

**GUIDE TECHNIQUE D'ACCREDITATION  
POUR L'EVALUATION DES SYSTEMES  
INFORMATIQUES EN BIOLOGIE MEDICALE**

**SH GTA 02**

**Révision 00**

LA VERSION ELECTRONIQUE N'EST PAS LA VERSION OFFICIELLE



*Santé humaine*

## SOMMAIRE

<b>1</b>	<b>OBJET DU DOCUMENT</b> .....	<b>5</b>
<b>2</b>	<b>TERMINOLOGIE ET REFERENCES</b> .....	<b>5</b>
2.1	Définitions .....	5
2.2	Abréviations .....	8
<b>3</b>	<b>DOMAINE D'APPLICATION</b> .....	<b>11</b>
<b>4</b>	<b>MODALITES D'APPLICATION</b> .....	<b>12</b>
<b>5</b>	<b>SYNTHESE DES MODIFICATIONS</b> .....	<b>12</b>
<b>6</b>	<b>RECENSEMENT ET TYPOLOGIE DES ARCHITECTURES DE SYSTEMES</b> .....	<b>12</b>
6.1	Introduction.....	12
6.2	<b>Architecture des serveurs</b> .....	<b>13</b>
6.2.1	Les serveurs non critiques.....	13
6.2.2	Les serveurs critiques .....	13
6.2.3	Rappel des recommandations de la norme NF EN ISO 15189 sur l'architecture serveur.....	13
6.2.3.1	Sécurité des locaux.....	14
6.2.3.1.1	Locaux « serveurs ».....	14
6.2.3.1.2	Locaux informatiques des sites distants.....	14
6.2.3.2	Points clefs dans l'analyse de l'environnement.....	14
6.2.3.3	Pannes matérielles et logiciels .....	15
6.2.4	Typologie d'hébergement des serveurs critiques.....	15
6.2.5	Agrément de l'hébergeur des données.....	16
6.2.5.1	Rappel du cadre juridique .....	16
6.2.5.2	Les cas soumis à la procédure d'agrément .....	17
6.2.5.2.1	Base de données confiée à un prestataire spécialisé dans l'hébergement de données .....	17
6.2.5.2.2	SIL mutualisé entre deux LBM .....	17
6.2.5.2.3	MW mutualisé entre deux LBM .....	17
6.2.5.2.4	Serveur de résultats mutualisé entre deux établissements.....	18
6.3	<b>Architecture terminaux et réseaux</b> .....	<b>18</b>
6.3.1	Rappel des recommandations de la norme NF EN ISO 15189 sur les terminaux et réseaux .....	18
6.3.2	Typologie des terminaux .....	19
6.3.3	Typologie des réseaux locaux du site.....	19
6.3.3.1	Réseau Physique .....	20
6.3.3.2	Anti-virus.....	20
6.3.3.3	Pare-feu.....	20
6.3.3.4	Gestion des identités utilisateurs.....	21
6.3.4	Typologie des réseaux intersites.....	21
6.3.5	Recensement et typologie des connexions à distance .....	22
6.3.5.1	Connexion à distance par un personnel interne habilité .....	22
6.3.5.2	Connexion à distance par un fournisseur d'un serveur ou logiciel critique.....	22
6.4	<b>Architecture Applicative Critique</b> .....	<b>23</b>
6.4.1	Rappel des exigences de la norme NF EN ISO 15189 sur les applications critiques.....	23
6.4.2	Recensement et typologie des architectures multi-sites .....	24
6.4.2.1	Architecture Multi SIL, Multi MW – échange SIL par messagerie .....	24
6.4.2.2	Architecture Multi-SIL, plateau technique commun.....	25
6.4.2.3	Architecture mono SIL, Mono/Multi MW .....	26
6.4.3	Recensement des échanges de données d'un LBM.....	26
6.4.3.1	Phase pré-analytique .....	27
6.4.3.1.1	La feuille de prescription .....	28

6.4.3.1.2	Messages électroniques de données démographiques patients .....	28
6.4.3.1.3	Manuel de prélèvement sous forme électronique structurée .....	29
6.4.3.1.4	La prescription connectée .....	30
6.4.3.2	Phase analytique.....	31
6.4.3.3	Phase post-analytique.....	33
6.4.3.4	Biologie délocalisée .....	35
<b>6.5</b>	<b>Cartographie des systèmes et des échanges .....</b>	<b>36</b>
6.5.1	LBM de ville bi-sites travaillant avec deux établissements.....	37
6.5.2	LBM hospitalier .....	38
<b>7</b>	<b>PRECONISATIONS POUR LE FONCTIONNEMENT DES SYSTEMES INFORMATIQUES EN REGARD DES EXIGENCES .....</b>	<b>39</b>
<b>7.1</b>	<b>Environnement.....</b>	<b>39</b>
7.1.1	Matériels et logiciels .....	39
7.1.2	Critères de sélection d'un SIL ou d'un MW .....	40
<b>7.2</b>	<b>Maîtrise du paramétrage et des dictionnaires/tables .....</b>	<b>40</b>
7.2.1	Annuaire des tiers .....	40
7.2.2	Catalogue des examens.....	41
7.2.3	Harmonisation des systèmes unitaires .....	41
7.2.4	Gestion de l'adresse postale .....	41
<b>7.3</b>	<b>Maîtrise informatique de la phase pré-analytique.....</b>	<b>42</b>
7.3.1	Gestion informatique de l'identité des patients .....	42
7.3.1.1	Identités et mouvements de patients transmis par le SIH .....	43
7.3.1.2	Données d'identité patient lues sur la carte Vitale .....	43
7.3.1.3	Données patients reçues dans les demandes d'examens dématérialisées.....	43
7.3.2	Fusion des dossiers patients.....	43
7.3.3	Prescription (papier et/ou connectée).....	44
7.3.4	Cas particulier de l'autocréation de demande d'examens.....	45
7.3.5	Saisie de plusieurs demandes d'examens avec des analyses communes pour un même prélèvement.....	46
<b>7.4</b>	<b>Maîtrise informatique de la phase analytique .....</b>	<b>46</b>
7.4.1	Connexions des analyseurs en direct sur le SIL ou via MW .....	46
7.4.2	Règles de contrôle du processus analytique .....	47
7.4.3	Contrôle(s) de qualité connecté(s).....	48
<b>7.5</b>	<b>Maîtrise informatique de la phase post-analytique.....</b>	<b>48</b>
7.5.1	Dématérialisation des données .....	48
7.5.1.1	Serveurs de résultats intégrés à la chaîne de production des soins .....	49
7.5.1.2	Passerelle d'échange.....	49
7.5.2	Transfert des données par Module Fax informatique.....	50
7.5.3	Signature électronique et signature électronique présumé fiable.....	50
7.5.4	Systèmes d'aide à la validation biologique (SAVB) .....	50
7.5.4.1	Catégories de systèmes.....	50
7.5.4.2	Etudes préalables à l'adoption .....	50
7.5.4.3	Paramétrages des règles d'expertise .....	51
7.5.4.4	Exploitation du système .....	51
7.5.4.5	Surveillance du système .....	51
<b>7.6</b>	<b>Organigramme informatique .....</b>	<b>52</b>
<b>7.7</b>	<b>Maîtrise de la sécurité informatique .....</b>	<b>53</b>
7.7.1	Sensibilisation des utilisateurs à la sécurité informatique .....	53
7.7.2	Sécurité du système - Droits d'accès (hiérarchisation des accès, ...).....	53
7.7.3	Délai de verrouillage après inactivité .....	53
<b>7.8</b>	<b>Procédures en cas de panne informatique : mode dégradé .....</b>	<b>54</b>

<b>7.9</b>	<b>Traçabilité, Intégrité et Conservation des données</b>	<b>55</b>
7.9.1	Traçabilité des données	55
7.9.2	Intégrité des données	55
7.9.3	Archivage des données	55
7.9.4	Archivage des demandes et des comptes rendus	55
7.9.4.1	Archivage/désarchivage des demandes d'examens en ligne	56
7.9.4.2	Archivage des compte rendus dans leur format de diffusion	56
7.9.5	Cas d'un changement de SIL	57
7.9.6	Cas spécifique du séquençage	57
<b>7.10</b>	<b>Sauvegarde des données</b>	<b>57</b>
7.10.1	Types de sauvegarde	57
7.10.2	Supports de sauvegarde	58
7.10.3	Fréquence des sauvegardes	58
7.10.4	Sauvegarde et hébergement de données de santé	58
<b>8</b>	<b>VALIDATION ET VERIFICATION DES SYSTEMES INFORMATIQUES</b>	<b>59</b>
<b>8.1</b>	<b>Données fournisseurs (marquage CE DM DIV)</b>	<b>59</b>
<b>8.2</b>	<b>Vérification du paramétrage (examens, textes codés, connexions, règles)</b>	<b>59</b>
8.2.1	Examens	60
8.2.2	Textes ou commentaires codés	61
8.2.3	Vérification des connexions	61
8.2.4	Vérification des règles de gestion des examens	61
8.2.5	Vérification des alarmes transmises par les analyseurs	61
8.2.6	Format de rendu du résultat	62
8.2.6.1	Chiffres significatifs	62
8.2.6.2	Règles d'arrondissement	62
<b>8.3</b>	<b>Vérification initiale (ou intégration fonctionnelle)</b>	<b>62</b>
<b>8.4</b>	<b>Vérification après changement de version (ou non régression fonctionnelle)</b>	<b>63</b>
<b>8.5</b>	<b>Vérification continue (dont signalement vigilance)</b>	<b>64</b>
8.5.1	Vérification du paramétrage	64
8.5.2	Vérification du paramétrage des règles	64
8.5.3	Vérification des sauvegardes et de l'archivage	64
8.5.4	Transmissions des résultats des examens spécialisés	64
8.5.5	Suivi des droits	65
8.5.6	Cas des logiciels de bureautique	65
<b>9</b>	<b>ANNEXES</b>	<b>66</b>
<b>9.1</b>	<b>Annexe 1 : exemple de convention de preuve</b>	<b>66</b>
<b>9.2</b>	<b>Annexe 2 : exemple de fiche de fonction de responsable informatique du LBM</b>	<b>67</b>
<b>9.3</b>	<b>Annexe 3 : Exemple de charte informatique</b>	<b>68</b>
<b>9.4</b>	<b>Annexe 4 : exemples de formulaires de paramétrage</b>	<b>71</b>
<b>9.5</b>	<b>Annexe 5 : exemple de vérification de connexions par visualisation des fichiers transmis par l'analyseur</b>	<b>79</b>
<b>9.6</b>	<b>Annexe 6 : exemple d'un test des règles d'un MW</b>	<b>81</b>
<b>9.7</b>	<b>Annexe 7 : exemple de vérification de transmission des codes alarmes des analyseurs</b>	<b>82</b>
<b>9.8</b>	<b>Annexe 8 : exemple de test de cohérence des données transmises</b>	<b>83</b>
<b>9.9</b>	<b>Annexe 9 : exemple de vérification de non régression fonctionnelle</b>	<b>84</b>
<b>9.10</b>	<b>Annexe 10 : exemple d'enregistrement des traçabilités des logiciels</b>	<b>85</b>
<b>9.11</b>	<b>Annexe 11 : exemple de formulaire de vérification des transferts de données</b>	<b>85</b>
<b>9.12</b>	<b>Annexe 12 : Analyse de risques appliquée aux systèmes informatiques des LBM</b>	<b>86</b>
<b>10</b>	<b>BIBLIOGRAPHIE</b>	<b>92</b>

## 1 OBJET DU DOCUMENT

La norme NF EN ISO 15189 définit les exigences particulières concernant la qualité et la compétence, pour les Laboratoires de Biologie Médicale. Quant à la norme NF EN ISO 22870, elle définit les exigences concernant la qualité et la compétence pour les examens de biologie médicale délocalisés (EBMD).

Dans le présent guide les Laboratoires de Biologie Médicale et toutes autres structures accréditées ou candidates à l'accréditation selon ces référentiels sont appelées « LBM ».

Le présent Guide Technique d'Accréditation (GTA) définit les recommandations relatives à l'application de ces référentiels en matière de maîtrise des moyens informatiques et de dématérialisation des données au sein des LBM concernés par les référentiels précités.

Les recommandations présentées dans ce guide, que le LBM est libre d'appliquer, sont celles reconnues par le Cofrac comme étant appropriées pour répondre aux prescriptions et exigences des normes NF EN ISO 15189 et NF EN ISO 22870, ainsi qu'au document Cofrac [SH REF 02](#) correspondant. Toute autre démarche argumentée et documentée est cependant acceptable. Dans tous les cas, il appartient au LBM de démontrer que les dispositions prises permettent de satisfaire pleinement aux exigences de la norme utilisée.

En effet, le phénomène d'informatisation et de dématérialisation, favorisé par les évolutions technologiques, conduit à une évolution profonde des organisations et des modes de production. Les LBM sont, dans ce cadre, conduits à mettre en œuvre des méthodes et des outils nouveaux. Cette « révolution numérique » concerne bien évidemment le compte rendu d'examens de biologie médicale émis par le LBM mais également tout le processus du traitement de l'information mis en œuvre au sein du LBM. L'enjeu pour les LBM est donc de savoir quelles politiques et quelles pratiques mettre en œuvre en regard de ce mouvement d'informatisation. L'objectif est toujours de satisfaire aux exigences du référentiel en tirant partie de l'informatisation et de la dématérialisation pour augmenter le niveau de performance de l'organisation.

La **maîtrise des moyens informatiques** (matériels et logiciels) dans les LBM est à considérer au même titre que tous les autres équipements d'analyses en transposant à leur utilisation les exigences du référentiel.

## 2 TERMINOLOGIE ET REFERENCES

Pour les besoins du présent document, les termes et définitions ci-après s'appliquent. Ces définitions sont issues notamment de normes internationales se rapportant à l'accréditation ou de documents du Cofrac.

### 2.1 Définitions

**Aliquotage** : action de répartir en différentes fractions, ou parties aliquotes, un ou des spécimens de liquide(s) biologique(s). Du latin : aliquot « un certain nombre de ».

**Aliquot** : une partie aliquote.

**Analyse** (d'après NF EN ISO 15189) : en biologie médicale, correspond à la phase analytique de l'examen de biologie médicale. Un examen comporte une ou plusieurs analyses. L'exécution de chacune produit un ou plusieurs résultats qui concourent au compte rendu des résultats de l'examen.

Une analyse peut être identifiée par un code LOINC dans les échanges de données comportant des résultats d'examens et dans les comptes rendus d'examens électroniques.

**Analyse réflexe** : analyse additionnelle déclenchée en fonction du résultat d'autres analyses, soit manuellement, soit automatiquement en fonction d'algorithmes et de critères prédéfinis. Les anglo-saxons parlent de « reflex test ».

**Analyseur** : automate (voir ce terme) permettant de déterminer la nature et/ou la concentration d'un ou plusieurs constituants d'un spécimen selon un mode opératoire défini. L'analyseur exécute des analyses sur le spécimen et produit, pour chacune, un ou plusieurs résultats. L'analyseur peut être sur un plateau technique du LBM ou délocalisé à l'extérieur, par exemple dans une unité de soins.

**Annuaire** : structure regroupant des informations (identité, adresse, coordonnées, ...) sur une catégorie d'acteurs (professionnels de santé, établissements de santé, services d'un établissement, personnel du LBM, ...) ou d'objets (systèmes, automates, sites webs, ...)

**Archivage en ligne des demandes d'examen** : opération consistant à clore les demandes d'examens pour lesquelles le travail est terminé. Ces demandes restent accessibles dans le SIL mais ne sont plus dans le circuit de production et ne sont plus modifiables, en dehors d'une procédure dédiée (remise en encours pour modifications).

**Archivage des comptes rendus dans leur format de diffusion** : le compte rendu diffusé sous forme papier ou électronique est archivé sous son format de diffusion pour conserver un élément majeur de la preuve légale du rendu de résultats.

**Auditabilité** : aptitude à fournir à une autorité compétente la preuve que la conception et le fonctionnement du système et de ses contrôles internes sont conformes aux exigences.

**Automate** : dispositif réalisant une ou plusieurs opérations de façon automatique.

En biologie, un automate réalise des opérations sur un spécimen. Ce peut être un appareil robotique réalisant des opérations pré ou post analytiques, ou un analyseur (voir ce terme).

**Biothèque** : dispositif de conservation de spécimens biologiques qui peuvent être de diverses natures : liquides, tissus, cellules, ADN, ... Une biothèque de conservation de spécimens de sérums sanguins s'appelle une sérothèque.

**Cluster** : Architecture informatique regroupant en réseau plusieurs ordinateurs ("computer") indépendants, formant des nœuds ("node"), afin de permettre une gestion globale et de dépasser les limitations d'un ordinateur pour :

- augmenter la disponibilité ;
- faciliter la montée en charge ;
- permettre une répartition de la charge, chacun des nœuds restant capable de fonctionner indépendamment des autres (par exemple en cas de défaillance d'un nœud).

**Demande d'examens** : objet informatique traduisant dans le SIL une prescription d'examens de biologie médicale. Le terme de "*demande d'examens*" est choisi de préférence à celui de "*dossier*" jugé trop ambigu. L'exécution d'une demande d'examens produit un compte rendu d'examens qui rassemble, commente et interprète l'ensemble des résultats obtenus pour cette demande.

**Domaine d'identification** : structure possédant un système informatique attribuant un numéro unique d'identification d'un patient, ce domaine peut-être un établissement de santé, un LBM, la caisse primaire d'assurance maladie, ...

**Dossier administratif d'établissement** : ensemble des données se rapportant à un séjour ou à une venue en consultation externe d'un patient dans un établissement de soins, et identifié par un numéro unique à l'échelle de l'établissement : le NDA ou l'IEP (voir la définition de ces abréviations).

**Dossier patient** : ensemble des données se rapportant à un même patient, enregistrées dans un système informatique (par exemple dans un SIH ou un SIL).

**Examen** (Cf. article L. 6211-1 et L.6211-2 du CSP) : un examen de biologie médicale est un acte médical qui concourt à la prévention, au dépistage, au diagnostic ou à l'évaluation du risque de survenue d'états pathologiques, à la décision et à la prise en charge thérapeutiques, à la détermination ou au suivi de l'état physiologique ou physiopathologique de l'être humain.

Note 1 : un examen de biologie médicale comprend l'ensemble des phases pré-analytiques, analytiques et post-analytiques au sens des normes NF EN ISO 15189 et NF EN ISO 22870.

Note 2 : La phase analytique décompose l'examen en une ou plusieurs analyses (voir ce terme).

**Identifiant de patient et domaine d'identification** : un identifiant de patient est associé à un domaine d'identification : L'ASIP Santé pour l'INS-c, l'établissement qui a attribué cet identifiant pour un IPP ou un identifiant de dossier administratif d'établissement, le LBM pour l'identifiant attribué au patient par le SIL. L'identifiant est utilisable par les systèmes associé à son domaine d'identification.

**Intégration fonctionnelle** : installation d'une nouvelle fonctionnalité locale à un système ou en interaction avec d'autres systèmes.

**Jeu test** : ensemble d'exemples de données entrant dans la procédure de qualification/vérification informatique d'une fonctionnalité locale à un système ou en interaction avec d'autres systèmes.

**Marquage CE DM DIV** : Les dispositifs médicaux de diagnostic in vitro ont l'obligation de répondre à des exigences essentielles qui permettent de garantir :

- la sécurité du patient : qualité du résultat ;
- la sécurité des utilisateurs et des biens :
  - innocuité des réactifs et des instruments,
  - identification des dangers.

Le marquage CE indique que ces exigences ont été respectées.

Ce marquage est réglementaire. Il consiste en une auto-certification de conformité d'un dispositif médical de diagnostic in vitro (DM DIV) aux exigences essentielles définies par la directive européenne 98/79 CE. Pour les DM DIV de l'annexe II de la directive une vérification du marquage par un organisme notifié est nécessaire.

**Non régression fonctionnelle** : vérification de la préservation d'une fonctionnalité locale à un système ou en interaction avec d'autres systèmes, suite à une mise à jour du logiciel de l'un des systèmes.

**Passerelle d'échange** : système intermédiaire d'échange de données entre le SIL et l'environnement extérieur. Une passerelle peut permettre d'émettre ou de recevoir des demandes d'examen, des résultats d'examen, des comptes rendus. Elle peut aussi servir à recevoir les données d'identités et mouvements des patients des établissements. Ce système est dans le périmètre et sous la responsabilité du LBM ou de l'établissement qui le contient. Il peut accomplir des conversions de format avant transmission ou en réception. Il peut disposer de différents moyens d'acheminement (messagerie sécurisée de santé, transfert de fichiers, transactions IHE ...).

**Prélèvement** : action de recueil d'un spécimen (ou échantillon biologique) par un préleveur

**Préleveur** : rôle fonctionnel joué par un agent de santé (IDE, médecin, technicien, biologiste ...), qui prélève des spécimens.

**Recette d'intégration** : document validant la réception d'une intégration fonctionnelle ou d'une non-régression fonctionnelle. A noter : Le marquage CE DM DIV intègre cette notion.

**Repasse** (contrôle, repassage) : réexécution d'une analyse sur un spécimen, déclenchée pour contrôle du résultat produit par la (ou les) exécution(s) précédente(s) de cette même analyse sur ce même spécimen. Le déclenchement peut être volontaire ou automatique suivant des critères prédéfinis. Les anglo-saxons parlent de « re-run » ou « new run ».

**Serveur de résultats** : système concentrant des résultats et/ou des comptes rendus d'examens sous forme électronique, et offrant aux destinataires de ces résultats et de ces comptes rendus des interfaces de diffusion et/ou de consultation. Ce système peut être dans le périmètre d'un LBM ou d'un établissement, ou bien externe et alimenté par plusieurs LBM. Dans ce dernier cas, il s'agit d'un SISP soumis à l'obligation d'agrément d'hébergeur de données de santé.

**Site** : unité géographique et fonctionnelle du LBM.

Note : dans la norme NF EN ISO 15189, le terme site comprend tous les sites dont le LBM est responsable, c'est-à-dire les sites au sens du CSP, ainsi que les lieux de réalisation de prélèvements (par exemple domicile du patient) ou de "biologie délocalisée" au sens de la norme NF EN ISO 22870.

**Spécimen** (d'après NF EN ISO 15189) : pour éviter une confusion avec le terme échantillon (au sens : groupe d'individus extrait d'une population), il est préféré le terme "spécimen" pour désigner une ou plusieurs parties issues d'un prélèvement biologique (spécimen de sang, spécimen urinaire, ...). Correspond à l'"échantillon biologique" au sens du CSP.

**Spécimen primaire** versus **spécimen secondaire** : le spécimen primaire est recueilli sur le patient. Le spécimen secondaire est un sous-produit du spécimen primaire obtenu par décantation, aliquotage, dilution, ...

**Tiers** : ce terme s'applique à l'ensemble des partenaires pouvant échanger de l'information avec le LBM. Exemples : médecin, organisme payeur, établissement de soins, service, LBM sous-traitant ...

**Validation** (ou validation biologique) : opération de contrôle de la vraisemblance et de la cohérence de l'ensemble des résultats d'une demande d'examens, dans le contexte du dossier patient, confrontant cet ensemble de résultats avec les résultats antérieurs disponibles et avec les éléments cliniques pertinents disponibles (état clinique du patient, motif de la demande d'examens, traitements mis en œuvre ...).

La validation des résultats de la demande produit ou confirme dans le même temps l'interprétation contextuelle de ces résultats qui figurera dans le compte rendu d'examens.

## 2.2 Abréviations

- **ADSL** : Asymmetric Digital Subscriber Line : technique de communication numérique sur ligne téléphonique, mise en œuvre par les fournisseurs d'accès à internet. Comme son nom l'indique, la technologie ADSL fournit un débit asymétrique (contrairement à la technologie SDSL). Le flux de données est plus important dans un sens de transmission que dans l'autre.
- **AFNOR** : Agence Française de Normalisation.
- **ANSM** : Agence Nationale de Sécurité du Médicament.
- **ASIP Santé** : Agence des Systèmes d'Information Partagée de Santé.
- **CDA** : Clinical Document Architecture est le standard de document médical électronique structuré produit par HL7.
- **CE** : Communauté Européenne.
- **CIQ** : Contrôle Interne de Qualité.
- **CI-SIS** : Le Cadre d'Interopérabilité des Systèmes d'Information de Santé est un corpus de référentiels maintenu et publié par l'ASIP Santé pour les échanges et le partage de données dématérialisées entre systèmes d'information du domaine de la santé. Ce corpus s'appuie sur des profils IHE et des standards internationaux tels que HL7 CDA ou LOINC.
- **CPS** : Carte électronique de Professionnel de Santé.
- **CPx** : Famille des cartes professionnelles électroniques (CPS, ...).

