexte local.
 - Privilégier une navigation intuitive et simple, avec des menus clairs et des icônes explicites.
 - Assurer la compatibilité avec les navigateurs web les plus utilisés en RDC (Chrome, Firefox).
 - Prendre en compte les limitations de bande passante et optimiser l'interface pour un chargement rapide.
- **Fonctionnalités** :
 - L'interface utilisateur doit permettre aux utilisateurs d'effectuer toutes les opérations nécessaires à la gestion des activités du laboratoire, notamment :
 - Enregistrement des patients et des échantillons.
 - Saisie des demandes d'analyse.
 - Gestion des résultats d'analyse.
 - Génération de rapports.
 - Gestion des stocks.
 - Gestion des équipements.
 - Fournir des exemples de captures d'écran pour illustrer l'interface utilisateur.
- **Technologies** :
 - Utiliser des technologies web modernes pour développer l'interface utilisateur (HTML5, CSS3, JavaScript).
 - Envisager l'utilisation de Framework JavaScript (React, Angular, Vue.js) pour faciliter le développement et la maintenance de l'interface.

4.3 Base de Données

- **Type de base de données** : Utiliser une base de données relationnelle (PostgreSQL, MySQL) pour stocker les données du SIGIL. Ce type de base de données offre une bonne performance, une sécurité et une intégrité des données.

- **Structure de la base de données** : La base de données doit être conçue pour stocker toutes les informations nécessaires à la gestion des activités du laboratoire, notamment :
 - Informations sur les patients.
 - Informations sur les échantillons.
 - Informations sur les analyses.
 - Résultats d'analyse.
 - Informations sur les stocks.
 - Informations sur les équipements.
 - Informations sur les utilisateurs.
- **Sécurité** : Mettre en place des mesures de sécurité pour protéger la base de données contre les accès non autorisés et les cyberattaques.
 - Contrôle d'accès basé sur les rôles des utilisateurs.
 - Chiffrement des données sensibles.
 - Sauvegardes régulières et système de restauration en cas de panne.

4.4 Intégration, interopérabilité et échange des données

Le système devra permettre :

L'intégration avec :

- Systèmes locaux (LIS existants, automates d'analyse)
- Dossiers médicaux électroniques (EMR)
- Applications tierces (gestion des stocks, comptabilité)

En utilisant des web services et des API.

L'interopérabilité :

- Respect strict des standards nationaux (HL7 FHIR, terminologies standardisées)
- Communication fluide et compréhensible par tous les systèmes partenaires tels que les systèmes d'information hospitalier (SIH), le système national d'information sanitaire (SNIS), le systèmes d'information des programmes nationaux de santé (ex : programme national de lutte contre le VIH/SIDA).

Les échanges de données :

- Importation et exportation de données sous formats standards (CSV, XML, JSON)
- Facilitation des échanges ponctuels ou réguliers entre divers systèmes.

4.5 Sécurité

- **Authentification** : Utiliser des mécanismes d'authentification forte pour protéger l'accès au SIGIL.

- Mots de passe complexes.
- Authentification à deux facteurs.
- Authentification unique (SSO).
- **Chiffrement** : Chiffrer les données sensibles, aussi bien en transit qu'au repos.
- **Audit** : Enregistrer toutes les actions effectuées dans le système pour permettre l'audit et la traçabilité.

4.6 Performance

- **Temps de réponse** : Le temps de réponse du système pour les opérations courantes doit être inférieur à 3 secondes.
- **Scalabilité** : Le système doit pouvoir gérer un volume croissant de données et d'utilisateurs sans dégradation des performances.
- **Disponibilité** : Le système doit avoir un taux de disponibilité de 99,9 %.

4.7 Maintenance

- **Mises à jour** : Le fournisseur doit proposer des mises à jour régulières du système pour corriger les bogues et ajouter de nouvelles fonctionnalités.
- **Support technique** : Le fournisseur doit assurer un support technique adéquat, avec une assistance téléphonique et en ligne.

6. Conclusion

La mise en œuvre d'un Système Intégré de Gestion de l'Information des Laboratoires (SIGIL) en République Démocratique du Congo est une étape cruciale pour moderniser le système de santé et améliorer la qualité des services de laboratoire. Ce document de spécifications définit un cadre rigoureux pour la sélection et le déploiement d'un SIGIL robuste, fiable et adapté au contexte congolais, en détaillant les exigences fonctionnelles et non fonctionnelles, ainsi que les spécifications techniques nécessaires. Ce projet de transformation numérique, axé sur l'utilisateur et les standards internationaux, permettra d'améliorer la qualité des diagnostics, la prise de décision et la surveillance épidémiologique, grâce à la collaboration étroite entre les différentes parties prenantes pour garantir le succès de cette initiative stratégique au bénéfice de la population congolaise.