- **CSP** : Code de la Santé Publique.
- **DM DIV** : Dispositif Médical de Diagnostic In Vitro.
- **DMP** : Dossier Médical Personnel. Le système DMP est un SISP.
- **DMZ** : une zone démilitarisée (ou DMZ, de l'anglais Demilitarized Zone) est un sous-réseau séparé du réseau local par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accessibles depuis Internet.
- **DSI** : Directeur/trice/tion des Systèmes d'Information.
- **EBMD** : Examen de Biologie Médicale Délocalisée (en dehors du LBM, par exemple dans une unité de soins).
- **EEQ** : Evaluation Externe de la Qualité.
- **EFS** : Etablissement Français du Sang.
- **EN** : Norme Européenne. L'organisme de diffusion de ces normes en France est l'AFNOR.
- **FTP** : File Transfer Protocol : Protocole de transfert de fichier sur un réseau TCP/IP.
- **HL7** : Health Level Seven (HL7) est une organisation internationale produisant des standards d'interopérabilité pour le domaine de la santé.
- **IDE** : Infirmier/infirmière diplômé(e) d'état.
- **IEP** : Identification Externe du Patient, système qui attribue un numéro différent à chaque venue du patient à l'hôpital (hospitalisation), contrairement à l'IPP qui reste identique puisque "attaché" à une identité.
- **IHE** : Integrating the Healthcare Enterprise : organisation internationale produisant des profils de standards pour les échanges de données électroniques entre systèmes d'information du domaine de la santé.
- **IHE LAW** : Laboratory Analytical Workflow. Profil d'intégration des échanges de données entre analyseurs et MW ou SIL.
- **IHE LCSD** : Laboratory Code Set Distribution. Profil d'intégration des échanges de données liés à la diffusion du manuel de prélèvement sous une forme dématérialisée et structurée.
- **IHE LPOCT** : Laboratory Point Of Care Testing. Profil d'intégration des échanges de données liés à la biologie délocalisée.
- **IHE LTW** : Laboratory Testing Workflow. Profil d'intégration des échanges de données liés à la prescription connectée.
- **IHE PAM** : Patient Administration Management. Profil de diffusion des données démographiques des patients d'un établissement.
- **IHE PDQ** : profil d'interrogation des données démographiques des patients d'un établissement.
- **INS** : Identifiant National de Santé d'un patient. Cet identifiant de portée nationale est disponible pour les bénéficiaires de l'assurance maladie. On l'appelle aussi INS-C. Il est calculé par un système au moment de la lecture de la carte Vitale, à partir des traits d'identité lus en carte. Il peut ensuite être conservé dans le système et communiqué d'un système à l'autre.  
L'INS est une donnée personnelle. Ce n'est pas une donnée médicale. C'est un trait d'identité qui n'a rien de confidentiel, au même titre que le nom de famille de la personne.

Un SIL peut obtenir l'INS d'un patient de trois façons :

1. par lecture directe de la carte Vitale du patient,
2. dans un message électronique transmis par un autre système,
3. par lecture d'un code barre sur la feuille de prescription ou sur un document l'accompagnant.

▪ **InVS** : Institut National de Veille Sanitaire

▪ **IPP** : Identifiant Permanent du Patient, attribué à un patient lors de sa première venue dans un établissement, par le système de gestion des patients de cet établissement. Ce N° reste valide lors des hospitalisations successives, contrairement à l'IEP qui change à chaque hospitalisation. On parle aussi de NIP.

▪ **IVD** : In Vitro Diagnostic (en français DIV : Diagnostic In Vitro).

▪ **Kermit** : Protocole de transfert de fichiers point à point dont l'usage tend à disparaître.

▪ **LBM** : Laboratoire de Biologie Médicale (article L.6212-1 du CSP) : Structure, privée ou publique, au sein de laquelle sont effectués les examens de biologie médicale. Le LBM est constitué d'un ou plusieurs sites. Le Laboratoire de Biologie Médicale peut également réaliser des activités biologiques d'assistance médicale à la procréation ainsi que des examens d'anatomie et de cytologie pathologiques.

▪ **LDAP** : Lightweight Directory Access Protocol est, à l'origine, un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication.

▪ **LGC** : Logiciel de Gestion de Cabinet médical.

▪ **LOINC** : Logical Observation Names and Codes est une nomenclature internationale, permettant la codification des résultats d'examens, notamment ceux de biologie médicale, pour les échanges de ces résultats sous forme dématérialisée, entre systèmes d'information. La licence d'utilisation de LOINC est gratuite. LOINC traduite en français est mise en accès public par l'ASIP Santé.

▪ **MPLS** : MultiProtocol Label Switching est un mécanisme de transport de données basé sur la commutation d'étiquettes ou "labels".

▪ **MSSanté** : Système des messageries sécurisées de santé instituant un espace de confiance regroupant des domaines de messagerie autorisés, une sécurisation du canal d'échange, des utilisateurs certifiés et authentifiés référencés dans un annuaire national partagé.

▪ **MW** : Un Middleware est un système de gestion de plateau technique ou d'un sous-ensemble de celui-ci, et/ou d'un ensemble d'analyseurs délocalisés par exemple dans les unités de soins.

▪ **NDA** : Numéro de Dossier Administratif : Identifie de façon univoque le dossier administratif d'un séjour ou d'une consultation externe d'un patient dans un établissement. Le NDA est exploitable dans le contexte de son domaine d'identification représenté par l'établissement.

▪ **NF** : Norme Française. L'organisme de diffusion de ces normes est l'AFNOR.

▪ **NIP** : Numéro d'Identification Permanent attribué à un patient lors de sa première venue dans un établissement, par le système de gestion des patients de cet établissement. Ce numéro reste valide lors des hospitalisations successives, contrairement à l'IEP qui change à chaque hospitalisation. On parle aussi d'IPP.

▪ **PFS** : Plateforme de services d'un fournisseur d'analyseurs.

- **SaaS** : Le logiciel en tant que service ou en anglais le Software as a Service est un concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence. Les ressources (données, application, serveurs ...) sont externalisées.
- **SAV** : Service Après-Vente d'un fournisseur du LBM.
- **SAVB** : Système d'Aide à la Validation Biologique.
- **SDSL** : Symmetric Digital Subscriber Line. Technique de communication numérique sur ligne téléphonique, mise en œuvre par les fournisseurs d'accès à internet. Comme son nom l'indique, la technologie SDSL fournit un débit asymétrique (contrairement à la ligne ADSL): son débit en réception (download) est égal au débit en émission (upload).
- **SFBC** : Société Française de Biologie Clinique.
- **SFIL** : Société Française d'Informatique de Laboratoire.
- **SIH** : Système d'Information Hospitalier.
- **SIL** : Système Informatique de gestion du Laboratoire.
- **SIQ** : Système d'Information du management de la Qualité du laboratoire.
- **SISP** : Système d'Information de Santé Partagé entre le LBM et d'autres organisations ou professionnels de santé. Un serveur de résultats de biologie entre dans cette catégorie. Le DMP est un SISP de portée nationale.
- **SMQ** : Système de Management de la Qualité.
- **TCP/IP** : Protocole des couches liaison, réseau et transport sur lequel s'appuie le réseau internet et la quasi-totalité des réseaux locaux.
- **UF** : Unité Fonctionnelle.
- **VPN** : Le réseau privé virtuel (Virtual Private Network en anglais) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel » avec cryptage des données de bout en bout.
- **XP Z 10-011** : Norme de présentation des adresses géopostales, publiée par l'AFNOR.

### 3 DOMAINE D'APPLICATION

Le domaine d'application du présent guide concerne le cadre spécifique de la maîtrise des moyens informatiques et de dématérialisation des données au sein des LBM.

En particulier, le présent guide s'attache à couvrir le champ du processus de traitement et de transmission informatique depuis la production de la donnée jusqu'à son archivage, ainsi que la gestion des moyens informatiques mis en œuvre.

Ce guide correspond à l'état de la réglementation et de la normalisation au jour de sa publication. Il s'agit d'une première version qui présente un état des lieux des bonnes pratiques et établit certaines recommandations dans le cadre de l'accréditation. Toutefois, s'agissant d'une première version certains aspects ne sont pas encore développés. Ce guide sera également régulièrement revu en correspondance de l'évolution des textes réglementaires. Ainsi, il n'a pas été développé dans cette version la signature électronique et la signature électronique présumé fiable.

Ce guide s'adresse :

- Aux Laboratoires de Biologie Médicale (LBM) et autres structures engagés dans une démarche d'accréditation Cofrac selon les normes NF EN ISO 15189 et NF EN ISO 22870 ; dans ce cas il représente des recommandations, toute autre démarche argumentée et documentée étant cependant acceptable ;
- Aux membres des instances du Cofrac (Comité de Section, Commission Technique d'Accréditation Santé Humaine) ;
- Aux évaluateurs du Cofrac, et constitue une base d'harmonisation à leur usage ;
- Aux fournisseurs, pour comprendre et aider les LBM et autres structures dans leur démarche.

## 4 MODALITES D'APPLICATION

Le présent guide technique d'accréditation est applicable à compter du **15 juillet 2013**.

Dans le domaine considéré de la biologie médicale, et au jour de son approbation, ce guide technique d'accréditation reflète l'état d'avancement des connaissances en termes de préconisations pour l'accréditation dans ce domaine.

## 5 SYNTHÈSE DES MODIFICATIONS

S'agissant de la première version du document, qui porte l'indice de révision 00, aucune marque de modification n'est donc indiquée.

## 6 RECENSEMENT ET TYPOLOGIE DES ARCHITECTURES DE SYSTEMES

### 6.1 Introduction

Ce chapitre recense et classe les architectures de systèmes d'information que l'on peut rencontrer dans les LBM, avec leurs déclinaisons matérielles, logicielles, connectiques et applicatives.

Le chapitre recense et classe aussi les échanges de données que l'on peut rencontrer entre applications au sein du LBM et avec les applications extérieures. Ces échanges sont présentés dans le contexte des processus métiers qu'ils sous-tendent.

Le chapitre met l'accent sur les opérations et les échanges informatisés, mais signale aussi autant que de besoin les modes dégradés et les circuits manuels qui peuvent exister.

Ce recensement est délimité par le périmètre du volet informatique de la norme NF EN ISO 15189. Il se limite aux systèmes impliqués dans le cycle de production du LBM qui s'étend des phases pré-analytiques au rendu des résultats. En particulier les systèmes, composants, applications, échanges de données touchant la facturation sont hors champ du présent guide.

L'architecture des systèmes d'information peut se décliner sous trois aspects :

- L'architecture des serveurs qui comprend le SIL, et souvent aussi d'autres serveurs entrant dans la chaîne de production du LBM ;
- L'architecture des terminaux et celle des réseaux, cette dernière méritant une attention particulière dans les LBM multi-sites ;
- L'architecture applicative et les échanges de données entre applications.

Les sections suivantes de ce chapitre présentent successivement ces trois aspects.

## 6.2 Architecture des serveurs

Il faut différencier deux niveaux de criticité des serveurs :

- Les serveurs qui sont sur le chemin critique du cycle de production du LBM (du pré-analytique au rendu de résultats) et/ou qui stockent des données médicales à caractère personnel des patients (SIL, MW, ...) soumis à des contraintes clairement exprimées en termes de disponibilité, intégrité et confidentialité des données, auditabilité des opérations, ainsi qu'en termes de conditions d'exploitation (local sécurisé et climatisé, ...)
- Les serveurs qui sont en support (serveur du SIQ, serveur de supervision du parc matériel, ...) mais qui ne sont pas sur le chemin critique et qui ne contiennent pas de données médicales à caractère personnel.

### 6.2.1 Les serveurs non critiques

Un serveur est non critique si son arrêt physique n'impacte pas la chaîne de production du LBM et s'il ne contient pas de données médicales à caractère personnel.

Pour les serveurs non critiques, les vérifications à faire se limitent :

- Au contrat de maintenance des serveurs ;
- A la sauvegarde effective, périodique de ces serveurs, (périodicité définie dans le SMQ).

### 6.2.2 Les serveurs critiques

Les serveurs critiques d'un LBM sont en général les suivants :

- Les SIL ;
- Les MW ;
- Les analyseurs et leurs systèmes auxiliaires (console analytique, système d'interprétation/expertise des résultats bruts) ;
- Les systèmes d'aide à la validation biologique ;
- Les serveurs de résultats alimentés avec les résultats d'examens produits par le LBM ;
- Les passerelles d'échange ;
- ...

C'est sur ces serveurs que se focalise l'attention du LBM.

La taille et le type de structure du LBM justifient pour chacun des serveurs critiques une étude préalable de gestion de risques en cas de coupure informatique de longue durée. Les moyens à mettre en œuvre devront être raisonnés et adaptés aux contraintes de chacun des serveurs critiques afin d'assurer l'efficacité du LBM dans la permanence des soins (urgences) et dans le service rendu aux patients.

### 6.2.3 Rappel des recommandations de la norme NF EN ISO 15189 sur l'architecture serveur

Aux recommandations de la norme NF EN ISO 15189 (paragraphe B2 de l'annexe B) et à leurs implications exposées dans cette section, s'ajoutent les contraintes de la loi concernant l'hébergement des données de santé exposées plus loin dans la section 6.2.5.

### 6.2.3.1 Sécurité des locaux

#### 6.2.3.1.1 Locaux « serveurs »

- Dans le cas d'un hébergement sur un seul site, afin de réduire les risques tout en maîtrisant les coûts et les performances, il est préférable que les serveurs soient redondés physiquement et/ou logiquement, et placés dans des pièces éloignées, avec un plan de reprise.
- Il existe une protection contre les incendies.
  - Les murs et plafonds peuvent utiliser des matériaux retardant la propagation d'un incendie extérieur.
  - Les salles peuvent être équipées d'un système d'extinction automatique d'incendie ne détériorant pas les composants informatiques.
- Les câbles sont protégés s'ils sont dans un endroit de passage.
- Le site est équipé d'un système de sécurisation d'alimentation électrique.
  - Onduleurs permettant d'alimenter les serveurs critiques le temps nécessaire à l'arrêt des systèmes.
  - En fonction du niveau de risque accepté, il peut être discuté de manière plus large de l'alimentation électrique des équipements critiques du LBM et de ses ressources informatiques jusqu'à envisager un investissement dans des onduleurs de grande capacité et/ou d'un groupe électrogène de taille proportionné.
- Les serveurs sont stockés dans un endroit conforme aux conditions fixées par le fournisseur. Ces conditions rendent souvent indispensable la mise en place d'une climatisation redondée.
- L'accès physique aux serveurs est impossible aux personnes non autorisées.
- Un système d'alarme peut être envisagé.

#### 6.2.3.1.2 Locaux informatiques des sites distants

Les routeurs et autres matériels informatiques critiques sont de préférence situés dans des locaux protégés, climatisés et permettant un contrôle d'accès maîtrisé.

### 6.2.3.2 Points clefs dans l'analyse de l'environnement

L'objectif est d'assurer une continuité de service et de gagner du temps en cas de panne bloquante ou de baisse de performances. A ce titre, les solutions de back-up font partie intégrante des solutions de continuité et de reprise d'activité.

- Une analyse de risque (Cf. annexe 12) permet de déterminer les points critiques du système informatique et de les sécuriser en regard des coûts induits de leur dysfonctionnement (redondance des accès « télécom », routeurs et autres matériels éventuellement pré-paramétrés).
- Les solutions techniques de redondance matériels et logiciels tiennent compte de contraintes d'architecture du système informatique (virtualisation, cluster, ...).
- Les administrateurs réseaux, référents informatiques ou référents techniques (titulaires et suppléants) sont régulièrement formés et testent à intervalles réguliers, en réel si possible, en période de faible activité et dans un environnement maîtrisé, les solutions préalablement définies dans le cadre d'un plan de continuité d'activité.
  - Conduite à tenir en cas de panne électrique de longue durée.
  - Conduite à tenir en cas de basculement sur groupe électrogène ou onduleur.

### 6.2.3.3 Pannes matérielles et logiciels

- Un logiciel de supervision du système informatique (réseau, connexions physiques et logiques, systèmes et applications) peut être mis en œuvre, en interne ou en externe.
- Les contrats de maintenance et la disponibilité des équipes techniques sont en adéquation avec les délais de reprise attendus.
- La gestion de la sécurité prend en compte les risques de détérioration d'origine externe et interne des systèmes et des données.

### 6.2.4 Typologie d'hébergement des serveurs critiques

Les différentes formes d'hébergement des serveurs critiques que l'on rencontre sont :

- Hébergement sur un site du LBM dans un endroit non sécurisé (exemple sur le plateau technique, dans un local ouvert, à l'accueil, ...). Ce type d'hébergement n'est pas recommandé au vu des risques auxquels il expose la confidentialité et l'intégrité des données patients (vol des serveurs ou des disques, intrusion sur le serveur et altération ou copie des données ...).
- Hébergement sur un site du LBM dans un endroit à accès sécurisé mais sans dispositif anti-feu et/ou sans onduleur (secours électrique) et/ou sans climatisation redondée. Ce type d'hébergement n'est pas recommandé au vu des risques auxquels il expose la disponibilité du système. Cependant, le dispositif anti-feu n'est pas indispensable si, par exemple, le LBM dispose d'un cluster de deux serveurs répartis sur deux sites différents dans deux salles sécurisées différentes. Egalement, le cas d'une salle serveur avec une seule climatisation est acceptable si une climatisation mobile de secours peut être utilisée, ...
- Hébergement des serveurs dans la salle machine d'un autre LBM non agréée comme hébergeur de données de santé. Ce type d'hébergement n'est pas conforme à la réglementation sur l'hébergement de données de santé (voir §6.2.5) et de plus expose le LBM au risque de perte de son outil informatique en cas de cession du LBM hébergeur (en particulier sur la propriété intellectuelle du paramétrage des examens).
- Hébergement sur un site du LBM dans une salle répondant aux recommandations des fournisseurs, avec accès sécurisé. Ce type d'hébergement est, entre autres, conforme à la norme.

*Si l'accès à la salle serveur est contrôlé par un dispositif électronique, il est important de vérifier qu'en cas de coupure électrique, l'accès à la salle serveur est toujours possible.*

- Hébergement dans deux salles sécurisées suivant les recommandations des fournisseurs, réparties entre deux sites du LBM, avec dispositif de réplication temps réel ou régulier. Ce type d'hébergement est également conforme à la norme, à condition que les deux salles disposent d'un accès sécurisé. Si l'une au moins des deux salles n'a pas de contrôle d'accès le LBM se retrouve exposé à des risques de confidentialité, d'intégrité, de disponibilité.
- Hébergement chez un hébergeur agréé. Cet autre type d'hébergement est conforme. Le contrat entre le LBM et l'hébergeur précise les engagements de ce dernier pour assurer la sécurité, en particulier concernant la disponibilité et la confidentialité, ainsi que les modalités de restitution des données au LBM en fin de contrat.

## 6.2.5 Agrément de l'hébergeur des données

Les dispositions relatives à l'agrément pour l'hébergement de données de santé à caractère personnel s'appliquent aux activités de biologie médicale.

Les contraintes d'agrément de l'hébergeur de données de santé d'un LBM ne seront à vérifier, dans le cadre de l'accréditation, qu'à partir de la date fixée par le SH REF 02.

### 6.2.5.1 Rappel du cadre juridique

Le législateur a souhaité définir une nouvelle sphère de protection des données de santé à caractère personnel, notamment en encadrant leurs conditions d'hébergement.

L'article L 1111-8 du code de la santé publique dispose que « *les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée* ».

Les conditions d'hébergement de données de santé à caractère personnel sur support informatique ont été précisées par le décret 2006-6 du 4 janvier 2006 (codifié aux articles R 1111-9 à R 1111-15-1 du code de la santé publique).

Conformément à l'article L 1111-8 du code de la santé publique et au décret 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel, toute personne physique ou morale hébergeant des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic ou de soins pour le compte d'un tiers, doit être agréée par décision du ministre en charge de la santé qui se prononce après avis de la CNIL et d'un comité d'agrément (organe consultatif créé par le décret 2006-6 sus-cité).

Lorsque l'établissement de santé ou le professionnel de santé conserve par ses propres moyens et localement les données de santé de ses patients, il n'est pas soumis à la nécessité d'être agréé.

L'article L 1111-8 du code de la santé publique est d'interprétation large et vise toute structure de soins et de prise en charge de patients.

Par conséquent, lorsque le LBM conserve par ses propres moyens les données de santé des personnes qu'il prend en charge, il n'est pas soumis à l'agrément.

Lorsqu'une phase de l'examen de biologie médicale est confiée pour réalisation à un autre LBM, ce dernier devient destinataire des données afin de participer à l'examen de biologie médicale. En cette qualité il est donc tenu de conserver, y compris pour son propre compte les données de santé ainsi transmises. Cette qualité le distingue donc d'un hébergeur de données de santé soumis à agrément et qui conserverait pour le compte d'un tiers des données de santé à caractère personnel.

Référentiel de la procédure de demande d'agrément sur le site de l'ASIP Santé :

[www.esante.gouv.fr/services/referentiels/secureite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrement-des](http://www.esante.gouv.fr/services/referentiels/secureite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrement-des)

La liste à jour des hébergeurs agréés pour l'hébergement de données de santé à caractère personnel est disponible sur le site esante.gouv.fr :

<http://esante.gouv.fr/services/referentiels/secureite/hebergeurs-agrees>

## 6.2.5.2 Les cas soumis à la procédure d'agrément

### 6.2.5.2.1 Base de données confiée à un prestataire spécialisé dans l'hébergement de données

Lorsqu'un LBM souhaite confier l'hébergement des données de santé des patients qu'il prend en charge à un prestataire tiers, le LBM est tenu de faire appel à un hébergeur agréé à cet effet.

Nous pouvons citer à titre d'exemple :

- Le cas de l'utilisation d'une application externalisée chez un hébergeur, notamment d'une application en mode SaaS ;
- Le cas d'un serveur de résultats d'examens de biologie médicale hébergé par un prestataire tiers aux LBM participant à la réalisation de l'examen de biologie médicale ;
- Le cas d'une location d'espace de stockage numérique externalisé dans une infrastructure technique d'hébergement.

A contrario, l'externalisation de l'activité de mise sous pli des comptes rendus en tant que telle n'entraîne pas l'obligation d'agrément du prestataire. Le LBM porte cependant une attention particulière à la confidentialité des échanges.

### 6.2.5.2.2 SIL mutualisé entre deux LBM

Le LBM A et le LBM B décident de mutualiser leur SIL et de confier l'hébergement du SIL au LBM A.

Dans ce cas, le LBM B ne conserve aucune donnée de santé localement.

Si le LBM B prend également en charge des patients pour lesquels aucune phase de l'examen de biologie médicale n'est sous-traitée au LBM A, alors le LBM A joue le rôle d'hébergeur pour le compte du LBM B et est agréé à cet effet.

Un contrat d'hébergement de données de santé est conclu entre les deux LBM.

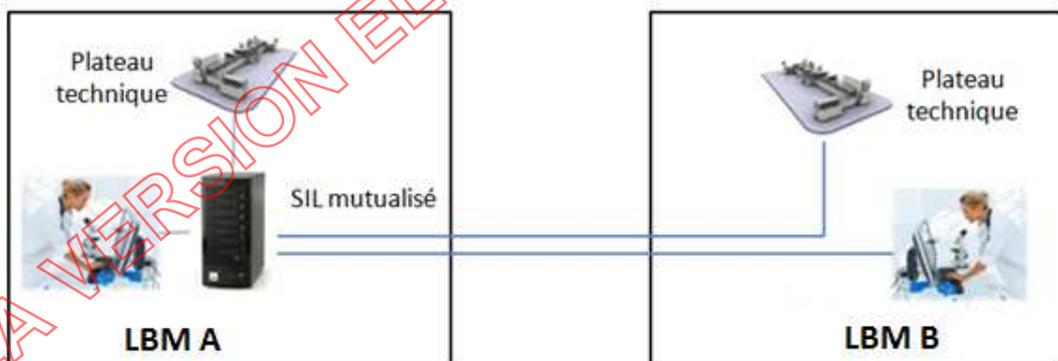


Figure 1: SIL mutualisé entre deux LBM

### 6.2.5.2.3 MW mutualisé entre deux LBM

Les LBM A et B exploitent chacun leur propre SIL, mais les deux LBM décident de mutualiser un MW (middleware).

Le LBM A est chargé de l'hébergement du MW.

Le MW hébergé par le LBM A reçoit et stocke des données de santé à caractère personnel de patients que le LBM A ne prend pas en charge dans le cadre de l'examen de biologie médicale.

Dans ce cas, le LBM A joue le rôle d'hébergeur pour le compte du LBM B et est agréé à cet effet.

Un contrat d'hébergement de données de santé est conclu entre les deux LBM.

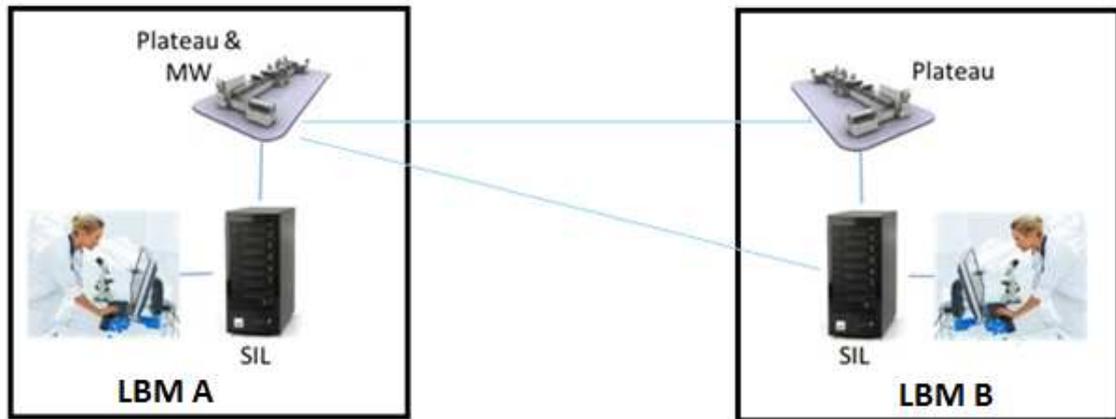


Figure 2: MW mutualisé entre deux LBM

#### 6.2.5.2.4 Serveur de résultats mutualisé entre deux établissements

Les LBM A et B utilisent un serveur de résultat commun hébergé par un des deux LBM.

Si ce serveur de résultat leur permet uniquement d'échanger des résultats de patients communs et donc pris en charge par les deux LBM, dans cette hypothèse, le LBM qui héberge le serveur de résultat n'est pas soumis à l'agrément.

En revanche, si ce serveur a vocation à contenir des données de patients qui ne sont pas pris en commun par les deux LBM, le LBM qui héberge le serveur est agréé pour l'hébergement de données de santé à caractère personnel.

### 6.3 Architecture terminaux et réseaux

L'architecture terminaux et réseaux comprend :

- Les terminaux locaux ;
- Le réseau local du site ;
- Le réseau inter-sites pour les LBM multi-sites ;
- Les connexions à distance.

Il est important de noter que la possibilité d'extraction de données patient d'un SIL depuis un terminal fait de ce terminal un matériel informatique contenant des données sensibles et qui donc nécessite un contrôle d'accès.

#### 6.3.1 Rappel des recommandations de la norme NF EN ISO 15189 sur les terminaux et réseaux

Les paragraphes de la norme NF EN ISO 15189 qui influent sur les terminaux sont :

- 5.1.7 et 5.3.11-d sur l'autorisation d'utilisation des ordinateurs du LBM ;
- B4.1 concernant la protection des programmes informatiques ;
- B4.3 sur le cloisonnement des applicatifs ;
- B5.8 sur l'identification des utilisateurs.

Le LBM pourra s'appuyer sur les points de sécurité de la norme simplifiée 53 de la CNIL qui demande la traçabilité des accès et des traitements sur toutes les données nominatives et le cryptage des échanges.

### 6.3.2 Typologie des terminaux

On distingue deux familles de terminaux installés dans les LBM :

- Les **terminaux passifs** qui ne contiennent localement aucune donnée. Ils peuvent être de différentes natures :
  - Terminaux en mode caractère connectés à un serveur (AS400, VMS, Unix,...). Ces terminaux n'ont pas un vrai système d'exploitation installé. Ils sont facilement identifiables puisqu'ils ne démarrent pas si la prise réseau est débranchée.
  - Les postes de travail virtualisés qui affichent une interface graphique Windows ou Linux exécutée sur un serveur (Microsoft Remote Desktop Protocol, Citrix, Vmware). Comme les terminaux précédents, ils ne démarrent pas si la prise réseau est débranchée.
- Les **postes intelligents** sont identifiables par la possibilité de travailler en local même si le réseau est débranché.
  - Les ordinateurs : portables ou de bureau, tablettes, smartphones, sous des systèmes d'exploitation variés (Windows, Linux, iOS, Android, ...), sur lesquels s'exécutent tout ou partie des applications.
  - Les ordinateurs portables ou de bureau, utilisés en émulation de terminal en mode caractère.
  - Les terminaux passifs émulant un poste de travail virtualisé.
  - Les postes de travail virtualisés sur un ordinateur disposant d'un système d'exploitation.

Les terminaux passifs bénéficient nativement d'un haut niveau de sécurité puisqu'aucune donnée ne peut être stockée sur le terminal et toute la sécurité repose sur le contrôle d'accès de l'utilisateur aux applications depuis le poste.

Il est très rare dans un LBM que tous les postes soient des terminaux passifs.

Il est courant que des extractions nominatives soient effectuées en dehors du SIL (liste épidémiologique, transmission de courrier ponctuel pour les patients ou prescripteurs,...) et stockées sur le poste de travail intelligent.

Il est fréquent que les postes intelligents ne soient pas soumis à une politique d'authentification similaire à celle du SIL ou des autres applicatifs contenant des données patient. Ceci n'est pas recommandé.

Si les locaux où se situe le poste intelligent sont ouverts au public ou à accès non contrôlé, il est recommandé de faire en sorte que les données stockées localement soient cryptées, pour se protéger du risque de divulgation d'information nominative en cas de vol du poste ou de son disque.

Dans tous les cas, il est recommandé de doter le poste intelligent d'un contrôle d'accès par authentification personnelle.

### 6.3.3 Typologie des réseaux locaux du site

Les quatre composantes importantes concernant le réseau local du site sont le réseau physique, le pare-feu, les anti-virus et la gestion des identités.

### 6.3.3.1 Réseau Physique

Il peut être soit filaire, soit Wifi, soit mixte.

Le réseau filaire bénéficie de la sécurité d'accès physique du site et de la sécurité du poste de travail.

Le réseau wifi peut être accessible depuis l'extérieur. C'est pourquoi il est recommandé de le sécuriser par une clé d'un niveau suffisant, et de mettre en place une procédure documentant le changement régulier de la clé wifi, pour protéger le réseau d'une intrusion par un ex-personnel du site.

On ne devrait pas pouvoir se connecter au réseau wifi depuis un portable ou un téléphone wifi non répertorié dans le réseau.

### 6.3.3.2 Anti-virus

Une bonne configuration anti-virus consiste en l'installation d'un serveur anti-virus en local qui distribue de manière régulière les mises à jour de signatures anti-virus sur les postes du réseau et qui offre la possibilité à un administrateur de superviser la bonne mise à jour des postes et l'homogénéité de la politique de sécurité.

De nombreux postes sont encore aujourd'hui protégés par des anti-virus gratuits. Or, la plupart des anti-virus gratuits sont trop peu performants pour une utilisation professionnelle dans le cadre des métiers de la santé.

Il existe quelques rares anti-virus gratuits performants mais limitant le nombre de postes (par exemple à 15 postes). Au-delà de cette limite le logiciel devient payant.

Il est recommandé de documenter la procédure de mise à jour de l'anti-virus et de vérification de son statut, et de communiquer cette procédure à l'ensemble des utilisateurs impliqués dans celle-ci.

Il existe aussi des sites avec des anti-virus professionnels installés localement sur les machines sans supervision. Dans ce cas, la mise à niveau de l'anti-virus est souvent réalisée manuellement par l'utilisateur qui dispose d'une procédure. Les risques sont d'avoir des anti-virus non à jour (donc vulnérables) et une dégradation des performances internet au moment du téléchargement simultané par tous les postes d'une nouvelle signature anti-virus.

Le LBM porte une attention particulière aux interactions entre antivirus et logiciels embarqués, notamment dans les dispositifs marqués CE, contribuant à l'élaboration des examens, pour éviter que les antivirus ne pénalisent trop fortement ces logiciels.

### 6.3.3.3 Pare-feu

Le pare-feu permet de réguler les flux réseau comme par exemple d'interdire à un équipement extérieur au réseau local de se connecter au réseau du site, de bloquer des flux réseau indésirables (vidéo par exemple).

Un pare-feu peut être embarqué sur un matériel, inclus avec un routeur réseau, assuré par l'opérateur ou par un logiciel installé sur un serveur. Lorsque le réseau du site comporte une sortie sur internet (pour les mails par exemple) ; le pare-feu permet de réguler tous les flux de/vers internet.

Si aucun logiciel n'est accessible de l'extérieur (pas de serveur de résultat interne par exemple), un seul pare-feu est suffisant dans le site.

S'il existe un serveur sur le réseau du site qui est accessible de l'extérieur, il est recommandé de mettre ce serveur dans une DMZ délimitée par deux pare-feu, l'un sur

l'arrivée internet, l'autre entre le serveur accessible de l'extérieur (serveur de résultat par exemple) et le réseau interne.

Un serveur accessible depuis internet mais hébergé chez un hébergeur agréé est, de fait, dans une DMZ.

Les pare-feu nécessitent des mises à jour régulières (contrat de maintenance).

#### 6.3.3.4 Gestion des identités utilisateurs

On distingue deux stratégies de gestion des identités : une approche centralisée et globale au réseau (LDAP) et une approche ad-hoc par application.

- La gestion d'un annuaire d'entreprise (LDAP) aussi appelé « gestionnaire de mot de passe » permet de créer un domaine de confiance interne à la structure juridique (LBM ou établissement). Pour avoir accès aux applications se situant dans le domaine de confiance chaque utilisateur est authentifié au regard des informations figurant dans l'annuaire d'entreprise. L'authentification peut se faire par carte CPx ou tout autre dispositif conforme à la politique de sécurité de la structure juridique comme un identifiant et mot de passe unique pour l'ensemble des applications. L'utilisateur, ainsi affranchi de la contrainte de se souvenir de ses différents mots de passe, peut aussi se permettre d'en choisir de plus compliqués (et donc de plus robustes). Dans certaines configurations, un utilisateur se connectant sur une prise réseau du LBM sans être authentifié n'aura accès qu'à internet, dans d'autres configurations, il n'aura accès à rien.
- La gestion en groupe de travail (Workgroup) permet à chaque terminal connecté au réseau local de communiquer avec les autres terminaux sans identification utilisateur. Cela laisse le réseau ouvert et toute personne qui se connecte physiquement au réseau du LBM sera capable de communiquer avec l'ensemble des postes et des serveurs du réseau (donc intégré immédiatement dans le domaine de confiance). Cela implique que chaque composant du réseau dispose de sa propre sécurité et que toute faille crée un risque sur la confidentialité et l'intégrité des données médicales à caractère personnel.

Les deux configurations sont conformes, mais dans le cas d'un réseau en Workgroup, il est conseillé de vérifier le niveau de sécurité de chaque poste et serveur et l'application des recommandations B4.3 et B5.8 nécessite des procédures plus détaillées et complexes.

#### 6.3.4 Typologie des réseaux intersites

Le partage d'informations dans un LBM multi-sites peut s'effectuer de différentes manières (Cf. section 6.4 Architecture Applicative Critique).

Les sites qui ont chacun leurs applications et utilisent la messagerie électronique MSS ou Hprim Net pour s'échanger des données n'ont pas besoin de mettre en place un réseau dédié entre les deux sites : MSS garantit, par construction, la confidentialité des échanges. Le protocole Hprim Net assure cette confidentialité par un cryptage des messages.

##### Point de vigilance :

	Dans certains cas d'échange de données, le protocole Hprim Labo est utilisé avec un transport sans cryptage (exemple fichiers transmis par transfert de fichier non sécurisé FTP ou Kermit), ce qui induit un risque sur la confidentialité des données médicales à caractère personnel.
---	--

Les systèmes d'information qui partagent un serveur (un MW, un SIL, ...) requièrent un réseau intersites.

On trouve différents types de réseau intersites :

- Une simple connexion ADSL, unique connexion d'un ou deux sites avec partage du réseau au travers d'internet et régulation au niveau du pare-feu. Ce type de réseau ne permettant pas de crypter l'information qui circule sur internet, elle induit un risque de divulgation de l'information médicale patient.
- Une exception serait que le site d'hébergement dispose d'un composant réseau supportant un VPN et que le site distant ouvre un tunnel VPN (cryptage) pour se connecter. Ce type de connexion est identifiable par l'application que le site distant lance pour se connecter au VPN avant de lancer son application SIL.
- Un lien SDSL réseau dédiée entre les deux sites qui permet d'avoir un réseau dédié et donc sécurisé.
- Un réseau MPLS entre les différents sites qui permet de raccorder plusieurs sites à un « backbone » réseau central de manière dédiée et cryptée avec si nécessaire une sortie sur Internet. Si ce réseau est complètement sécurisé entre les sites, il faut vérifier comment est géré le pare-feu vers/de internet, soit par l'opérateur, soit avec un pare-feu local.

Point de vigilance :



Une connexion par VPN n'offre une bonne sécurité qu'à condition que la clé de cryptage soit une clé personnelle, propre à chacun des utilisateurs habilités à emprunter cette connexion.

### **6.3.5 Recensement et typologie des connexions à distance**

Il existe deux cas de connexion à distance :

- La connexion en nomade ou en mobilité d'un personnel interne habilité ;
- La connexion par l'un des fournisseurs des serveurs ou applications critiques.

#### **6.3.5.1 Connexion à distance par un personnel interne habilité**

La connexion à distance permet à un utilisateur de se connecter depuis internet (Wifi public, Wifi domicile, 3G, ...) aux applications du LBM. La connexion à un Wifi interne au LBM n'est pas considérée comme une connexion à distance puisque restant sur le réseau local du LBM.

Toute connexion à distance aux systèmes internes du LBM s'effectue en utilisant un VPN, puisqu'elle passe forcément sur Internet. En lançant l'application VPN l'utilisateur crée un tunnel sécurisé et crypté sur internet qui est conforme avec le respect de la confidentialité des données nominatives patients. Dans le cas contraire, les données circulent en clair sur internet ce qui n'est pas acceptable.

Certains éditeurs diffusent des applications de validation à distance sur tablette ou sur Smartphone. Là aussi, il est indispensable de vérifier que la tablette ou le Smartphone nécessite le lancement d'un exécutable VPN préalable quand ce terminal n'est pas connecté au Wifi du LBM.

#### **6.3.5.2 Connexion à distance par un fournisseur d'un serveur ou logiciel critique**

Cette connexion est utilisée pour les opérations de télémaintenance par des tiers (fournisseurs de serveur, de logiciels ou d'automates).

Le biologiste reste responsable de toute action et de toute modification réalisée par un tiers à travers ce type de connexion, en particulier sur la qualification des modifications.

Dans la bonne pratique, cette connexion est activée par un personnel du LBM et permet l'enregistrement de l'ensemble des opérations effectuées par le télé-intervenant pendant la durée de la connexion. Une autre solution consiste à demander aux intervenants de réaliser un rapport d'intervention systématique.

Sont utilisés dans les LBM :

- La mise en place d'un système d'alerte dans le logiciel installé qui permet de transmettre les alertes critiques sans que le tiers ait à se connecter. Il demande ensuite l'accès au personnel du LBM en utilisant l'un des dispositifs suivants.
- La mise à disposition d'un VPN permanent pour le fournisseur qui se connecte quand il y a nécessité. Dans ce cas, une procédure établit un moyen de garantir la traçabilité des interventions par les tiers. De plus un changement régulier et a minima trimestriel de l'identifiant ou du mot de passe est documenté et tracé pour éviter qu'une personne démissionnaire de l'entreprise tiers puisse se connecter après son départ.
- Les logiciels de prise de main à distance. Ces logiciels nécessitent que le LBM ouvre un logiciel spécifique sur un poste et donne un mot de passe avant la prise de main effective par le fournisseur. Certains de ces logiciels permettent l'enregistrement des actions réalisées. Dans d'autres cas, une fonctionnalité standard du système d'exploitation peut être utilisée pour l'enregistrement.

## 6.4 Architecture Applicative Critique

L'architecture applicative critique varie en fonction de :

- La répartition des serveurs applicatifs identifiés comme critiques en section 6.2.1 entre les sites d'un LBM multi-sites ;
- La nature des échanges de données des serveurs applicatifs critiques du LBM entre eux et avec l'extérieur.

### 6.4.1 Rappel des exigences de la norme NF EN ISO 15189 sur les applications critiques

Les paragraphes de la norme NF EN ISO 15189 qui concernent les applications critiques sont :

- Chapitre 4.5.2 et 4.5.3, 5.4.1, 5.8.7 concernant les analyses transmises à des LBM sous-traitants ;
- Chapitre 4.13.1 et 4.13.2 sur la conservation et la suppression des enregistrements qualité et technique ;
- Chapitre 5.1.8 sur la différenciation des rôles entre utilisateurs ;
- Chapitre 5.4 sur la phase pré-analytique, incluant feuille de prescription et manuel de prélèvement ;
- Chapitre 5.6.1 sur les systèmes de contrôle interne de la qualité (i.e. concerne la validation automatique) ;
- Chapitre 5.7.1 sur la validation biologique ;
- Chapitre 5.8.1 à 5.8.7 sur la formalisation des résultats.

Le LBM peut s'appuyer sur les points de sécurité de la [norme simplifiée 53 de la CNIL](#) touchant la communication des résultats.

Pour la transmission électronique des résultats en France, il est recommandé de s'appuyer sur le référentiel CI-SIS :

<http://www.esante.gouv.fr/services/referentiels/referentiels-d-interoperabilite/cadre-d-interoperabilite-des-systemes-d-inform>

## 6.4.2 Recensement et typologie des architectures multi-sites

Dans les LBM multi-sites, plusieurs types d'architecture peuvent être mis en place dont :

- Multi SIL – Multi MW – échange SIL par messagerie sécurisée de santé ;
- Multi SIL – mono MW – liaison dédiée ou MPLS ;
- Mono SIL – Mono/Multi MW - Réseau dédié ou MPLS de communication entre sites.

### 6.4.2.1 Architecture Multi SIL, Multi MW – échange SIL par messagerie

Dans cette configuration, deux sites travaillent ensemble sur un périmètre identifié mais restent sur des systèmes séparés. Les échanges de données sont réalisés entre les deux SIL par messagerie sécurisée de santé.



Figure 3: Architecture multi SIL, multi MW, échanges par messagerie

Dans cette configuration :

- Un premier niveau de validation biologique est réalisé par le LBM exécutant ;
- Le paramétrage des analyses dans les SIL est potentiellement différent ;
- Le paramétrage des feuilles de prescription est potentiellement différent ;
- Les MW sont potentiellement différents.

Pour que les systèmes communiquent de manière efficace, il est de la responsabilité du LBM exécutant de :

- Vérifier la formalisation des codes examens entre les SIL dans un document partagé et signé par les deux parties ;
- Vérifier le processus de modification des lignes de résultats connectées lors d'une modification de paramétrage ;
- Vérifier la formalisation du processus de mise à jour associé entre les deux parties ;
- Vérifier le processus de mise à jour du manuel de prélèvement lors d'une modification de paramétrage et sa rediffusion ;
- Vérifier que les informations présentes sur les feuilles de prescription sont conformes au paragraphe 5.4 de la norme NF EN ISO 15189 et que l'ensemble de ces informations sont bien transmises par Hprim ou ressaisies le cas échéant.

Dans le cas où ces échanges se basent sur des référentiels électroniques comme l'utilisation d'un catalogue LCSD pour synchroniser les codes demandes et l'utilisation de LOINC pour la

codification des lignes de résultats, ces vérifications sont simplifiées, chaque partie étant responsable de sa cohérence vis-à-vis des référentiels.

Il existe une autre déclinaison de ce modèle qui suppose les mêmes contraintes et qui repose sur une communication entre les middlewares à la place d'une communication entre SIL.

#### 6.4.2.2 Architecture Multi-SIL, plateau technique commun

Dans cette configuration, un plateau technique travaille pour plusieurs sites qui utilisent chacun leur propre instance du SIL (voire un SIL différent).

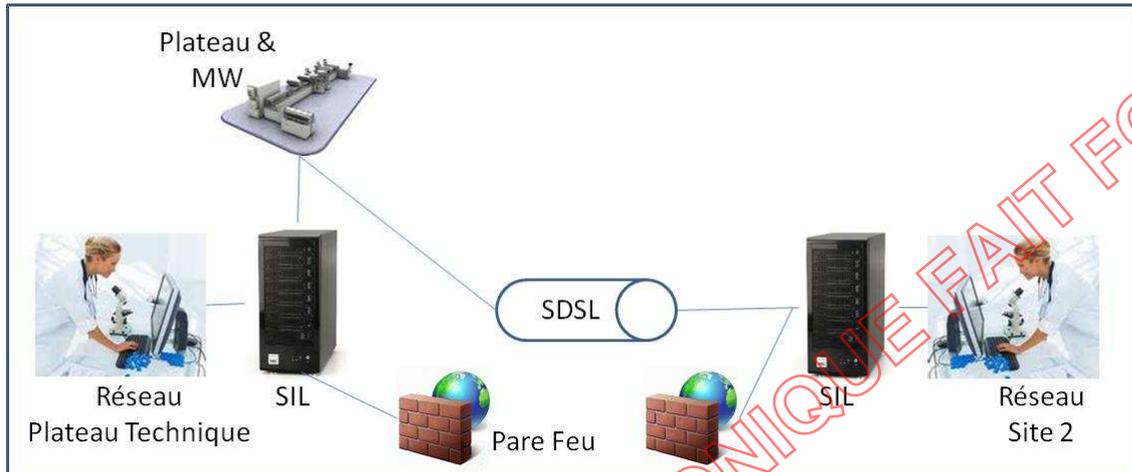


Figure 4: Architecture Multi SIL, plateau technique commun

Dans cette configuration :

- Chaque site réalise sa validation dans son instance de SIL ;
- Le paramétrage des examens dans les SIL est potentiellement différent ;
- Le paramétrage de chaque analyse est unique sur un middleware ;
- Les échanges ne reposent pas sur des feuilles de demandes mais uniquement sur les numéros de tubes et les codes analyses du ou des MW.

Pour que les systèmes communiquent de manière efficace, il est nécessaire de s'assurer que :

- Toute modification de paramétrage réalisée dans le MW est communiquée à tous les sites distants avant sa mise en application avec une date d'application ;
- Un document est tenu à jour sur le plateau technique avec l'ensemble des codes et du paramétrage du MW comme référence pour les sites distants ;
- A chaque modification du paramétrage du MW, le site distant effectue des tests de connexions sur le nouveau paramétrage et assure la traçabilité de ces tests ;
- Des plages de numéros de tubes sont réservées par SIL/site et sont formalisées sous peine de mélanger les tubes et les patients de plusieurs sites.

### 6.4.2.3 Architecture mono SIL, Mono/Multi MW

Dans cette configuration, un plateau technique centralise l'informatique pour plusieurs sites, qu'il s'agisse du SIL ou du MW, les sites distants se connectant au SIL central.

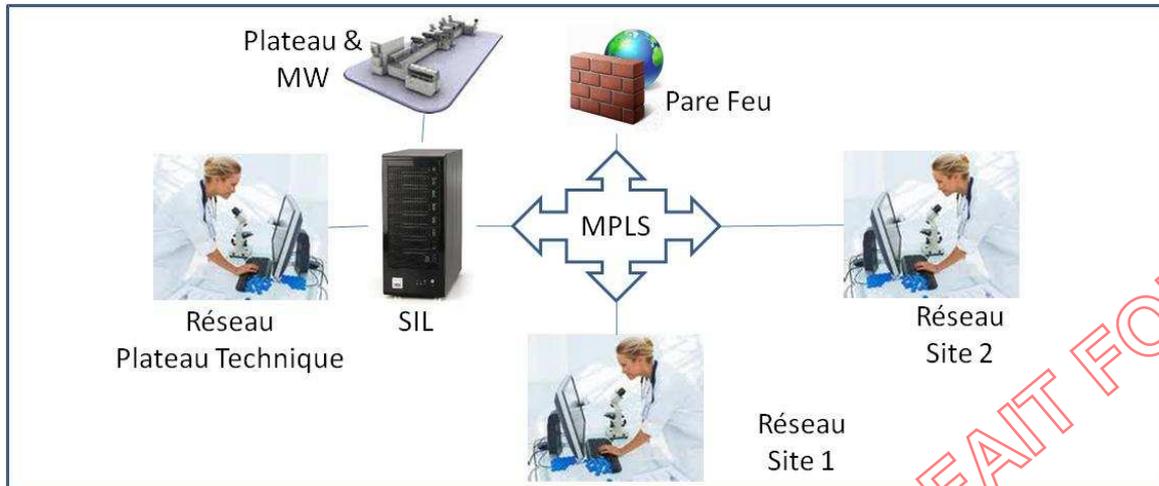


Figure 5: Architecture Mono SIL, Mono/Multi MW

Dans cette configuration :

- La validation est réalisée sur le SIL central, indifféremment depuis les sites distants ou depuis le site local ;
- Le paramétrage des examens dans le SIL est unique ;
- Le paramétrage de chaque analyse est unique sur un MW ;
- Les échanges ne reposent pas sur des feuilles de demandes mais uniquement sur les numéros de tubes attribués par le SIL central (pas de réservation de plage).

La communication entre les sites est de fait intégrée et aucune procédure particulière de communication n'est à mettre en place.

### 6.4.3 Recensement des échanges de données d'un LBM

Légende des diagrammes de cette section :

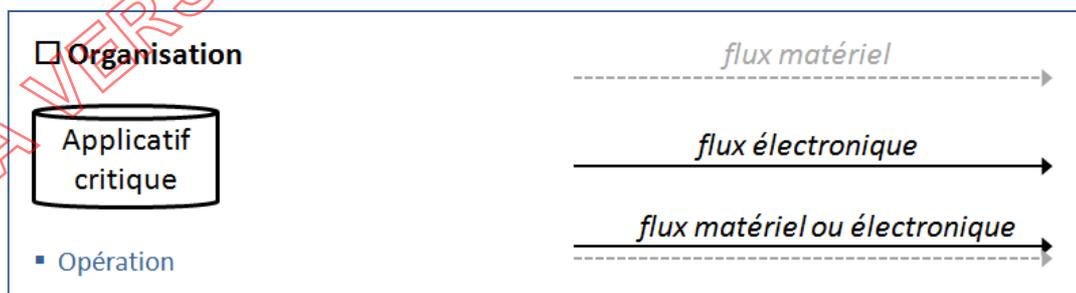


Figure 6: Légende des diagrammes de flux

### 6.4.3.1 Phase pré-analytique

(Référence : NF EN ISO 15189 §5.4)

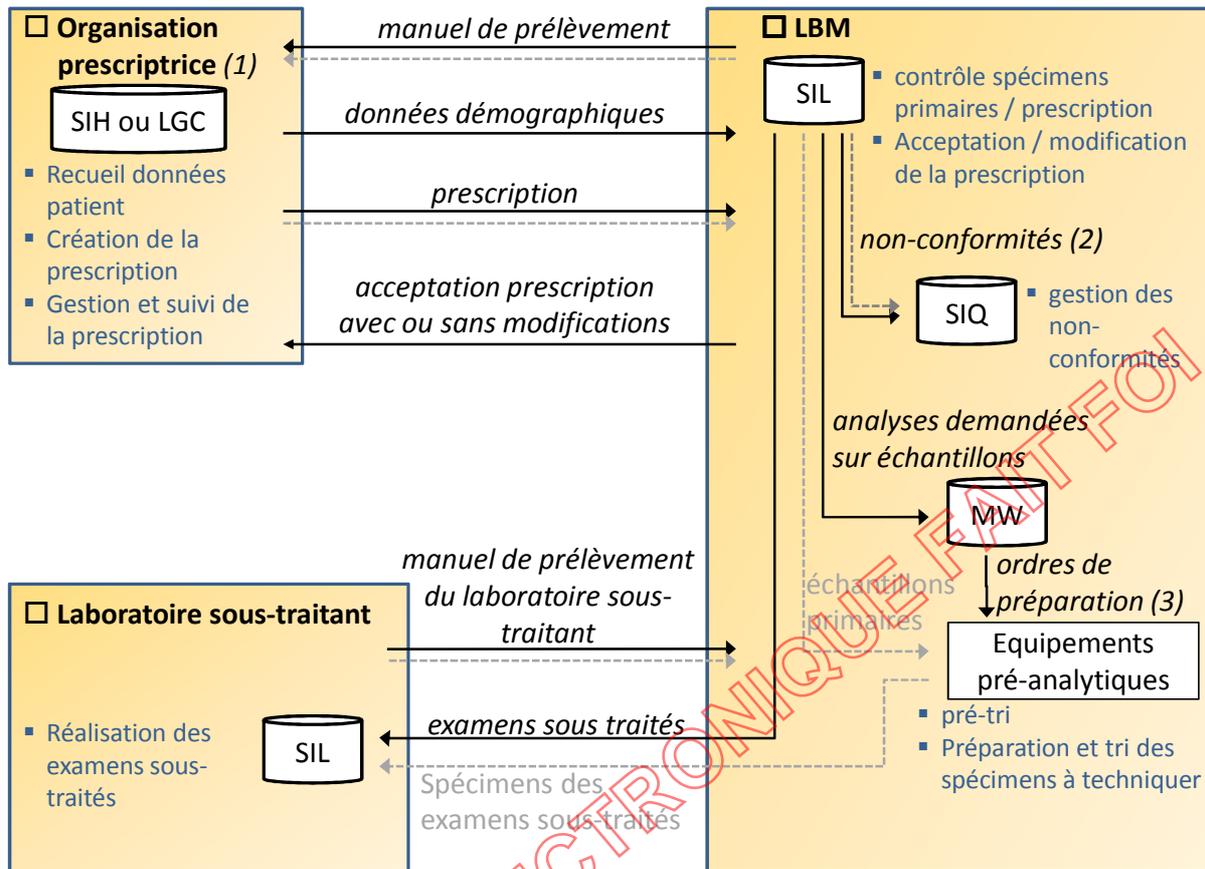


Figure 7: Flux de la phase pré-analytique

Notes :

(1) : L'organisation prescriptrice peut être un établissement de soins équipé d'un SIH ou un cabinet médical équipé d'un LGC. Dans le premier cas, le SIH peut transmettre les données démographiques des patients par voie électronique (Cf. section 6.4.3.1.2). Le SIH peut aussi transmettre la prescription sous forme électronique (Cf. section 6.4.3.1.4), dans ce cas l'acceptation des spécimens par le LBM et les éventuelles modifications du contenu de la prescription sont notifiées au SIH également sous forme électronique.

(2) : L'enregistrement et le suivi des non-conformités peuvent être assurés par le SIL ou par un SIQ externe. Dans ce dernier cas, la détection d'une non-conformité par le SIL est reportée dans le SIQ, soit manuellement, soit par un flux électronique (Cf. section 6.4.3.1.3).

(3) : S'il existe une chaîne pré-analytique robotique pilotée par un MW celui-ci traduit le contenu de la demande d'examens en ordres de préparation des spécimens à techniquer.

(4) : Le LBM communique son manuel de prélèvement à l'organisation prescriptrice, par voie électronique ou papier. De même, en cas de sous-traitance, le LBM sous-traitant communique son manuel de prélèvement au LBM de première intention (Cf. section 6.4.3.1.3)

(5) : Le colisage des spécimens transmis au LBM sous-traitant est hors champ de ce guide d'évaluation des systèmes informatiques.

#### 6.4.3.1.1 La feuille de prescription

(Référence : NF EN ISO 15189 §5.4.1)

La feuille de prescription parvient au LBM sous forme papier et/ou sous forme d'un flux électronique. Le contenu de cette feuille est décrit au chapitre 7.3.3.

En cas de sous-traitance d'examens, la demande d'examens adressée au LBM sous-traitant sous forme papier et/ou électronique comporte les mêmes éléments que la feuille de prescription, auxquels s'ajoutent :

- L'identification du LBM demandeur :
  - Nom du LBM,
  - N°FINESS ou identifiant attribué à ce LBM par le LBM sous-traitant.
- En cas de flux électronique, transcodage des examens sous-traités dans la codification fournie avec le manuel de prélèvement du sous-traitant.

L'enregistrement informatique de la feuille de prescription dans le SIL produit une demande d'examens.

#### 6.4.3.1.2 Messages électroniques de données démographiques patients

(Référence : SH REF 02 §5.4 "Une procédure d'identitovigilance interne au LBM ou à l'établissement de santé est fortement recommandée".)

Lorsque l'organisation prescriptrice est un établissement de santé, il existe couramment une liaison informatique du SIH de l'établissement vers le SIL du LBM, acheminant les données démographiques des patients. L'envoi de ces données démographiques est déclenché par les événements administratifs "entrée ou visite du patient", "sortie du patient", "transfert du patient d'un service à un autre", "correction d'identité", "fusion d'un doublon". Le SIL reçoit donc ces données pour l'ensemble des patients de l'établissement mais il n'exploite réellement ces données que pour les patients de l'établissement ayant des examens de biologie au LBM.

Deux standards existent pour ces flux électroniques, tous les deux diffusés par l'association interop'santé. Ce sont par ordre de pertinence décroissante :

- Le profil IHE PAM dans sa version française, maintenue régulièrement, au rythme d'une version par an ;
- Le message ADM de l'ancien format Hprim Santé, figé depuis 2004. Ce format ancien, encore très répandu dans les liaisons entre établissements de soins et LBM de ville, ne fournit pas l'INS du patient et ne décline pas l'identité du patient sous une forme réglementaire (nom de jeune fille et nom, au lieu de nom de famille et nom d'usage).

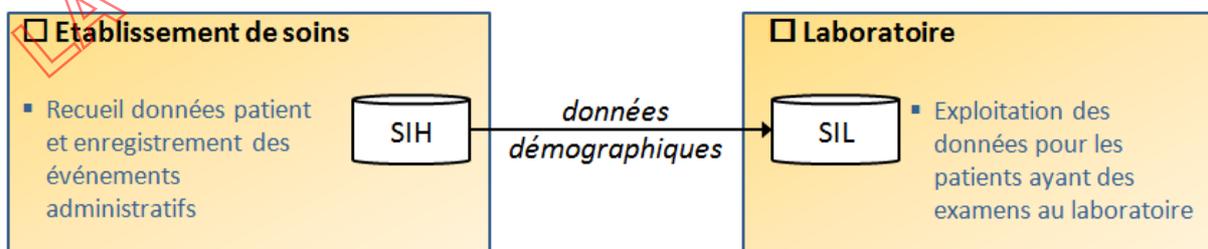


Figure 8: Flux de données démographiques

Ce flux électronique de données démographiques contient les éléments suivants :

- Identification de l'établissement émetteur : Nom et/ou N°FINESS ;
- Patient :
  - Identifiant permanent au sein de l'établissement de soins ;
  - INS, si connu, avec sa date d'obtention (possible uniquement avec IHE PAM) ;
  - Identité : prénom, nom de famille, et le cas échéant, nom d'usage ;
  - Sexe ;
  - Date de naissance.
- Dossier administratif et mouvements :
  - Identifiant du dossier (n° d'hospitalisation, de v isite, de consultation ...) ;
  - Date d'entrée, si connue ;
  - Date de sortie, si connue ;
  - Service ou UF de présence, si connu ;
  - Type d'événement déclencheur du message : entrée, sortie, mouvement interne, correction ou enrichissement de données administratives, fusion de doublon.

#### **6.4.3.1.3 Manuel de prélèvement sous forme électronique structurée**

(Référence : NF EN ISO 15189 §5.4.2, 5.4.3, 5.4.4)

Le manuel de prélèvement des échantillons primaires guide à la fois :

- La prescription, en listant les examens de biologie que le LBM est capable de réaliser, et en stipulant les conditions associées : horaires, délai de réalisation, renseignements cliniques attendus ;
- Le prélèvement des échantillons primaires en précisant pour chaque examen de biologie, le ou les échantillons attendus, (nature, volume, type de tube, conditions de prélèvement, de conservation, de transport).

Ce manuel de prélèvement peut être communiqué aux prescripteurs, LBM demandeurs, et préleveurs sous diverses formes : papier, site web, pdf, messages électroniques structurés.

Dans le cas d'une communication par messages électroniques structurés, un seul format standard existe : le profil IHE LCSD maintenu régulièrement et diffusé dans sa version française par l'association interop'santé. Ce mode de communication permet en outre de diffuser les codes informatiques des examens de biologie et de leurs éléments, pour une utilisation ultérieure dans les messages d'échanges de demandes et résultats avec le SIL (prescription connectée, sous-traitance).

Les messages diffusant le manuel de prélèvement sous forme électronique structurée précisent la version qu'ils diffusent. Il est recommandé que les messages de demandes d'examens, prescription connectée, envois de résultats, rappellent un numéro de version du manuel de prélèvement sur lequel ils s'appuient.

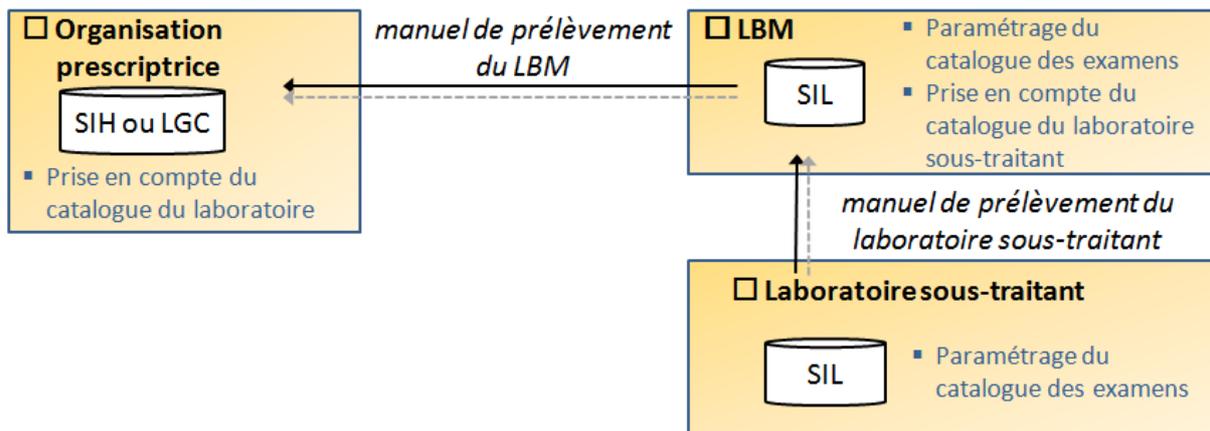


Figure 9: Flux de manuels de prélèvement

Point de vigilance :



Continuité du processus de mise à jour : Une nouvelle version du paramétrage du catalogue des examens du SIL se traduit par une nouvelle version du manuel de prélèvement communiqué aux acteurs (mise à jour du site web, nouvel envoi papier, fichier pdf ou flux de messages électroniques structurés).

**6.4.3.1.4 La prescription connectée**

(Référence : NF EN ISO 15189 §5.4)

La prescription connectée peut exister entre établissements de soins et LBM intra-établissement ou de ville. Elle consiste à dématérialiser la feuille de prescription sous la forme d'un flux électronique. Dans ce cas, la réception des échantillons primaires au LBM et leur vérification par rapport à la prescription électronique déclenche un flux électronique d'acceptation de la prescription retourné vers le prescripteur.

Deux standards existent pour les flux de prescription connectée, tous les deux diffusés par l'association interop'santé. Ce sont par ordre de pertinence décroissante :

- Le profil IHE LTW ;
- L'ancien format Hprim Santé figé depuis 2004, à l'exception d'un seul aménagement consenti pour y insérer l'INS-c du patient.

Les données du message de prescription connectée sont celles de la feuille de prescription (voir chapitre 7.3.3).

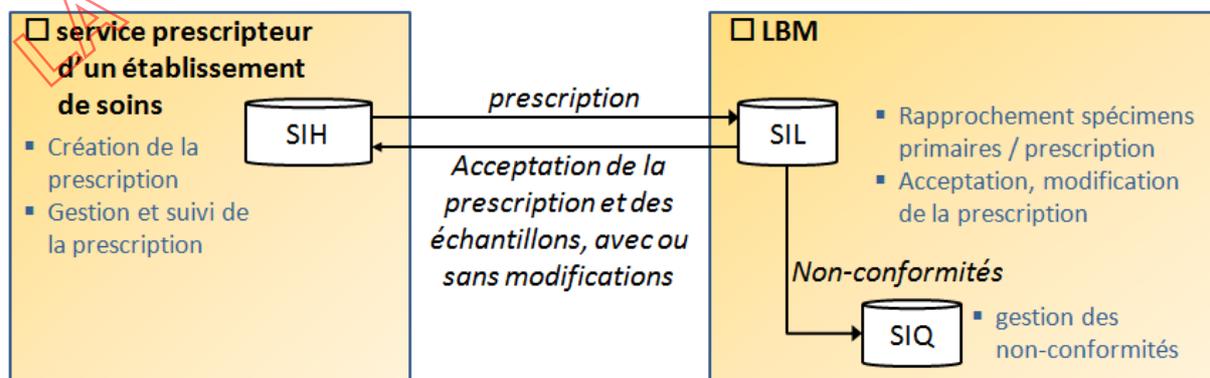


Figure 10: Flux de prescription connectée

Points de vigilance :



Seul le profil IHE LTW permet de gérer convenablement les modifications de la prescription (examens ajoutés ou substitués), ainsi que les refus de spécimen, avec communication des motifs de refus.



La procédure de rapprochement de la prescription des spécimens primaires, implémentée dans le SIL permet :

- le rapprochement sur identifiant de spécimen ou de patient ou de prescription ;
- de donner la possibilité d'accepter ou de refuser le spécimen, en motivant le refus et en chaînant vers l'enregistrement des non conformités pré-analytiques ;
- de prévoir la gestion des prescriptions orphelines (durée maximale de conservation, purge, signalement).

### 6.4.3.2 Phase analytique

(Référence : NF EN ISO 15189 §4.13, 5.5)

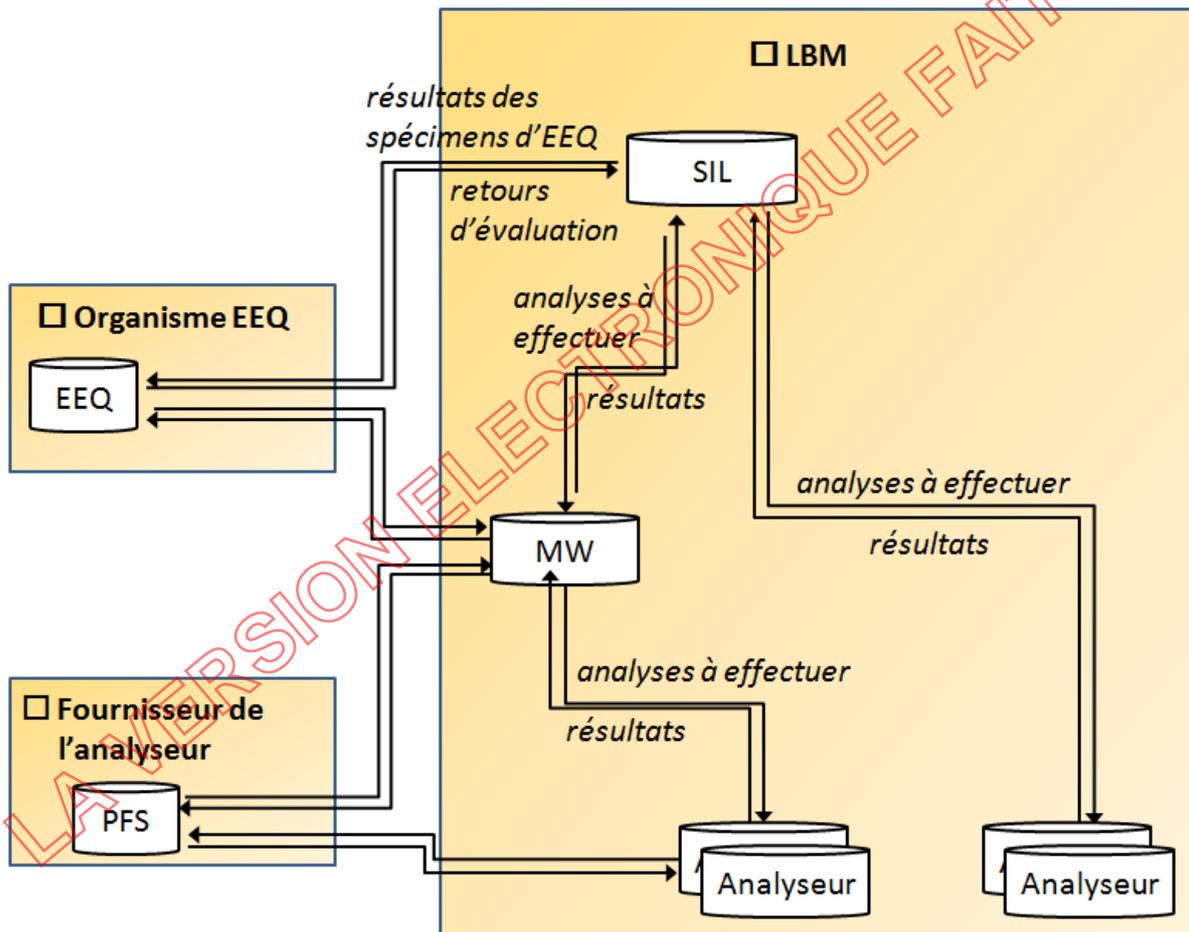


Figure 11: Flux de la phase analytique

Un analyseur peut être connecté directement au SIL ou bien au travers d'un MW. Dans un LBM mono site, il n'est pas rare que le SIL soit connecté directement avec l'ensemble des analyseurs. Quelle que soit la configuration il importe de vérifier la traçabilité des contrôles qualité et la méthode de conservation des résultats bruts édités par les instruments, ainsi que la validité des transferts analyseur – SIL.

L'enregistrement et le suivi des non-conformités peuvent être assurés par le SIL ou par le SIQ. Dans ce dernier cas, la détection d'une non-conformité par le SIL ou par le MW peut déclencher un flux vers le SIQ pour enregistrement.

Les CIQ sont traités sur l'analyseur. Le contrôle et la vérification des résultats de CIQ peuvent être gérés sur l'analyseur, sur le MW, dans le SIL ou tout autre outil ad-hoc.

L'acceptation technique des résultats peut suivant les cas être réalisée sur l'analyseur, sur le MW ou sur le SIL.

Le LBM conserve les résultats bruts (NF EN ISO 15189 §4.13.3). Les formats de transmission par les analyseurs peuvent être considérés comme des formats valides de conservation des données brutes.

Les standards disponibles pour les échanges de données SIL – MW sont, par ordre de pertinence décroissante :

- Le profil IHE LTW ;
- Le standard HL7 2.x utilisé hors contexte du profil IHE LTW ;
- Les standards ASTM E1394 et E1381 figés depuis 1997 et retirés du portefeuille de standards valides d'ASTM depuis 2002 ;
- Le standard H' Santé non conçu pour cet usage.

Les standards disponibles pour les échanges de données avec les analyseurs sont, par ordre de pertinence décroissant :

- Le profil IHE LAW ;
- Le standard HL7 2.x utilisé hors contexte du profil IHE LAW ;
- Les standards ASTM E1394 et E1381 figés depuis 1997 et retirés du portefeuille de standards valides d'ASTM depuis 2002 ;
- Le standard H' Santé non conçu pour cet usage.

Sur le terrain, les interfaces des analyseurs sont encore assez peu standardisées et leur paramétrage est souvent fermé.

Certains fournisseurs d'analyseurs de biologie médicale exploitent dans leur périmètre une PFS à laquelle leurs analyseurs et/ou leurs MW déployés dans les LBM peuvent se connecter.

Les données qui remontent vers la PFS sont exclusivement des données techniques. Par ailleurs, cette connexion peut aussi être utilisée pour les interventions de télémaintenance du fournisseur sur l'analyseur (selon les modes exposés au §6.3.5.2).

Si la PFS reçoit des données médicales à caractère personnel des LBM, le fournisseur est un hébergeur agréé en contrat avec les LBM utilisant ces analyseurs (comme exposé au § 6.2.5.2).

### 6.4.3.3 Phase post-analytique

(Référence : NF EN ISO 15189 5.7.1 & 5.8)

SH-REF-02 – encadré réglementaire associé au §5.8 :

*La validation d'un résultat d'examen de biologie médicale est réalisée par un biologiste médical avant toute communication à l'extérieur du LBM (L.6211-2), à l'exception des examens de biologie délocalisée. (...) La possibilité de transmettre un résultat provisoire d'examen, ouverte par la norme (§5.8.9), est supprimée par la législation française.*

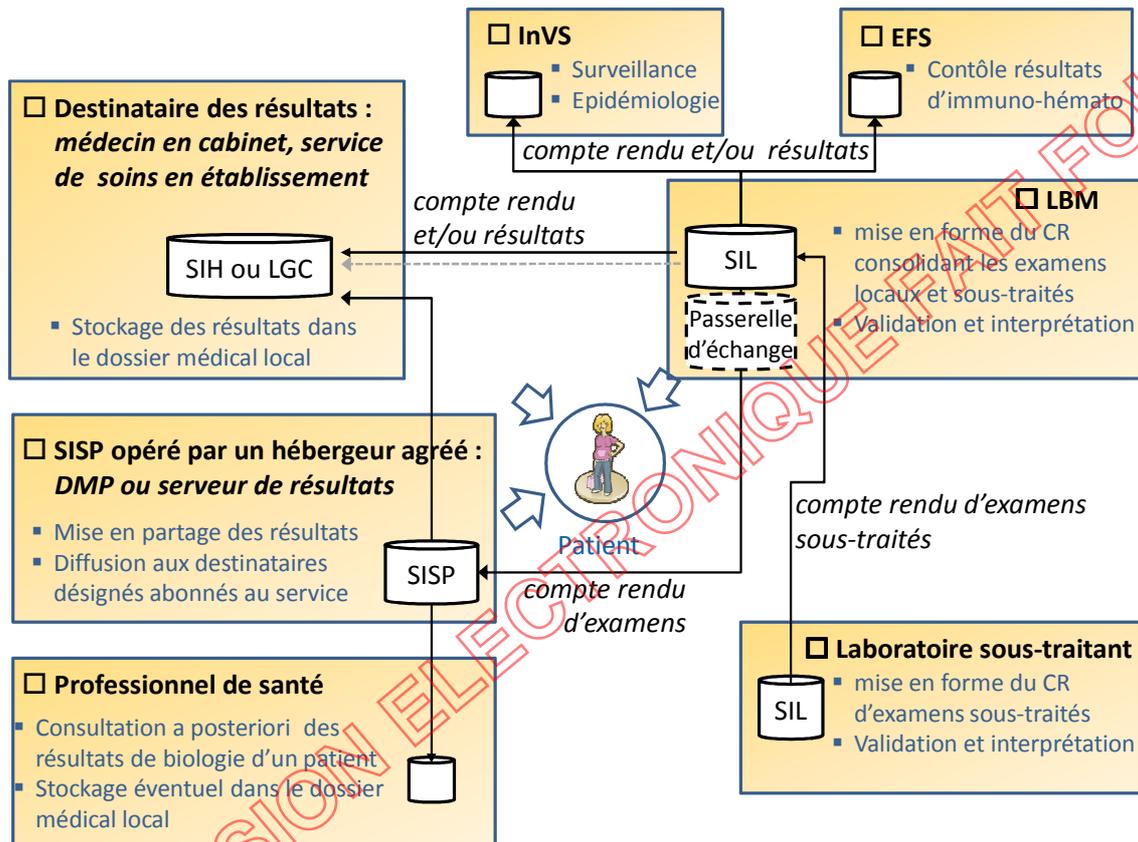


Figure 12: Flux de la phase post-analytique

Les résultats et/ou comptes rendus d'examens ne sont transmissibles qu'après validation et interprétation sous la responsabilité d'un biologiste médical (Cf. 5.8 du SH-REF 02).

La diffusion de résultats et/ou de comptes rendus d'examens dématérialisés dans les formats électroniques attendus peut être opérée directement par le SIL ou peut être confiée, en tout ou partie, à une passerelle d'échange qui peut, le cas échéant, réaliser des conversions de formats et des remises en forme des résultats avant diffusion. La passerelle, est dans le périmètre et sous la responsabilité du LBM ou de l'établissement qui le contient.

En ce qui concerne la diffusion de résultats d'examens en intra-établissement par un LBM d'établissement de soins :

- Les standards disponibles pour le format et la structuration des résultats sont, par ordre de pertinence décroissante :
  - Le profil IHE LTW ;
  - Le compte rendu structuré de biologie au standard CDA, selon le modèle spécifié par le CI-SIS ;
  - L'ancien format Hprim Santé figé depuis 2004 ;
  - Le compte rendu pdf sans autre mise en forme.
- Le moyen de transport est choisi par l'établissement en conformité avec son infrastructure réseau interne.

En ce qui concerne la diffusion de résultats vers un professionnel de santé ou un système d'information situé hors de l'entité juridique du LBM :

- les standards disponibles pour le format et la structuration des résultats sont, par ordre de pertinence décroissante :
  - Le compte rendu structuré de biologie au standard CDA, selon le modèle spécifié par le CI-SIS ;
  - L'ancien format Hprim Santé/Image figé depuis 2004 ;
  - Le compte rendu pdf encapsulé dans un document CDA non structuré, tel que spécifié par le CI-SIS ;
  - L'ancien format Hprim Médecin figé depuis 2000 ;
  - Le compte rendu pdf sans autre mise en forme.
- Le moyen de transport est soit une messagerie sécurisée de santé, soit un autre protocole déterminé par le système informatique destinataire. Par exemple l'alimentation du DMP se fait par web service.

Dès lors que la diffusion des résultats d'examens de biologie exploite un format structuré (profil IHE LTW, document électronique CDA structuré, message Hprim Santé ou Hprim Médecin) il est recommandé d'identifier les analyses porteuses de résultats à l'aide de la nomenclature LOINC traduite en français et publiée dans le CI-SIS.

L'envoi électronique du compte rendu au patient peut se faire via un SISP (DMP ou serveur de résultats). Le format et le transport sont déterminés par le SISP.

L'envoi du compte rendu directement au patient par messagerie sans autre protection n'est pas recommandé.

### 6.4.3.4 Biologie délocalisée

(Référence : norme NF EN ISO 22870 en complément de la norme NF EN ISO 15189 et SH-REF-02 encadré réglementaire "Tests d'orientation diagnostique et biologie délocalisée")

*Les tests (tels que l'auto-surveillance glycémique pratiquée par les patients diabétiques avec un lecteur de glycémie personnel), les recueils et traitements de signaux biologiques (tels que la mesure oxymétrique transcutanée) à visée de dépistage, d'orientation diagnostique ou d'adaptation thérapeutique immédiate pratiqués hors du LBM, par le clinicien, l'infirmier ou le patient lui-même, qui relèvent de l'article L.6211-3 du code de la santé publique ne sont pas des examens de biologie médicale et ne sont donc pas des activités à accréditer.*

*Ces tests se distinguent des examens de biologie médicale dite « délocalisée » (tels que « les gaz du sang par voie artérielle » réalisés dans les unités de soins), qui sont des examens de biologie médicale à part entière (L.6211-18). Ils sont à accréditer et entrent dans le champ d'application du présent recueil. Ils doivent respecter également les exigences de la norme NF EN ISO 22870.*

La biologie délocalisée se rencontre dans les établissements de soins et concerne les LBM d'établissement ou travaillant avec un établissement.

La biologie délocalisée n'a pas, à proprement parler, de phase pré-analytique : le prélèvement du patient produit un spécimen biologique exploité tel quel et immédiatement par la phase analytique réalisée par le personnel de l'unité de soins. Ce personnel est formé au maniement des analyseurs délocalisés par le LBM qui supervise le processus.

Les résultats obtenus sont utilisés sans délai par les soignants. Cependant, le LBM qui supervise le processus collecte l'ensemble des résultats pour contrôler et assurer la qualité du processus de biologie délocalisée.

La biologie délocalisée fait interagir 4 catégories de systèmes :

- Les analyseurs délocalisés dans les unités de soins ;
- Un ou plusieurs systèmes intermédiaires (MW) de pilotage de ces analyseurs ;
- Le SIL du LBM de supervision qui est destinataire de l'ensemble des résultats de la biologie délocalisée qu'il supervise ;
- Le SIH de l'établissement, qui est la source de vérité pour l'identification des patients, et pour celle des soignants.

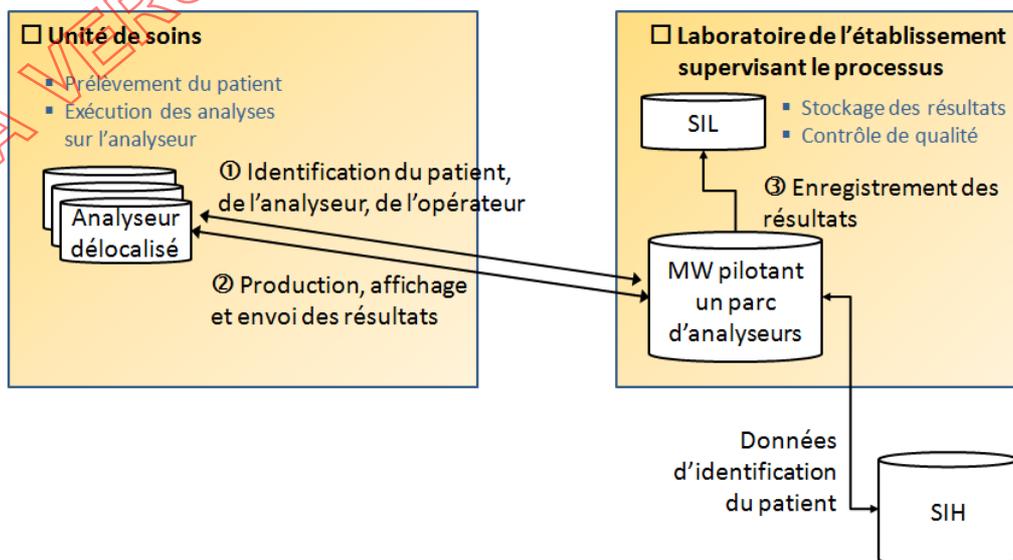


Figure 13: Flux de biologie délocalisée

Points à vérifier :

- Fiabilité de l'identification du soignant sur l'analyseur et remontée de cette identification avec les résultats dans le SIL ;
- Fiabilité de l'identification du patient sur l'analyseur : lecture étiquette code barre ou saisie manuelle. L'identité du patient est obtenue du SIH et affichée sur l'écran de l'analyseur pour contrôle ;
- Remontée de l'ensemble des informations de traçabilité avec les résultats vers le SIL : Identifiants de l'analyseur, du soignant, du patient, horodatage, alarmes ;
- Le contrôle de qualité peut se faire sur le système intermédiaire de pilotage (MW) ou sur le SIL. Vérifier les actions déclenchées en cas de détection d'anomalie : Alerte au biologiste, blocage automatique de l'analyseur par le système intermédiaire, ...

Un seul standard est disponible pour les flux 1, 2, et 3 : le profil IHE LPOCT qui s'appuie sur le standard POCT1-A, ce dernier exploitant des messages HL7.

Le moyen de transport est choisi par l'établissement en conformité avec son infrastructure réseau interne.

L'interface de contrôle de l'identification du patient entre le MW et le SIH, lorsqu'elle est présente, peut s'appuyer sur :

- Le profil IHE PAM (Cf. §6.4.3.1.2) qui sert alors à pré-alimenter le MW avec les identités des patients de l'établissement ;
- Le profil IHE PDQ qui permet au MW d'interroger en temps réel le SIH, à réception de l'identifiant patient transmis par un analyseur délocalisé.

Sur le terrain, les interfaces des analyseurs de biologie délocalisée sont très rarement standardisées, et leur paramétrage est souvent fermé.

## 6.5 Cartographie des systèmes et des échanges

Pour maîtriser son environnement, il est recommandé que le LBM s'appuie sur une cartographie de ses systèmes mettant en évidence les échanges de données entre eux et avec les systèmes extérieurs.

Chaque système est repéré sur ce schéma par son nom et son adresse réseau (suivant les cas : nom DNS, url, adresse IP, ...).

Exemples de cartographie :

### 6.5.1 LBM de ville bi-sites travaillant avec deux établissements

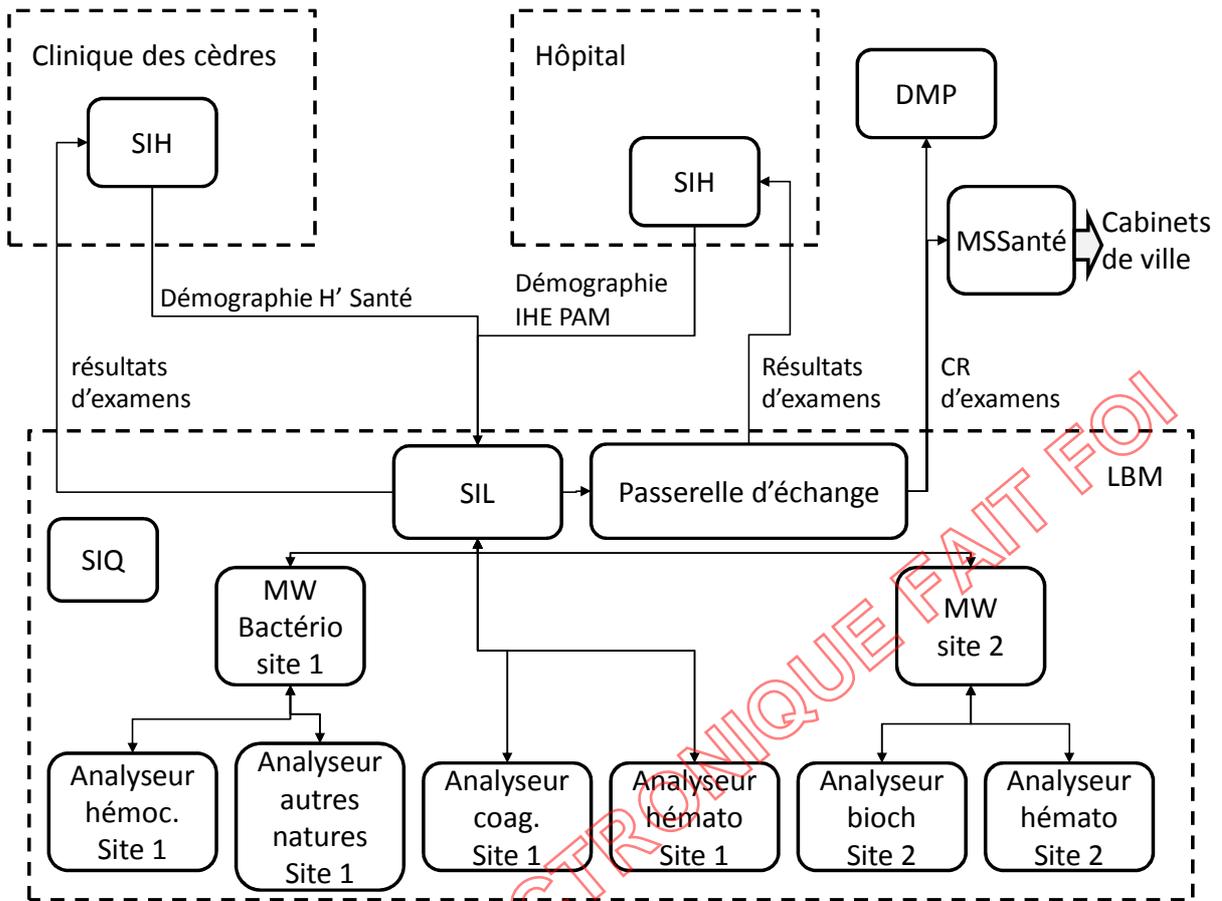


Figure 14: Cartographie des flux d'un LBM de ville à deux sites travaillant avec une clinique et un hôpital

**Notes :**

Les flux de téléfacturation avec l'assurance maladie peuvent éventuellement être montrés, mais ils restent hors périmètre de l'évaluation.

Les périphériques (terminaux, douchettes, lecteurs Vitale, imprimantes, scanners ...) peuvent être montrés ou non.

### 6.5.2 LBM hospitalier

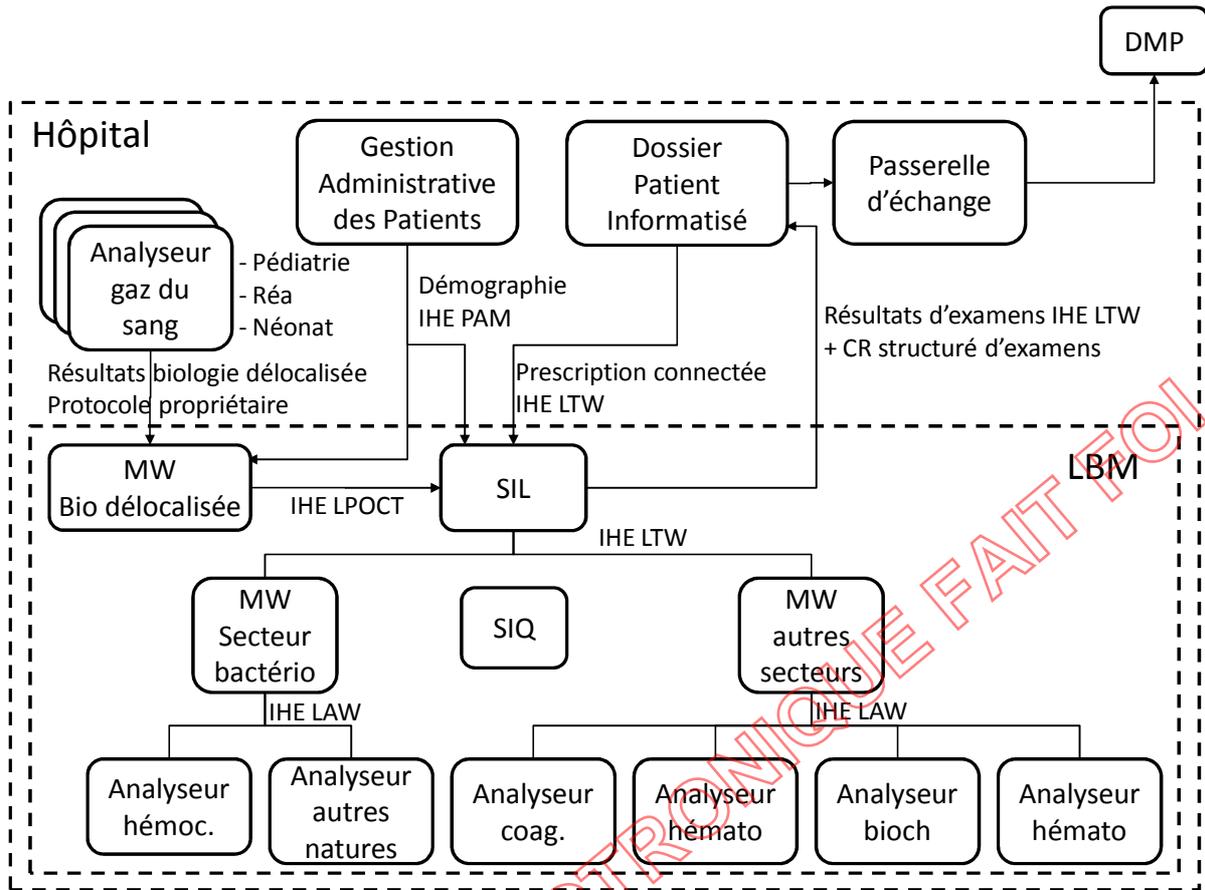


Figure 15: Cartographie des flux d'un LBM intra-établissement

## 7 PRECONISATIONS POUR LE FONCTIONNEMENT DES SYSTEMES INFORMATIQUES EN REGARD DES EXIGENCES

### 7.1 Environnement

#### 7.1.1 Matériels et logiciels

(Référence : SH REF 02 §4.2

« ...Toutefois, les incidents qui mettent en cause les logiciels définis au 18° de l'article L.5311-1 sont signalés sans délai à l'ANSM, par les professionnels de santé qui les utilisent (décret n°2011 - 1448). Le SMQ du LBM comporte les dispositions relatives à la protection des systèmes d'information et à la déclaration des incidents »).

Les logiciels isolés (non intégrés dans un dispositif médical) utilisés dans un LBM pour la gestion des examens de biologie médicale et lors de la validation, de l'interprétation, de la communication appropriée et de l'archivage des résultats, se répartissent :

- En logiciels qui sont des dispositifs médicaux devant être marqués CE ;
- En logiciels qui ne sont pas des dispositifs médicaux.

Les logiciels sont considérés comme des dispositifs médicaux marqué CE en fonction de leur finalité médicale (modification et/ou création d'une donnée). Dans la directive 98/79/CE, il s'agit le plus souvent d'un auto-marquage CE. Les procédures de réacto-vigilance du LBM s'appliquent directement à ces dispositifs et une déclaration à l'ANSM est obligatoire en cas d'anomalies. Sont exclus par exemple le changement d'unité, les calculs simples ou les comparaisons de résultats, ...

Pour les logiciels non dispositifs médicaux (les plus nombreux) l'ordonnance 2010-49 les a ajoutés dans le champ des produits couverts par l'ANSM. Un décret spécifique décrit une vigilance spécifique (identique à la réacto-vigilance).

« Art. R. 5232-17. – La vigilance comporte :

1° Pour les professionnels de santé utilisateurs mentionnés à l'article L. 5232-4, le signalement à l'Agence française de sécurité sanitaire des produits de santé de tout incident consistant en une défaillance ou une altération des caractéristiques ou des performances des produits de santé mentionnés à la présente section, ou une inadéquation dans l'étiquetage ou la notice d'utilisation, susceptibles d'entraîner des effets néfastes pour la santé des personnes ».

Le SMQ du LBM comporte l'ensemble de ces dispositions.

#### Point de vigilance :



Les fonctionnalités de facturation des systèmes sont hors du champ de ce guide cependant la préservation de la confidentialité des données patient peut induire des contraintes sur la circulation des données de facturation. Ainsi, quand une facture risque d'arriver dans un environnement non médical le LBM veillera à faire en sorte qu'un nom d'examen ne puisse être relié à un nom de patient.  
Exemple : demande d'examens de médecine du travail facturée à l'entreprise employeuse du patient.

### 7.1.2 Critères de sélection d'un SIL ou d'un MW

(Référence : NF EN ISO 15189 §4.6.1)

Il est important de bien identifier les étapes du processus de manière à faciliter l'expression des besoins et, avant tout, d'anticiper sur les points à risques, notamment :

- Fonctionnalités ;
- Performance (coûts, délais) ;
- Ergonomie ;
- Marquage CE DM DIV ;
- Compatibilité des systèmes entre eux ;
- Maintenance, SAV ;
- Mode dégradé ;
- Formation, évaluation, habilitation, ...

Différentes sociétés scientifiques mettent à disposition des outils et des documents (Descriptifs Standardisés en Automatisation – dont MW - de la SFBC et guides de la SFIL, ...) sur lesquels les LBM pourront s'appuyer pour mettre en place leur propre cahier des charges. Ce dernier permet de définir ses besoins fonctionnels en fonction des exigences réglementaires, normatives et internes.

## 7.2 Maîtrise du paramétrage et des dictionnaires/tables

Ce chapitre traite de la gestion globale des différents dictionnaires/tables. Cette gestion englobe la création, la mise à jour, l'inactivation/suppression et l'archivage.

Point de vigilance :



Le LBM met en œuvre un dispositif d'alerte lors de toute mise à jour d'un des éléments de la chaîne des systèmes d'information (exemple de personne à alerter : biologiste responsable, référent informatique, ...).

### 7.2.1 Annuaire des tiers

Le terme « tiers » regroupe l'ensemble des partenaires pouvant échanger des informations avec le LBM (médecins, maïeuticiens, IDE, LBM sous traitants, administrations, organismes payeurs, UF, CNR, INVS, ANSM, EFS, fournisseurs, ...).

Le LBM met en œuvre une procédure de gestion d'un tiers et de vérification de la transmission des données entre tiers et LBM. La maîtrise des champs de l'annuaire de tiers a un impact direct sur la diffusion des données biologiques (dématérialisation du compte rendu au format CDA, Hprim, impression centralisée et/ou déportée, serveur de résultats, fax, ...). L'annuaire contient l'ensemble des données permettant de piloter les échanges avec le tiers.

Exemples de données :

- Données d'adressage (postales, informatiques, téléphoniques, ...) ;
- Données d'identification (FINESS, RPPS, ...) ;
- Données de hiérarchisation (Etablissements de santé, UF ou services, médecins, maïeuticiens, ...) ;
- Modalités de codification en fonction de la qualité du tiers (par exemple codification en utilisant les premières lettres du nom et les premières du prénom pour les prescripteurs, la distinction des praticiens travaillant en cabinet et en établissement

de santé pourra s'effectuer en utilisant les premiers caractères pour identifier l'établissement et les suivants pour identifier le praticien, ...).

### 7.2.2 Catalogue des examens

Le LBM définit sur son SIL les règles de gestion des codes examens. La mise en place d'un catalogue des examens étant une opération critique, les étapes de création et de modification sont réalisées par des personnes habilitées.

Note : en termes d'interopérabilité, le transcodage sur l'ensemble des interfaces a un impact direct sur le traitement des examens par les automates.

Exemple de catalogue :

- Classement par sous domaine, famille (biochimie générale et spécialisée, hématocytologie, ...);
- Classement suivant le lieu de réalisation des examens : sur site, LBM sous-traitants.

Exemple de caractérisation de l'examen au niveau du SIL :

- Code analyse, code de transcodage, ... ;
- Famille d'appartenance (hémostase, bactériologie, ...);
- Nature du spécimen ;
- Unités, normales, ... ;
- Code nomenclature avec traçabilité des mises à jour ;
- Lieu de réalisation (site, LBM sous-traitant, ...);
- Pour les LBM sous-traitants : conditions de transport ;
- Gestion de la redondance, du délai de réalisation, du délai de stabilité, ... ;
- Méthode utilisée ;
- Mode de saisie (manuelle, interface, ...);
- Type de résultat (numérique, texte, ...);
- Syntaxe, commentaire examens... ;
- Règles associées au code (changement d'unité, ...);
- Acceptation technique, ... ;
- Impression ou non de l'examen.

### 7.2.3 Harmonisation des systèmes unitaires

Le système unitaire entre deux systèmes interconnectés pouvant être différent, il est primordial de vérifier, pendant les vérifications, les éventuelles conversions d'unités.

Lorsqu'elle est disponible la codification LOINC présentant des codes différents en fonction du système unitaire est recommandée dans les échanges de données entre systèmes.

### 7.2.4 Gestion de l'adresse postale

En termes d'adressage, le LBM porte une attention particulière aux normes en application du ou des prestataire(s) responsable(s) qui peuvent avoir des conséquences sur la transmission des comptes rendus.

Exemple : Norme AFNOR XP Z 10-011

« Quelques règles élémentaires concernant la norme de l'adresse :

- l'adresse doit comporter 6 lignes maximum (éventuellement une 7ème pour le pays),
- d'une longueur maximum de 38 caractères,
- les informations dans l'adresse partent du plus précis (ligne 1 : Titre / Prénom / Nom) pour aller au plus vaste (ligne 6 : Code Postal / Ville),
- la dernière ligne (Code Postal / Ville) est impérativement en majuscules  
La Poste Française recommande toutefois de mettre également la ligne 4 (numéro, type de voie, voie) et la ligne 5 (lieu-dit – Boîte Postale) en majuscules, ce qui maximise la performance de la reconnaissance optique,
- Les accents, signes de ponctuation ou style (souligné, gras, ...) sont proscrits par la norme de l'adresse à partir de la ligne 4 (voie),
- les abréviations (Res., Bat., Bd, Bvd, ...) ne sont tolérées que si elles sont nécessaires pour le respect des 38 caractères par ligne »

## 7.3 Maîtrise informatique de la phase pré-analytique

### 7.3.1 Gestion informatique de l'identité des patients

(Références : SH REF 02 §5.4.5

Note : "Une procédure d'identitovigilance interne au LBM ou à l'établissement de santé est fortement recommandée".)

Etat des lieux des sources de données d'identités patients :

- SIH : données d'identités patients gérées par une administration externe au LBM ;
- Carte vitale : données d'identités gérées par l'organisme d'assurance maladie ;
- Système informatique du demandeur/prescripteur pour un LBM recevant ses demandes d'examen en format électronique, en prescription connectée ou en sous-traitance.

Le SIL gère plusieurs domaines d'identification de patient. Chaque identifiant permanent de patient est visiblement rattaché à son domaine d'identification et n'est exploité que dans le contexte de ce domaine d'identification :

- Le domaine national pour l'INS-c ;
- Autant de domaines d'identification que d'établissements de soins fournissant des données démographiques au LBM (exemple : NIP ou IPP, IEP ou NDA...) ;
- Son propre domaine pour l'identifiant interne attribué par le SIL.

Point de vigilance :



L'exploitation correcte par le SIL des domaines d'identification est primordiale : le patient identifié 1234 par la clinique A n'a aucune raison d'être la même personne que le patient identifié 1234 par l'hôpital B.

### **7.3.1.1 Identités et mouvements de patients transmis par le SIH**

La contrainte sur les identifiants permanents exposée ci-dessus s'applique de la même façon aux NDA transmis par les SIH des établissements. Le LBM s'assure que chaque NDA est rattaché au domaine d'identification de l'établissement émetteur.

La procédure d'identitovigilance du LBM prend en compte ces flux électroniques de données démographiques. Les données du SIH et/ou du SIL n'étant pas forcément exactes, la procédure intègre les modalités de correction et de communication des données « identité et mouvements de patients ».

Le LBM, en lien avec l'établissement de santé, prévoit une procédure de saisie des identités et mouvements de patients en mode dégradé afin d'assurer la continuité de service en cas de panne du SIH.

En pratique, toute discordance nécessite une étude d'impact et est gérée comme une non-conformité.

### **7.3.1.2 Données d'identité patient lues sur la carte Vitale**

Les modalités de gestion des données d'identité lues dans la carte vitale sont intégrées dans la procédure d'identitovigilance. Une attention particulière est portée à la gestion des discordances entre la carte vitale et les informations d'identité communiquées par le patient ainsi qu'à la prise en compte des cas où les données de la carte vitale du patient ne sont pas accessibles.

### **7.3.1.3 Données patients reçues dans les demandes d'examens dématérialisées**

L'association des demandes d'examens reçues du système demandeur à des dossiers patients existants dans le SIL fait l'objet des mêmes précautions que dans le cas d'une liaison fournissant identités et mouvements : utilisation des identifiants fournis dans le contexte de leur domaine d'identification ; contrôle de concordance des traits d'identité fournis avec ceux du dossier existant.

## **7.3.2 Fusion des dossiers patients**

Le recours aux fusions de dossiers permet, en réduisant les dossiers en doublons, de maintenir une cohérence du suivi des patients. La fusion de dossiers étant une opération critique, il convient que celle-ci soit tracée et effectuée par des opérateurs en nombre limité et dûment habilités. Une autorisation d'accès spécifique à cette fonctionnalité dans le SIL ou le SIH peut être prévue par le fournisseur informatique. Si ce n'est pas le cas, la procédure en tient compte.

Afin d'éviter tout problème d'identitovigilance, la fusion de dossiers de patients ayant des groupes sanguins différents n'est pas possible. Le LBM s'assure de cette impossibilité lors de la création de dossier patients-tests. Le cas échéant, le LBM prend des dispositions pour pallier le manquement de son SIL.

Plus généralement, toute discordance entre les deux dossiers à fusionner fait l'objet d'un message d'avertissement retourné par le logiciel avant validation de cette fusion. Si le logiciel n'offre pas ce mécanisme de contrôle, la procédure en tient compte.

Cette fonctionnalité devant être encadrée, il importe de définir une liste de critères permettant d'identifier les doublons lorsqu'ils sont identiques et de bloquer la fusion lorsqu'ils sont différents, ceci afin de respecter l'intégrité du dossier patient.

Exemples de critères de fusion à associer :

- Date de naissance ;
- Nom de famille ;
- Nom d'usage ;
- Prénom ;
- Groupe sanguin ;
- Adresse ;
- INS-c ;
- ...

Point de vigilance :



La fusion étant une opération critique pour le suivi des patients, il est souhaitable que si un doublon est suspecté sur l'association de plusieurs critères, la fusion en cas de discordance d'un des critères ne puisse se faire qu'après une étude de risque.

### 7.3.3 Prescription (papier et/ou connectée)

(Références : NF EN ISO 15189 §5.4.1)

La feuille de prescription parvient au LBM sous forme papier et/ou sous forme d'un flux électronique. La feuille de prescription comporte les éléments suivants :

- Identification du prescripteur et de l'organisation prescriptrice (établissement de soins et service, ou cabinet médical). L'identification peut être le nom et/ou le n°FINESS de l'organisation ;
- Identification du prescripteur et des autres médecins destinataires du compte rendu ;
- Adresse de l'organisation prescriptrice / du prescripteur et adresse des autres destinataires du compte rendu ;
- Identification univoque du patient :
  - L'identité du patient comporte son nom de famille, son prénom et le cas échéant un nom d'usage. Chacune de ces informations étant portées dans un champ individualisé et clairement identifié. En cas de prescription anonymisée, l'identité n'est pas fournie ou est remplacée par une chaîne de caractères anonymisée ;
  - Le sexe du patient est renseigné dans un champ dédié, distinct de la civilité ;
  - La date de naissance du patient est fournie, si elle est connue précisément. Pour les patients dont la date de naissance n'est pas connue précisément, celle-ci peut se résumer à une année de naissance ou à une date de naissance dite lunaire fournie par l'organisme d'assurance maladie via la carte Vitale du patient ;
  - L'INS-c du patient, si connu. En l'absence d'INS-c le LBM ou l'établissement met en œuvre une procédure d'identitovigilance renforcée ;
  - Le NDA (n° d'hospitalisation ou de visite) du patient au sein de l'établissement, lorsque l'organisation prescriptrice est un établissement.
- En cas de flux électronique, identifiant de la prescription dans le système de l'organisation prescriptrice ;
- Nom du préleveur ;

- Examens de biologie prescrits :
  - Désignation explicite, de préférence respectant la NABM, non ambiguë de chaque examen ;
  - En cas de flux électronique, codification de l'examen conforme à celle définie dans le manuel de prélèvement du LBM.
- Eléments cliniques pertinents :
  - Le(s) motif(s) de la prescription (visée diagnostique, pronostique, de suivi, de dépistage, de bilan pré-acte ou post-acte, de bilan périodique de santé...);
  - Les autres renseignements cliniques requis en fonction des examens prescrits, pour les besoins de l'interprétation des résultats.
- Pour chaque spécimen primaire requis par la prescription :
  - La nature du spécimen et le cas échéant le site de prélèvement ;
  - La date et l'heure de prélèvement dans le cas où le spécimen est fourni par l'organisation prescriptrice.

En cas de sous-traitance d'examens, la demande d'examens adressée au LBM sous-traitant sous forme papier et/ou électronique comporte les mêmes éléments que la feuille de prescription, auxquels s'ajoutent :

- L'identification du LBM demandeur :
  - Nom du LBM ;
  - N°FINESS ou identifiant attribué à ce LBM par le LBM sous-traitant.
- En cas de flux électronique, transcodage des examens sous-traités dans la codification fournie par le catalogue des examens du sous-traitant.

#### Points à vérifier sur le SIL :

L'enregistrement informatique de la feuille de prescription dans le SIL produit une demande d'examens sur laquelle on retrouve l'ensemble des informations listées ci-dessus auxquelles s'ajoutent la date et l'heure de réception des spécimens primaires au LBM.

### **7.3.4 Cas particulier de l'autocréation de demande d'examens**

Le LBM prend des dispositions afin de sécuriser ce mode de connexion.

Exemple de dispositions :

- L'opérateur analyse le spécimen sur l'analyseur sans enregistrement préalable sur le SIL ;
- Les opérateurs sont formés/habilités ;
- L'opérateur identifie son spécimen sur l'analyseur avec l'identifiant patient (IPP ou NDA) ;
- Le ou les résultats sont transmis au SIL avec l'identifiant, en connexion directe ou via un MW ;
- La demande est générée automatiquement sur le SIL qui lui affecte un numéro et y range les examens avec leurs résultats.

Il est important que le LBM définisse les paramètres de maîtrise de cette fonctionnalité, concernant :

- Le ou les élément(s) administratif(s) permettant(s) d'interroger le SIL ou le SIH afin de sécuriser l'affectation des résultats au dossier patient. Exemples : IPP, NDA, nom de famille, prénom, ... ;
- Le mode de transfert des données ainsi que leur traçabilité, ...

NB : en cas de panne de ce mode de fonctionnement, le LBM prévoit une procédure en mode dégradé afin d'assurer une diffusion des données biologiques (Cf. §7.8).

### 7.3.5 Saisie de plusieurs demandes d'examens avec des analyses communes pour un même prélèvement

Il est fréquent d'avoir plusieurs prescriptions pour un même prélèvement. Si le SIL ne peut pas rattacher plusieurs demandes d'examens à un même prélèvement, le LBM, en cas d'analyses communes, prend des dispositions (recopie automatique et/ou saisie manuelle) pour éviter de rendre des résultats différents et pour gérer les antériorités.

De façon idéale le SIL gère les antériorités en fonction de l'horodatage du prélèvement.

## 7.4 Maîtrise informatique de la phase analytique

(Référence : NF EN ISO 15189 §4.13 & 5.5)

### 7.4.1 Connexions des analyseurs en direct sur le SIL ou via MW

La sécurisation des connexions d'analyseurs, en direct ou via MW, nécessite d'établir les pré-requis avant de mettre en production les échanges d'informations entre les différents systèmes informatiques du LBM.

Le type de connexion est à définir par le LBM, en tenant compte des possibilités des différents systèmes.

Concernant le choix du format des étiquettes codes barres, le LBM respecte les caractéristiques des fournisseurs d'analyseurs.

Etat des lieux : deux modes de connexion sont utilisés à ce jour :

- **Connexion monodirectionnelle** : flux de données dans un seul sens. L'analyseur détermine (par configuration ou par saisie manuelle de l'opérateur) son ordre de travail sur un spécimen (les analyses à réaliser sur ce spécimen). Il exécute l'ordre, puis renvoie au SIL ou au MW les résultats associés à l'identifiant du spécimen ou à sa position sur l'analyseur ou à son rang dans une liste de travail.
- **Connexion bidirectionnelle** : flux de données dans les deux sens. L'analyseur obtient du SIL ou du MW son ordre de travail sur le spécimen (la liste des analyses à réaliser ainsi que les informations contextuelles nécessaires comme, par exemple, le numéro de la demande d'examens, l'identité du patient, celle du prescripteur, ...). Ce flux aller peut se dérouler de deux façons :
  - Connexion bidirectionnelle en mode chargement: le SIL ou le MW envoie au préalable les ordres de travail à l'analyseur qui les mémorise passivement en attendant de traiter les spécimens.
  - Connexion bidirectionnelle en mode interrogatif : l'analyseur est l'initiateur et interroge le SIL ou le MW au vu du spécimen (reconnaissance de l'étiquette code barre) et reçoit en réponse l'ordre de travail à exécuter pour ce spécimen.

Après avoir exécuté l'ordre de travail l'analyseur renvoie les résultats avec les informations de contexte au SIL ou au MW.

Exemples de points sensibles du flux de transmission des ordres de travail:

- Définir les éléments qui composent l'ordre de travail.
  - Numéro de spécimen : dispositions permettant d'éviter les collisions de numéros (nombre de caractères, délai de rotation, identifiant pérenne, ...) ;
  - Codes analyses : habilitation au paramétrage/maîtrise de la table de transcodage ;
  - Antériorités (valeur, date, unité, ...) ;
  - Données du dossier patient : identité, sexe, date de naissance, date d'entrée, IPP, NDA, ... ;
  - Données de la demande d'examens : numéro, prescripteur, unité de soins, données cliniques et observations fournies par le prescripteur (température, diurèse, durée d'aménorrhée, infection connue, ...) ;
  - Données du spécimen : date de prélèvement, date de réception, préleveur, risques associés, ...
- Déterminer le mode de fonctionnement de la connexion lorsque la connexion passe par un MW la composition des ordres de travail est à définir sur chacune des étapes de communication : SIL <-> MW, MW <-> analyseur. Le MW a souvent besoin de plus de données contextuelles que l'analyseur. D'autre part, le MW peut répartir le travail entre plusieurs analyseurs et produire ainsi plusieurs sous-ordres à partir de l'ordre de travail transmis par le SIL. De même, le mode de connexion est à configurer sur chacune des étapes de communication.

Exemples de points sensibles du flux de retour des résultats :

- Définir les éléments qui composent le flux de résultats. identifiants à retourner (patient, demande) ;
- Numéro de spécimen dans une taille et un format compatibles entre les deux systèmes et assurant la protection contre les collisions ;
- Codes analyses : habilitation au paramétrage/maîtrise de la table de transcodage ;
- Données du résultat : codage des résultats qualitatifs, unités des résultats numériques, alarmes codées, codes d'interprétation (> ou <, L ou H, ...), commentaires textuels et codés, ... ;
- ...
- Lorsque la connexion passe par un MW ces éléments sont à déterminer sur chacune des étapes de communication, le MW étant susceptible d'enrichir le flux de résultats initial de l'analyseur avec, par exemple, des données d'acceptation et d'interprétation des résultats. De plus, le MW est susceptible de générer des ordres de repasse, sur le même analyseur ou sur un autre, avec ou sans modification de l'ordre initial : dilution, concentration, ajout d'analyses, ... ;
- Traçabilité des opérateurs ayant réalisé (sur l'analyseur, sur le MW) une action (acceptation du résultat, interprétation, commentaire, décision de repasse, choix entre les résultats de deux passages, ...).

#### **7.4.2 Règles de contrôle du processus analytique**

La mise en place de règles opérationnelles permet d'automatiser, de standardiser et de sécuriser le processus analytique. Le LBM maîtrise l'utilisation de ces règles et s'assure de leur stabilité dans le temps.

Exemple de règles utilisées :

- Conversion d'unité ;
- Calcul d'index (MDRD...), de valeurs analytiques (LDL cholestérol, bilirubine liée, ...)
- Règle de gestion à déclenchement d'autres analytes (exemple si bilirubine totale au seuil critique faire la bilirubine libre ...)
- Règles de repasse, critères définis par le LBM ;
- ...

La criticité des règles opérationnelles est à définir par le LBM. Leur paramétrage est confié à des opérateurs habilités et est tracé. Le LBM met en place une politique concernant :

- L'exploitation ;
- La criticité ;
- La validation par l'utilisation de patients test ;
- La définition des extrêmes pour chaque type de calcul ;
- La vérification du fonctionnement des règles de gestion et le fonctionnement en cascade ;
- La traçabilité des règles mises en œuvre ;
- Le système de test en continu (règles mises en défaut, ...)
- ...

### 7.4.3 Contrôle(s) de qualité connecté(s)

Les contrôles de qualité peuvent être gérés par des systèmes informatiques comme le SIL, les MW ou d'autres systèmes. Le paramétrage des contrôles est effectué par des opérateurs habilités et selon les besoins exprimés dans la procédure de gestion des contrôles qualité (règles de Westgard par exemple).

La mise en place d'une liaison de gestion des contrôles qualité nécessite de définir des règles de fonctionnement et d'utilisation, concernant :

- Les règles de gestion des contrôles qualité avec blocage ou non de la production ;
- La traçabilité des opérations effectuées sur l'acceptation ou le refus d'un ou de plusieurs contrôles qualité ;
- La liste des opérateurs responsables de la validation des contrôles qualité ;
- La liste des opérateurs habilités à paramétrer et gérer le système des contrôles qualité en général ;
- ...

## 7.5 Maîtrise informatique de la phase post-analytique

(Référence : NF EN ISO 15189 §5.7.1 & 5.8)

### 7.5.1 Dématérialisation des données

Le format de communication des examens médicaux peut faire appel à des systèmes de transfert informatique des données (dématérialisation). Le LBM définit une politique de diffusion des comptes rendus dématérialisés.

A titre d'exemple la politique mise en œuvre peut comporter les items suivants :

- Catalogue des examens transmis avec indication du blocage de certains résultats d'examens (sérologie VIH positif, ...)
- Vérification du catalogue des examens transcodés au cours du temps et de l'évolution du SIL ;

- Modalités de transfert des données biologiques : numériques, codes textes, unités, intervalles de référence, antériorités, commentaires, prestation de conseils, techniques, ... ;
- Règles de confidentialité (par exemple pour les examens concernant le personnel de l'établissement de santé, ... ) ;
- Surveillance de fonctionnement de ce mode de diffusion (mise en place d'un tableau de bord, ... ) ;
- Traçabilité de la consultation des comptes rendus par les tiers ;
- ...

#### 7.5.1.1 Serveurs de résultats intégrés à la chaîne de production des soins

Les serveurs de résultats sont exploitables dans le respect des dispositions concernant l'agrément des hébergeurs de données de santé exposées au chapitre 6.2.5.

Le LBM en concertation avec ses correspondants (prescripteur, personnel médical et paramédical, patient, ...) définit les droits d'accès, la durée de disponibilité, et les modalités de consultation des données pour :

- Les prescripteurs ;
- Les établissements de santé, accès par prescripteur, service, UF, ... Une attention particulière est portée en cas de mise en place d'un accès en mode « urgence vitale » (« bris de glace ») ;
- Les IDE, le personnel paramédical ;
- Les patients.

Une traçabilité nominative est mise en place.

##### Point de vigilance :



Le LBM prend des dispositions concernant la transmission des résultats jugés préoccupants et des examens à diffusion restreinte.

Exemple de modalité de consultation pour les patients lorsque le LBM met à disposition sur son serveur de résultats, les comptes rendus d'examens de biologie médicale pour les patients ayant donné leur accord explicite :

- Le compte rendu est disponible pendant une durée déterminée et la notification de sa disponibilité se fait par mail et/ou SMS ;
- L'accès se fait via un login et un mot de passe, communiqués séparément au patient. Un dispositif de mot de passe à usage unique transmis au patient par SMS ou mail, au moment de la connexion, donne un meilleur niveau de sécurité ;
- Le compte rendu n'est mis à disposition que lorsqu'il est complet.

#### 7.5.1.2 Passerelle d'échange

Dans certains contextes (en particulier en contexte hospitalier), les échanges post-analytiques peuvent être assurés par une passerelle d'échange ou EAI (Enterprise Application Integration). Le LBM qui souhaite s'équiper d'une nouvelle passerelle porte une attention particulière aux critères suivants :

- Connecteur DMP compatible disponible (liste disponible sur le site de l'ASIP Santé) ;
- Support d'une messagerie sécurisée de santé ;
- Possibilité de réceptionner les résultats des LBM sous-traitants.

## 7.5.2 Transfert des données par Module Fax informatique

(Référence : SH REF 02 §5.8)

La liaison SIL ↔ ligne téléphonique (mode fax) nécessite une maîtrise des points critiques suivants :

- L'intégrité des numéros de fax utilisés ;
- La mise en place d'une convention de preuve avec le tiers (Cf. annexe 1) ;
- Le suivi de la transmission (par exemple via un « Tableau de bord ») ;
- La traçabilité de la transmission.

## 7.5.3 Signature électronique et signature électronique présumé fiable

*Sous chapitre non développé dans l'attente du ou des textes législatifs d'application précisant les modalités de mise en place de la signature électronique présumée fiable.*

## 7.5.4 Systèmes d'aide à la validation biologique (SAVB)

Ces logiciels sont basés sur la combinaison d'un ensemble de règles d'expertise assorties de règles de priorité. Un tel système peut devenir un outil complexe à la faveur de l'accumulation et de l'interaction de règles multicritères du type : âge du patient, sexe, délai entre deux examens, évolution d'un résultat d'analyse dans ce délai, résultats d'autres analyses, indice de priorité de règle, ...

Les recommandations de ce chapitre s'appliquent aux règles d'expertise qui peuvent faire partie intégrante d'un SIL. En revanche, les systèmes experts intimement liés à des automates d'analyse sont, au titre des DM DIV, exclus du champ de ce présent document puisqu'ils sont soumis à une validation ou vérification de méthode (logiciels de calcul de risques de trisomie 21, systèmes experts d'antibiogramme, ...).

On s'assurera que les règles sont pertinentes, en vérifiant que le comité de spécialistes qui les a élaborées soit qualifié et que le système ait prouvé son efficacité via un dossier de validation.

### 7.5.4.1 Catégories de systèmes

▪ Les SAVB dits "partiellement ouverts" :

Dans ce cas le système est livré avec un ensemble de règles d'expertise préprogrammées, non modifiables, et leur mécanisme d'action est parfois inaccessible.

▪ Les SAVB dits « ouverts » :

Dans ce cas les règles sont toutes librement paramétrables. L'élaboration de ces règles qui représente un point sensible est maîtrisée par les biologistes.

### 7.5.4.2 Etudes préalables à l'adoption

La préparation au choix d'un tel système peut avantageusement passer par une analyse de risque afin de lister les écueils, d'adapter la taille et la durée des tests.

A réception, la vérification de l'adaptation du SAVB au contexte informatique et clinico-biologique du LBM est vivement recommandée.

Par exemple, un jeu-test de demandes d'examens par famille (Biochimie générale et spécialisée, Hémostase, ...) contenant l'ensemble des analyses concernées est mis en œuvre. Chaque analyse reçoit ensuite des résultats choisis pour leur diversité, leur caractère extrême ou selon les conséquences cliniques qui peuvent en découler. Enfin un jeu-test multi-familles de taille au moins identique pourra être utilisé dans le cas où plusieurs

analyses de ces familles interagissent au sein des règles.

La pertinence des expertises opérées est examinée avec soin par le biologiste.

Dans le cas où le SAVB est un logiciel indépendant du SIL, la mise en place de la connexion est une phase aussi poussée qu'une connexion type MW (Cf. §7.4).

#### **7.5.4.3 Paramétrages des règles d'expertise**

L'élaboration des règles d'expertise représente un point sensible qui est maîtrisé par les biologistes.

Il est recommandé que les règles :

- Soient validées par un comité de paramétrage constitué de biologistes exerçant dans le LBM ;
- Fassent l'objet d'enregistrements facilement disponibles et compréhensibles ;
- Aient été approuvées par tous les biologistes de l'établissement par exemple au cours d'habilitations en tant que signataires ;
- Ne soient modifiables que par un personnel autorisé choisi parmi le comité de paramétrage ;
- Aient été testées sur un nombre suffisant de demandes d'examens en rapport avec l'étude de risque menée.

Avant la mise en situation réelle, il est souhaitable de prévoir une phase probatoire pour les nouvelles règles. Celle-ci consiste à laisser agir le SAVB mais à maintenir une expertise, par les biologistes, des résultats de chaque demande d'examens. Les biologistes auront été correctement informés de cette activité de surveillance. Il en est de même pour toute évolution substantielle d'une règle.

Par exemple, à la suite de la modification de la règle d'expertise de la créatinine, le LBM pourra procéder à une phase probatoire d'un mois au cours de laquelle tous les examens contenant cette analyse seront retenus dans le menu des résultats à valider et assortis d'un marquage signifiant "*nouvelle règle d'expertise en test pour la créatinine*" du type « flag, zone colorée, un message court, ... ».

#### **7.5.4.4 Exploitation du système**

La trace de l'expertise d'une demande d'examens biologique par le SAVB est parfaitement visible, de préférence au niveau du tableau de bord de validation, avec un niveau de détail permettant de voir le comportement du système pour chaque analyse (flag, couleur, ...).

#### **7.5.4.5 Surveillance du système**

Le comportement du SAVB est périodiquement évalué, par une combinaison de moyens. Toute anomalie ou même toute insuffisance fait l'objet d'une action corrective.

On pourra par exemple mettre en œuvre :

- Une série de demandes-test. Le LBM peut entretenir un jeu de demandes d'examens, à définir, comportant de nombreuses analyses dont les résultats ont été choisis pour leur criticité et leur aptitude à faire fonctionner les règles en situation complexe. A période définie, trimestrielle ou semestrielle, ces examens sont représentés afin d'être de nouveau expertisés par le SAVB. Les indicateurs d'expertise (flag, couleur, ...) spécifiques à chaque analyse sont examinés et comparés à la situation attendue. Des copies d'écrans sont conservées comme traçabilité de la vérification.

- L'examen détaillé d'une série de demandes d'examen. Le biologiste d'un site est désigné pour examiner rétrospectivement toutes les demandes examens expertisées par le SAVB sur une période donnée (journée, demi-journée, ...) pour s'assurer de la pertinence des expertises effectuées par celui-ci. Cette évaluation est faite périodiquement : trimestrielle, semestrielle, ... Cela implique que le SIL trie dans une entité dédiée (menu, dossier, répertoire, ...) et sur une période donnée, les demandes dont au moins un résultat d'examen aura été expertisé par le SAVB.
- L'exploitation périodique des alarmes. Tout SAVB est équipé d'un système de détection des conflits entre règles décisionnelles qui conduit à :
  - La non expertise du ou des résultats concernés ;
  - L'enregistrement d'une alarme détaillant les sources du dysfonctionnement dans une entité facilement accessible par le biologiste.Le LBM peut mettre en place un examen périodique (hebdomadaire, mensuel, ...) de ces alarmes.
- Le suivi statistique des non-conformités et des réclamations liées à cette expertise assistée. Une sensibilisation au caractère systématique de leur enregistrement est ici tout particulièrement indiquée auprès de tous les acteurs du LBM.

## 7.6 Organigramme informatique

Le LBM met en place des dispositions visant à organiser les responsabilités informatiques ainsi que les niveaux d'habilitation afin d'en assurer la maîtrise.

S'il il le juge nécessaire, le LBM nomme un responsable informatique et éventuellement un suppléant. Ces nominations peuvent faire appel à des personnes internes et/ou externes au LBM en fonction des compétences et/ou de l'intégration du LBM dans une structure possédant une direction des systèmes d'information. Les fonctions et responsabilités sont définies (Cf. annexe 2).

Les responsabilités informatiques pouvant être à périmètre variable, il est nécessaire de définir précisément le rôle de chacun sur différents points comme :

- Gestion du catalogue des examens dans le SIL, paramétrage, mise à jour ;
- Gestion des connexions, paramétrage, maintenance, supervision ;
- Gestion des échanges électroniques, données d'identités et de mouvements, résultats ;
- Identitovigilance ;
- Gestion de l'impression et de la mise sous pli des résultats ;
- Gestion du parc matériel ;
- ...

En cas d'externalisation de responsabilités critiques concernant la sécurité ou la disponibilité du système, l'organigramme précise le contrat fournisseur qui couvre cette responsabilité. Le contrat fournisseur contient explicitement cette responsabilité et les conditions qui s'y appliquent en particulier sur les aspects :

- Sécurité des postes clients (antivirus, accès, ...) ;
- Sécurité du réseau (firewall, authentification réseau, VPN, ...) ;
- Redondance.

## 7.7 Maîtrise de la sécurité informatique

(Référence : SH REF 02 §5.3.11 « *Le LBM met en place des dispositions visant à maîtriser ses systèmes informatiques (SIL, système d'aide à la validation, middleware, serveur de résultats, ...)* :

- *droits d'accès (confidentialité, authentification, hiérarchisation des accès, ...),»*)

### 7.7.1 Sensibilisation des utilisateurs à la sécurité informatique

Une charte informatique est recommandée.

(Cf. annexe 3)

### 7.7.2 Sécurité du système - Droits d'accès (hiérarchisation des accès, ...)

Le SIL et la plupart des systèmes informatiques disposent d'un module LDAP de gestion des droits d'accès (Cf. §6). Si ce n'est pas le cas, les procédures en tiennent compte. Les droits d'accès sont à définir sur le SIL et les systèmes associés. Les intervenants sont référencés et les modifications tracées (Cf. §7.9). Il est vérifié que les droits définis sont en adéquation avec leurs compétences.

Exemple de hiérarchisation :

- Les intervenants : techniciens, secrétaires, biologistes, qualitatifs, ... ;
- Les fonctions : référent technique, référent métrologie, ... ;
- Les niveaux d'habilitation : maîtres ou administrateurs, utilisateurs, ... ;
- Les droits d'accès :
  - Validation ;
  - Paramétrage examens ;
  - Accès aux modifications administratives ;
  - Accès aux fusions de dossiers ;
  - Accès aux modifications de résultats après validation biologique ;
  - ...

### 7.7.3 Délai de verrouillage après inactivité

Afin de garantir l'immutabilité des actions aux utilisateurs, il est important de définir un délai de verrouillage ou déconnexion sur inactivité avec masquage des données affichées. Afin de protéger les données, de garantir la sécurité du système et de s'assurer de la traçabilité des actions, le LBM indique dans sa politique de sécurité informatique les modalités de verrouillage :

- Au moment de quitter son poste de travail ;
- En fonction d'un temps prédéfini d'inactivité ;
- En cas de changement d'utilisateur.

Certains LDAP (Cf. §6) permettent de définir de manière centralisée ce délai pour tous les postes et tous les utilisateurs authentifiés.

## 7.8 Procédures en cas de panne informatique : mode dégradé

Le LBM prévoit en cas de panne d'un ou de plusieurs de ses serveurs critiques (Cf. §6.2.2) une procédure en mode dégradé afin d'assurer la continuité de service.

Elle intègre notamment les modalités :

- De gestion des examens critiques et des demandes d'examens urgentes ;
- De communication des résultats ;
- ...

Le mode dégradé implique la mise en place d'un plan de continuité adapté en fonction de chaque incident (panne d'une ou plusieurs connexions, panne MW, panne SIL, panne serveur de résultats, ...).

Ce plan intègre :

- L'analyse de risques ;
- La reprise d'activité ;
- Les modalités de reprise des données (administratives, résultats, autres, ...) ;
- Les modalités de traçabilité.

Exemple de stratégie en mode dégradé (schéma à trois étapes) :

♦ Etape 1 : Etiquettes pré-imprimées

- génération de numéros avec le nombre de caractères habituellement utilisé au sein de la structure.

♦ Etape 2 : Le SIL est en panne – fonctionnement en mode dégradé ou après coupure du SIL

- Principe d'utilisation simple, chaque prélèvement du dossier se verra affecter un numéro à partir des « étiquettes pré-imprimées/panne » préparées en avance ;
- Ce numéro est défini au préalable (il n'est en aucun cas susceptible d'entrer en conflit avec un numéro habituellement attribué par le SIL) ;
- Le LBM prévient s'il le juge nécessaire les tiers ;
- Le LBM garde un listing papier de l'analyseur (impératif) et de la communication des résultats :
  - Rendu par les analyseurs ou MW ;
  - En respectant le plus possible les unités habituellement utilisées ;
  - ...

♦ Etape 3 : Le système redémarre – récupération des informations

- Le LBM prévient les tiers si nécessaire de la reprise et met en œuvre une stratégie :
  - D'enregistrement pour chaque demande d'examens avec les natures de prélèvement s'y rattachant ;
  - De changement de l'heure (et éventuellement de la date) sur chaque demande d'examens ;
  - De récupération des résultats des automates et concentrateurs ;
  - ...

## 7.9 Traçabilité, Intégrité et Conservation des données

### 7.9.1 Traçabilité des données

(Référence : SH REF 02 §4.13 « La durée de conservation des enregistrements, utiles pour garantir la traçabilité, doit être conforme à la réglementation en vigueur et satisfaire à la fois les besoins des patients, des prescripteurs et du LBM. Afin de permettre la réalisation successive de 2 évaluations Cofrac, elle ne peut être inférieure à 18 mois. »)

La traçabilité joue un rôle important dans la surveillance et l'appréciation de la qualité du processus analytique, ceci afin d'être en mesure d'agir de façon curative pour rectifier le plus rapidement possible la conformité du processus. Le LBM met en place les dispositifs, dès que cela est pertinent et critique, de traçabilité et ceci tout au long du processus analytique en incluant le système de management de la qualité (SMQ). La traçabilité informatique est un procédé qui permet l'observation d'une trace d'une action réalisée soit par :

- Un des acteurs effecteurs (techniciens, secrétaires, biologistes, ...)
- Un des systèmes (liaison identité, SAVB, MW, ...).

Point de vigilance :



Le LBM prend des dispositions concernant la traçabilité des modifications de paramétrage.

### 7.9.2 Intégrité des données

(Référence : SH REF 02 §5.3.11)

Les données et enregistrements qu'ils soient d'ordres administratifs, biologiques, techniques (CIQ, Maintenances, calibrations, ...) ou communicatifs, nécessitent pour le LBM de définir des dispositions permettant de maîtriser l'intégrité de ses informations.

Exemples :

- Exploitation des données analyseur sauvegardées (accès, lecture par logiciel automate (format exploitable ou lisible), ...)
- ...

### 7.9.3 Archivage des données

Le LBM met en œuvre une procédure d'archivage des données biologiques et des données du système qualité. L'objectif est de pouvoir relire les données au cours du temps sans perte d'information. La durée de conservation des données est conforme à la réglementation en vigueur et ne peut être inférieure à 18 mois afin de garantir la traçabilité entre deux évaluations successives Cofrac.

### 7.9.4 Archivage des demandes et des comptes rendus

La notion d'archivage désigne deux opérations distinctes dans le SIL :

- Le traitement de clôture d'une demande d'examen dont la phase post-analytique est terminée et dont la facture est générée. Il convient de verrouiller les possibilités de modifier les résultats et les prestations de cette demande, tout en la laissant accessible en ligne, pour consultation, ainsi que pour la poursuite du processus de facturation/recouvrement des prestations ;
- Le traitement d'archivage du compte rendu d'examen d'une demande, dans le format dans lequel il a été diffusé.

#### **7.9.4.1 Archivage/désarchivage des demandes d'examens en ligne**

Lorsque le post-analytique et la facturation d'une demande d'examens sont effectués, cette demande peut être basculée dans le statut « archivé » (appelé aussi « clôturé » ou « terminé » selon les SIL). C'est ce changement de statut que l'on appelle l'archivage en ligne des demandes d'examen.

Une demande dans le statut « archivé » a les caractéristiques suivantes :

- La demande reste accessible en ligne dans l'application avec l'intégralité de ses données, traçabilité comprise ;
- La demande est non modifiable (prestations, résultats, interprétation, compte rendu, ...).

L'archivage est réversible : le SIL offre une fonction de désarchivage d'une sélection de demandes d'examens, qui consiste à rebasculer ces demandes dans le statut « en cours ». Une demande désarchivée peut à nouveau être modifiée comme toute demande en cours, avec les mêmes conditions et répercussions :

- Toute modification d'examen, d'analyse, de résultat, réactive les phases analytique (notamment l'acceptation des résultats modifiés) et post-analytique (validation, rediffusion du compte rendu correctif aux destinataires) ;
- Une modification d'un des éléments d'identification du dossier patient (nom, prénom, sexe, date de naissance) est répercutée sur la chaîne analytique dans la mesure où la phase analytique de cette demande a été ré-ouverte.

Une fois les opérations ayant nécessité le désarchivage effectuées, et le cas échéant, après diffusion d'un nouveau compte rendu correctif, la demande d'examen peut être à nouveau basculée dans le statut « archivé ».

#### **7.9.4.2 Archivage des compte rendus dans leur format de diffusion**

En parallèle de l'archivage en ligne des demandes d'examen, le compte rendu diffusé sous format papier ou électronique est archivé sous son format de diffusion, et conservé dans un fichier informatique. Il est un élément majeur de la preuve légale du rendu de résultat. Si le fichier a fait l'objet d'une signature électronique, c'est le fichier signé électroniquement qui est archivé. Dans le cas d'un résultat d'examen qui a fait l'objet d'un rendu partiel puis complet ou d'un « désarchivage » puis « réarchivage », tous les fichiers résultats générés et transmis sont conservés.

Pour assurer la pérennité de format, deux formats principaux sont à privilégier :

- PDF/A : la spécification PDF/A-1 a été publiée par l'ISO et est utilisée par les organismes de normalisation du monde entier pour garantir la sécurité et la fiabilité de la diffusion des échanges de documents électroniques. PDF/A-1 optimise l'indépendance matérielle et logicielle. Le contenu de la norme ISO 19005-1 est très complet. Il comprend la définition du format PDF/A-1, mais aussi la façon de développer un outil de visualisation de fichier conforme à ce format. Cela garantit ainsi la possibilité future de toujours disposer d'un outil de visualisation ;
- Le format « compte rendu structuré de biologie » tel que spécifié par le cadre d'interopérabilité des SI de santé. Ce format s'appuie sur le standard CDA. Ses spécifications sont pérennes et compatibles avec une indépendance matérielle et logicielle.

### 7.9.5 Cas d'un changement de SIL

Dans le cas d'un changement de SIL (choix informatique ou rapprochement entre LBM), le système précédent est conservé en ligne pendant 18 mois pour permettre la vérification de traçabilité entre deux audits Cofrac. Après ce délai, l'archivage des comptes rendus dans leur format de diffusion dans la mesure où les résultats peuvent être retrouvés dans un laps de temps compatible avec les besoins des destinataires.

### 7.9.6 Cas spécifique du séquençage

Les techniques de séquençage ADN génèrent des données brutes très volumineuses en particulier dans le cas du séquençage à haut débit. L'objectif de la conservation des données brutes est de pouvoir assurer la traçabilité des données qui ont permis d'arriver à la conclusion. Si le système se compose d'un séquenceur puis d'un programme informatique complémentaire d'analyse des séquences, les deux étant fournis et validés par un seul et même fournisseur, la conservation des données utilisées dans les algorithmes de conclusion est suffisante.

Dans le cas où le LBM développe et valide son propre programme de bioinformatique, il conserve les données brutes du séquençage.

## 7.10 Sauvegarde des données

Il faut différencier sauvegarde des données et archivage des données. La sauvegarde des données est réalisée pour éviter toute perte de données dans le cas d'un incident majeur (crash système, incendie, ...) alors que l'archivage est réalisé pour « figer » les données importantes ou à valeur contractuelle d'un système d'information. Les archives sont d'ailleurs elles-mêmes sauvegardées.

### 7.10.1 Types de sauvegarde

Il existe de nombreuses stratégies de sauvegardes de données dont les grands types sont :

- La sauvegarde totale qui fait une image de l'ensemble d'un système à un instant donné. Cette sauvegarde considère aussi bien les fichiers relatifs à la base de données, les programmes du SIL, les traces et les archives ;
- La sauvegarde incrémentale (ou partielle) qui fait suite à une sauvegarde totale et enregistre uniquement les données modifiées depuis la dernière sauvegarde totale ou incrémentale. Ce type de sauvegarde est beaucoup plus rapide à réaliser mais nécessite aussi un délai plus important en cas de restauration (restauration d'abord de la sauvegarde totale puis des toutes les sauvegardes incrémentales) ;
- La sauvegarde en temps réel qui duplique chaque enregistrement sur deux dispositifs de stockage complètement dissociés (voir distants). La sauvegarde en temps réel peut-être réalisée par des logiciels spécifiques ou directement par les dispositifs de stockage eux même ;
- La sauvegarde de la base de données seule. Cette sauvegarde est considérée comme une sauvegarde partielle. Une mise à jour de la base de données pouvant être disponible pendant la sauvegarde, la sauvegarde peut être corrompue si le SIL n'est pas prévu pour une sauvegarde à système ouvert.

#### Point de vigilance :



Le LBM définit en partenariat avec son fournisseur de SIL les sauvegardes à effectuer et s'assure de leurs bons déroulements.



Les systèmes dits en cluster (un serveur principal et un serveur de secours) sur un seul et même site utilisent souvent un seul et même dispositif de stockage qui devient le maillon le moins redondant du système, ce qui nécessite une surveillance accrue du LBM pour s'assurer de son bon fonctionnement.

### 7.10.2 Supports de sauvegarde

Pour être parfaitement sécurisé, les sauvegardes sont réalisées sur deux supports différents, l'un des deux supports étant considéré comme une sauvegarde « hors feu » qui permet de réaliser une restauration en cas de destruction du site où se situe le système informatique, l'autre support permettant de faire une restauration dans un délai plus court et ne nécessitant pas de logistique particulière.

La sauvegarde « hors feu » contient l'ensemble des données patients. Elle est sécurisée physiquement et logiquement. Le fichier de sauvegarde est de préférence crypté et sécurisé avec un mot de passe pour éviter tout risque d'accès aux données en cas de vol pendant le déplacement. Le lieu de stockage est fermé à clé est accessible à un personnel habilité.

Donnons différents exemples de configuration de sauvegarde :

- Le SIL est sur un seul serveur qui est sauvegardé sur un disque externe. Cette même sauvegarde est aussi dupliquée sur bande magnétique (compression avec mot de passe) et la bande externalisée dans un local sécurisé sur un autre site ou un autre bâtiment du même site ;
- Le SIL est un système en haute disponibilité installé sur des serveurs sur deux sites physiques distants avec une réplication en temps réel entre les deux sites. Une sauvegarde est réalisée de manière périodique sur bande magnétique. La réplication en temps réel entre les deux sites est considérée comme une sauvegarde « hors feu » et aucune autre externalisation n'est nécessaire.

Point de vigilance :



La plus part des serveurs disposent de disques dits en RAID (réplication des données sur plusieurs disques dans le même dispositif de stockage). Ces disques étant dans le même dispositif de stockage, le RAID n'est pas considéré comme un système de sauvegarde mais simplement comme un système permettant une continuité de service cas de dysfonctionnement de l'un des disques.

### 7.10.3 Fréquence des sauvegardes

Après analyse des risques et des contraintes d'interruption et de restauration de service, le LBM définit dans son système qualité la fréquence des différentes sauvegarde et la fréquence d'externalisation des sauvegardes « hors feu ».

### 7.10.4 Sauvegarde et hébergement de données de santé

L'agrément hébergeur de données de santé implique le respect des règles énoncées ci-dessus. Le LBM hébergeant son SIL chez un hébergeur agréé dispose de fait d'un dispositif de sauvegarde garantissant l'intégrité et la sécurisation de ses données et de ses sauvegardes.

## 8 VALIDATION ET VERIFICATION DES SYSTEMES INFORMATIQUES

### 8.1 Données fournisseurs (marquage CE DM DIV)

A réception d'un système informatique, le LBM s'assure de la conformité des pré-requis exprimés au niveau de son cahier des charges ou de son appel d'offres. Le fournisseur remet au LBM les éléments attestant du bon fonctionnement du système informatique.

Certains logiciels disposent d'un marquage CE DM DIV. Il s'agit de logiciels isolés (non intégrés dans un dispositif médical) ayant une fonction de génération d'information nouvelle à finalité médicale (systèmes experts). La notion de risque n'est pas un critère de qualification. Le LBM adapte le niveau de vérification en fonction de ses exigences et du référentiel applicable.

NB : Quel que soit le logiciel, en cas d'incident consistant en une défaillance ou une altération des caractéristiques ou des performances de ces systèmes, ou une inadéquation de la notice d'utilisation, susceptibles d'entraîner des effets néfastes pour la santé des personnes, le LBM procède à un signalement à l'ANSM. A cet effet, le LBM intègre dans sa procédure de vigilance un dispositif afin de répondre à cette obligation réglementaire.

Les modalités de signalement sont disponibles sur le site de l'ANSM.

### 8.2 Vérification du paramétrage (examens, textes codés, connexions, règles)

Le paramétrage comprend trois phases :

- Phase de création ;
  - Expression du ou des besoin(s), par exemple à l'aide d'un enregistrement (Cf. annexe 4 – Exemple 1) ;
  - Conservation ou non des antériorités en cas de changement de méthode d'un examen existant ;
  - ...

NB : si le dossier de vérification/validation de méthode autorise la conservation de l'examen et des antériorités (résultats comparables entre l'ancienne et la nouvelle méthode), le LBM s'assure que les demandes d'examens créées antérieurement à la mise en service de la nouvelle méthode contiennent bien, en cas de réédition du compte rendu, toutes les données initiales (nom de la méthode, identification de l'analyseur, intervalle de référence, ...).

- Phase de vérification avant mise en service :

Le LBM réalise un jeu d'essai de patients tests afin de garantir la fonctionnalité du paramétrage et couvrir la majorité des scénarii (syntaxe, erreur automate, ...). Toutes les étapes de la saisie des demandes jusqu'à l'impression ou la transmission des résultats doivent faire l'objet de vérifications. Les preuves de vérification sont apportées par la réalisation de dossiers « patient-test », à chaque création d'examen, de connexion, de règle et de tout texte codé jugé critique par le LBM (par exemple les textes codés utilisés dans la saisie d'un groupe sanguin).

- Phase de production :

Au cours de l'existence d'un examen, le LBM peut être confronté à un scénario non testé ayant ou non une conséquence sur le rendu des résultats. Un correctif du paramétrage est

effectué et tracé sur l'examen. Une analyse de l'étendue de ce scénario est réalisée par le LBM.

Notion de jeux d'essai de patients tests :

La vérification des fonctionnalités du système, des transferts de données, ou de l'intégrité des données dans le temps est généralement effectuée à l'aide de « patients tests ». Ce sont des dossiers patients fictifs créés à la demande en fonction des items que le LBM souhaite vérifier, ou des dossiers patients réels qui contiennent les données ou les examens dont le LBM souhaite se servir pour vérifier le bon fonctionnement du processus testé.

Ces patients tests permettent de vérifier « de point à point » le bon fonctionnement du système. Par exemple, lorsque l'on souhaite vérifier le bon transfert des données entre l'automate et le SIL via le MW, la correspondance entre les données brutes issues de l'automate et les résultats présents sur le compte rendu permet de valider (ou d'invalider) le bon transfert des données, la bonne gestion des arrondis, des calculs secondaires, des commentaires et texte codés automatisés, ou encore le bon fonctionnement des règles d'expertise du MW, ...

Le LBM s'attache à choisir des dossiers test en fonction du processus à vérifier en termes de :

- Contenu des dossiers (type d'examens, sexe, tranches d'âge, ...);
- Nombre de dossiers (suffisant pour tester « toutes les conditions »);
- ...

Il peut être utile, notamment en cas de mauvais fonctionnement de vérifier les fichiers de transferts utilisés aux différentes interfaces, mais cela nécessite un minimum de compétences en informatique pour leur exploitation.

Dans le cas des automates péri-analytiques, les patients tests peuvent également être accompagnés d'échantillons primaires afin de vérifier l'ensemble du processus d'aliquotage/sérothéguage. Une réalisation effective des analyses peut également être réalisée afin de vérifier le processus dans son intégralité.

Enfin, dans de nombreux cas la vérification du transfert de données peut se faire « au fil de l'eau » à l'aide des données réelles produites par la gestion quotidienne des examens. Par exemple en hématocytologie, lorsque le résultat de l'automate induit une vérification sur lame, l'opérateur peut en saisissant les résultats de son contrôle de formule vérifier en même temps le bon transfert des données de la numération et tracer cette vérification directement sur le « ticket automate » utilisé.

Dans la suite de ce guide, la notion de patients tests correspond à minima à une vérification de type « point à point ».

### **8.2.1 Examens**

Le paramétrage d'un examen est une opération critique qu'il convient de vérifier et de valider avant mise en service en se concentrant à minima sur les points suivants :

- Facteur de conversion (unités internationales / unités conventionnelles) ;
- Pertinence du nombre de chiffres significatifs dans les règles d'arrondissements. Il ressort que le nombre de chiffres significatifs peut être différent selon que l'on exprime les unités en SI ou en unités conventionnelles ;  
Exemple de la créatininémie : ne pas rendre de décimales pour les résultats exprimés en micromoles/l ; en revanche, il convient d'exprimer avec une décimale les résultats en unités conventionnelles (mg/l) ;

- Intervalles de référence : être particulièrement attentif dans la définition des tranches d'âges utilisées (jours, mois, années) ;
- Calculs intra ou inter analyses ;
- Choix du format d'étiquette code à barres;
- Vérification de la connexion (Cf. §8.2.3).

La modification d'un paramétrage d'examen est tracée avec une gestion de version et une possibilité de retour arrière.  
(Cf. annexe 4 – Exemple 2)

### **8.2.2 Textes ou commentaires codés**

Les textes codés sont également vérifiés avant utilisation en s'assurant de la concordance du code choisi avec le texte imprimé sur le compte rendu.

Les textes jugés non critiques peuvent être contrôlés par simple échantillonnage.  
(Cf. annexe 4 – Exemple 3)

### **8.2.3 Vérification des connexions**

Avant mise en service, le LBM vérifie les connexions analyseur <-> SIL et/ou analyseur <-> MW <-> SIL. A noter que la vérification se fait pour les connexions vers des systèmes hors du périmètre du marquage CE DM DIV de l'automate ou du système informatique.

Là encore, la réalisation de patients tests est souhaitable. Les preuves de vérifications peuvent être apportées par des copies d'écrans des différentes interfaces, ou la confrontation des données d'entrées (par exemple résultats de l'analyseur) et de sortie (par exemple compte-rendu d'examen).

La vérification de chacune des connexions est également à faire dans le cas d'un MW partagé avec plusieurs SIL. Même si la vérification peut être réalisée « de point à point », il est important de vérifier toutes les connexions.

(Cf. annexe 5)

### **8.2.4 Vérification des règles de gestion des examens**

Avant mise en service, le LBM vérifie la fonctionnalité des règles. Le LBM effectue des tests de cohérence afin de garantir l'efficacité des règles mises en œuvre.

Dans ce cas, l'analyse du processus considéré est déterminante pour le choix du type et du nombre de patients tests à effectuer.

(Cf. annexe 6)

### **8.2.5 Vérification des alarmes transmises par les analyseurs**

Il est important de vérifier dans le paramétrage de la connexion les modalités de transmission et de gestion des codes d'alarmes transmis par les analyseurs et de s'assurer que les éventuelles règles associées s'appliquent correctement.

Comme pour les règles d'expertise du MW, l'analyse du processus considéré est déterminante pour le choix du type et du nombre de patients tests à effectuer.

(Cf. annexe 7)

## 8.2.6 Format de rendu du résultat

### 8.2.6.1 Chiffres significatifs

Le nombre de chiffres significatifs d'un résultat dépend de la valeur de son incertitude. Les règles suivantes peuvent être appliquées :

- Arrondir l'incertitude élargie à deux chiffres significatifs en majorant ;
- Arrondir le résultat avec le même nombre de décimales que l'incertitude.

Exemple	
Mesure brute :	5,6789
Incertitude associée	0,6243
Résultat	5,68 (+/- 0,63)

### 8.2.6.2 Règles d'arrondissement

Le biologiste veille à l'homogénéité du précédé employé :

- Troncature simple (déconseillée) ;
- Arrondi arithmétique (le plus courant en France) ;
- Arrondi au chiffre pair (employé dans certains pays et dans la finance).

## 8.3 Vérification initiale (ou intégration fonctionnelle)

Le LBM vérifie à l'aide de patients tests la chaîne d'information afin :

- De s'assurer de la transmission sans perte et/ou modification inappropriée des données d'un système à l'autre ;
- De valider les différents scénarii auxquels le LBM est confronté :
  - Vérification de cas courants (en tenant compte des limites de détection des techniques, vérifier la syntaxe >, <, ...)
  - Vérification de cas extrêmes, des alarmes analyseurs, ... ;
  - Vérification de cas ayant déjà posé problème(s) par le passé.

La vérification de transmission des données peut être effectuée par le biais de comparaisons de copies d'écran réalisées sur différents postes et à différentes étapes du processus (Cf. annexe 8), ou par comparaison de type « point à point » (Cf. §8.2).

Preuves documentaires possibles :

- Le LBM met en place une recette d'intégration visant à valider, d'un point de vue fonctionnel, que la nouvelle interface et/ou interopérabilité développée par le prestataire est bien conforme aux besoins fonctionnels réglementaires et/ou exprimés ;
- Le LBM trace les intégrations des interfaces et/ou interopérabilité des différents systèmes informatiques utilisés (SIL, MW, Système expert, ...) et conserve les preuves (copies d'écran, ...).

Exemple de recette d'intégration fonctionnelle:

La livraison par un prestataire d'une nouvelle version de la « liaison médecin de ville/LBM », afin de gérer les correspondants (autres médecins, unité de soins, ...), peut s'effectuer ainsi :

- Définition de correspondants dans le SIL ;
- Validation d'un résultat pour le prescripteur et les correspondants ;
- Vérification de la génération des fichiers pour l'ensemble des destinataires ;
- Vérification du format de fichier (entête, corps de fichiers, pied de page) ;

- Vérification de la cohérence des fichiers avec les données de biologie présentes dans le SIL ;
- Vérification des zones communes et différentes dans les fichiers générés, toutes les données devant être identiques sauf au niveau des données prescripteurs à savoir le nom de fichier et l'entête ;
- Là encore une vérification de type « point à point » entre les données validées issues du SIL (compte rendu) et les données visualisées ou imprimées à partir du logiciel médecin permet de valider le bon fonctionnement de la connexion.

#### 8.4 Vérification après changement de version (ou non régression fonctionnelle)

Une analyse de risques est réalisée afin d'évaluer l'impact du changement de version (vérification des échanges de données, formation des utilisateurs, mise à jour des procédures, ...). Celle-ci est fondée sur la consultation du rapport d'intervention que transmet le fournisseur de l'analyseur ou informatique au LBM. La mise en place d'un environnement de qualification (base de tests) sécurise la validation d'une nouvelle version de logiciel avant sa mise en production.

##### Point de vigilance :



Le LBM assure la traçabilité des modifications effectuées et des rapports d'intervention et prend des dispositions permettant d'informer le responsable des systèmes d'information lors de toute modification de logiciel, en particulier lors d'intervention extérieure.

Tout changement de version d'un logiciel embarqué sur un analyseur ou d'un SIL est évalué en fonction de l'analyse de risques dès son installation et fait l'objet de réalisation de patients tests. De même le changement du protocole de connexion d'un analyseur nécessite une vérification des interopérabilités.

La lecture du rapport d'intervention permet d'identifier les patients tests à réaliser (Cf. annexe 9) : tests de connexion, transmissions dématérialisées de comptes-rendus, ... Pour les analyseurs réalisant une expertise, comme par exemple les systèmes experts d'interprétation des antibiogrammes, le LBM teste quelques règles d'expertise par échantillonnage (saisie manuelle ou reprise de phénotypes caractérisés pour vérification des règles d'expertise par rapport aux référentiels choisis par le LBM).

Le LBM trace les changements de versions des différents systèmes informatiques utilisés (SIL, MW, Système expert, ...) (Cf. §8.7).

Exemple de non régression – Vérification de la Liaison LBM/prescripteur suite à l'ajout de la fonctionnalité LBM/correspondant :

- La nouvelle fonctionnalité LBM/correspondant est testée en intégration fonctionnelle ;
- Le LBM vérifie la non régression fonctionnelle concernant la connexion déjà existante LBM/prescripteur :
  - Vérification de la génération des fichiers sécurisés par le SIL ;
  - Vérification de l'envoi effectif du message sécurisé au(x) bon(s) destinataire(s).

(Cf. annexe 10)

##### Point de vigilance :



Après une analyse de risque en cas de régression le LBM peut envisager un retour à la version antérieure (à définir dans les pré-requis).

## 8.5 Vérification continue (dont signalement vigilance)

### 8.5.1 Vérification du paramétrage

Le LBM s'assure au cours du temps de la stabilité du paramétrage utile au transfert de données. Le LBM définit une périodicité de vérification continue. Le LBM met en place des patients tests connus dans une série afin de contrôler la cohérence des résultats d'examens. La vérification comprend l'ensemble du processus (vérification des connexions de prescription, des automates péri-analytiques (centrifugation, aliquotage et sérothéguage, ...). (Cf. annexe 11)

### 8.5.2 Vérification du paramétrage des règles

Le LBM s'assure au cours du temps de la stabilité des règles par des patients tests.

Point de vigilance :



Le LBM porte une attention particulière quant à la vérification des règles en cascade.

Exemple de règle en cascade :

Cas du taux de prothrombine inférieur à 10% :

- Si TP égal à 8%, *règle 1* : vérifier l'absence de caillot dans le tube ;
- Si absence de caillot : *règle 2* : relancer la demande d'examen à l'automate ;
- Si valeur confirmée : *règle 3* : rendre sur le compte rendu <10%, résultat vérifié ;
- Pour l'interprétation par rapport à l'hématocrite, *règle 4* : si numération dans le dossier, si hématocrite < 30% rendre un commentaire sous le résultat TP : « Compte tenu de la valeur de l'hématocrite < 30%, les résultats de l'INR et du TCA sont probablement sous-estimés ».

### 8.5.3 Vérification des sauvegardes et de l'archivage

*Archivage électronique : le LBM reproduit le rapport fidèlement durant toute la durée d'archivage définie.*

Le LBM s'assure de l'intégrité des données au cours du temps et vérifie à l'aide de dossiers patients la possibilité de consulter les archives.

Les sauvegardes sont vérifiées de manière régulières par le LBM et des exercices de restauration de données sont réalisés a minima une fois par an. Ces exercices de restauration peuvent se faire sous la forme :

- De restauration des sauvegardes complètes sur un serveur de test ;
- De restauration des sauvegardes sur un serveur loué pour une courte durée chez un hébergeur (cryptage des données et sécurisation par mot de passe avant transfert – suppression des données après test).

Point de vigilance :



La restauration des sauvegardes directement sur l'environnement de production est déconseillée. Si la sauvegarde n'est pas intègre, le LBM aura perdu ses données.

### 8.5.4 Transmissions des résultats des examens spécialisés

Dans le cas d'intégration dans le SIL des résultats d'examens transmis par les LBM spécialisés, le LBM s'assure de la bonne communication des résultats aux prescripteurs et/ou patients.

### 8.5.5 Suivi des droits

Le LBM définit les droits de chaque opérateur et hiérarchise les droits selon les métiers, les habilitations et compétences des opérateurs. Le suivi périodique est à définir en fonction de l'évolution du parc informatique et mouvement du personnel. Une vérification périodique (au moins une fois par an) des droits sur les systèmes informatiques est recommandée.

Exemple de droits sur le SIL ou MW ou interfaces informatiques :

- Maître ou administrateur,
- Utilisateur en précisant les sous niveaux en fonction des responsabilités définies :
  - Secrétaire ;
  - Technicien ;
  - Biologiste ;
  - ...

### 8.5.6 Cas des logiciels de bureautique

Les logiciels de bureautique ne sont pas à valider, mais leurs applications particulières (par exemple les feuilles de calcul de tableur) demandent une vérification et une protection appropriée.

LA VERSION ELECTRONIQUE FAIT FOI

## 9 ANNEXES

### 9.1 Annexe 1 : exemple de convention de preuve



Mr Le Dr xxxxxx

#### TRANSMISSION ELECTRONIQUE DE RESULTATS D'EXAMEN CONVENTION DE PREUVE

La transmission dématérialisée de résultats est soumise à des exigences imposées par l'Etat aux laboratoires de biologie médicale (norme ISO 15189, décret n°2007-960 du 15.05.07).

Ces exigences peuvent se résumer ainsi :

- Authentifier l'émetteur des comptes rendus et le destinataire (notion de non-répudiation)
- Tester l'exactitude des identifiants qui permettent la transmission électronique ; par exemple : n° de fax, adresse de messagerie, code de cryptage s, ...)
- Vérifier l'intégrité des données figurant dans les comptes rendus télétransmis
- Préserver la confidentialité de ces informations sur le lieu de réception

Nous sommes ainsi tenus de mettre en place un contrat encore appelé «convention de preuve» avec les destinataires de nos comptes rendus.

***Dans ce but, nous vous demandons de bien vouloir comparer le compte rendu test ci-joint au document qui vous a été transmis électroniquement et de nous retourner la présente convention à l'adresse ci-dessous:***

LBM xxx  
2, rue xxxx  
75 000 PARIS

Fax : 01 xx xx xx xx

Je soussigné, \_\_\_\_\_

- Atteste de la bonne réception du compte rendu test

Ceci en situation de confidentialité (matériel de réception à l'écart du public, droit d'accès réservé au personnel autorisé)

- Atteste de la totale similitude des informations entre la version papier et la version électronique

Protocole de transmission:  Messagerie sécurisée  Fax  Modem-Modem

Fait à \_\_\_\_\_ Le \_\_\_\_\_

Cachet et Signature

## 9.2 Annexe 2 : exemple de fiche de fonction de responsable informatique du LBM

### Fiche de fonction de responsable informatique

#### ▪ Mission principale :

Sous l'autorité des biologistes du LBM (et en lien avec l'équipe DSI de l'établissement de santé), le référent informatique est responsable du bon fonctionnement des SIL. Il assure, au sein de l'équipe et en relation avec les biologistes, une mission d'interface, d'assistance pédagogique et de maintenance. Il participe au choix et au développement d'outils informatiques.

#### ▪ Activités :

##### •Assistance et formation des utilisateurs des SIL :

- identifier et analyser les problèmes rencontrés dans l'utilisation des SIL,
- procéder à l'assistance des utilisateurs en lien avec la DSI,
- former, de manière individuelle ou collective, aux logiciels utilisés, aux nouvelles fonctionnalités et aux nouveaux logiciels et applications,
- évaluer les actions de formation,
- concevoir des supports pédagogiques.

##### •Assurer le paramétrage des SIL

- identifier et analyser les besoins des utilisateurs
- mettre à jour le paramétrage

##### •Gérer les demandes de requêtes et d'études ponctuelles

- cibler et reformuler les demandes de requêtes issues des services et directions ou des partenaires externes (établissements de santé, ...),
- traiter, mettre en forme et diffuser les résultats de la requête
- réaliser et mettre en forme les statistiques, les graphiques et les tableaux de bord à partir des données extraites des SIL,

##### •Assurer une maintenance de proximité des logiciels

- cibler et analyser les dysfonctionnements
- assurer la sauvegarde du serveur et le bon fonctionnement du matériel informatique en lien avec la DSI,
- assurer le suivi et la coordination de l'équipement des utilisateurs (planification et information)

##### •Participer au choix des nouveaux produits, au développement de projets et d'outils informatiques favorisant la modernisation du service rendu (système de contrôle d'effectivité, dématérialisation des données)

- recenser et analyser les nouveaux besoins des utilisateurs,
- identifier des axes d'amélioration des logiciels et du matériel informatique,
- participer à l'étude prospective relative au choix des nouveaux produits et au développement des outils informatiques du LBM,
- participer à des réunions et des groupes de travail,
- participer à l'élaboration de cahiers des charges,
- participer au choix et à la mise en place de nouveaux logiciels et du matériel informatique,
- accompagner la mise en place des nouveaux outils (procéder à des tests et réaliser des guides d'utilisation)

#### ▪Compétences requises :

##### •Connaissances :

- connaissance du domaine LBM,
- connaissance des activités des utilisateurs,
- bonne connaissance de l'outil et de l'environnement informatique (logiciels)

• **Aptitudes professionnelles :**

- aptitude au suivi et au contrôle
- capacité d'anticipation et de prévision
- aptitude au travail par projet
- force de proposition
- aptitude à la pédagogie
- aptitude à l'apprentissage

• **Comportements professionnels – motivations :**

- excellent relationnel
- disponibilité
- écoute
- rigueur et méthode
- sens du travail en équipe
- réactivité
- autonomie
- motivation pour la nouveauté technologique

### 9.3 Annexe 3 : Exemple de charte informatique

Charte produite dans le cadre des travaux de la SFIL

#### Maquette de charte d'utilisation du système d'information dans un LBM

*Pour la rédaction du présent document, nous nous sommes basés sur les objectifs de sécurité permettant le bon fonctionnement d'un système d'information ainsi que sur les règles de sécurité des données :*

- *intégrité ;*
- *confidentialité ;*
- *disponibilité ;*
- *non répudiation ;*
- *authentification ;*
- *continuité du service*

*et sur les textes légaux en vigueur.*

*Dans cette maquette, nous présentons les recommandations destinées aux utilisateurs dans deux chapitres « sécurité des accès au système » et « utilisation du système ».*

*Chaque entité juridique et/ou biologiste responsable pourra s'inspirer des items décrits dans ces chapitres, les compléter ou les modifier en fonction de son organisation et des outils informatiques mis à disposition du personnel afin d'élaborer sa propre charte d'utilisation intégrée à son système qualité.*

*Ces recommandations peuvent être intégrées au contrat établi entre biologiste responsable et le service informatique des établissements de santé.*

#### INTRODUCTION

***Nous conseillons de faire un rappel des textes légaux auxquels sont soumis les personnels des laboratoires de biologie médicale, parmi lesquels :***

- La loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 (plus connue sous le nom de loi informatique et libertés de 1978) ;

- L'article 1383 du Code Civil ;
- La loi 2004-801 du 6 août 2004 du Code Pénal.

**Rappel : Ces textes doivent être déjà référencés dans le règlement intérieur du laboratoire ainsi que dans les contrats de travail.**

### **Droit et devoir de l'administrateur système**

**Il peut être utile également de rappeler que l'administrateur du système d'information a une obligation de confidentialité vis-à-vis des données personnelles des utilisateurs et qu'il ne peut y accéder que si elles menacent l'intégrité du système.**

#### **1) Sécurité des accès au système**

Utilisation de login et mots de passe personnels et confidentiels ;

Respect des recommandations de la CNIL (mots de passe et login de 6 caractères minimum, mots de passe différents du nom, du prénom, de la date de naissance et de certains termes (« motdepasse », « sésame », ...), mots de passe comprenant au moins une lettre, un chiffre et un caractère spécial, modification tous les 90 jours, non réutilisation des 3 derniers mots de passe, ...)

Droits d'accès limités aux besoins des différents types d'utilisateurs (profils utilisateurs liés au mot de passe) ;

Authentification forte (utilisation de la CPS, autres systèmes, ...)

Lien avec l'annuaire du personnel ;

Mise en place de déconnexion automatique sur les postes clients ;

Obligation de se déconnecter du système en quittant son poste. En cas d'omission l'utilisateur suivant est déconnecté de la session précédente.

#### **2) Utilisation du système**

##### **a) Utilisation courante des ressources informatiques**

- Interdiction d'utiliser les ressources informatiques en dehors du cadre professionnel ;
- Utilisation exceptionnelle à des fins personnelles régie par le règlement intérieur, de même que les utilisations abusives.

##### **b) Usurpation d'identité**

- Interdiction de masquer son identité ou d'usurper l'identité de toute autre personne ;
- Obligation de signaler les tentatives d'accès anormales ou les anomalies constatées.

##### **c) Données d'autrui et confidentialité**

- Interdiction de lire, copier, modifier ou détruire des données de tiers, sauf autorisation du ou des détenteurs ;
- Interdiction d'intercepter des communications.

##### **d) Respect du droit des personnes et de l'ordre public**

- Interdiction de porter atteinte à la vie privée d'autrui par tout procédé ;
- Utilisation ou diffusion de l'image (photos, enregistrement vidéo ou audio) uniquement avec le consentement écrit de la personne ou du responsable légal pour un mineur ;
- Les données personnelles, quand elles existent, doivent être clairement identifiées comme telles.

##### **e) Droits de reproduction et respect du droit de la propriété intellectuelle**

- Respect des termes et conditions de la licence d'utilisations des logiciels ;
- Interdiction de reproduire des logiciels commerciaux sauf pour copie de sauvegarde ;
- Respect des droits de propriété intellectuelle sur les œuvres protégées.

f) Utilisation d'équipements étrangers au laboratoire

- Interdiction d'utiliser du matériel étranger au laboratoire (ordinateur personnel, ...) sans l'autorisation du responsable informatique ;
- Interdiction d'utiliser des supports externes de données (disquettes, disques durs externes, cd, dvd, clés USB, baladeurs mp3, téléphones portables, ...) sans l'autorisation du responsable informatique.

g) Utilisation de la messagerie

- Interdiction d'ouvrir la pièce jointe d'un e-mail de provenance incertaine ;
- Interdiction de cliquer sur un lien reçu par messagerie provenant de personnes ou de sites inconnus ;
- Obligation de suivre les recommandations de la CNIL (fiche pratique "données de santé, email et fax", ...) en particulier l'utilisation de la messagerie sécurisée ;
- Les e-mails personnels doivent être clairement identifiés comme tels.

h) Téléchargement et installation de logiciels

Le laboratoire est équipé d'antivirus, de pare-feu et de filtres bloquant certains sites et mots clés.

Toutefois, le système de protection n'est pas invincible et la sécurité la plus sûre est l'évitement :

- Interdiction de télécharger des logiciels ou des fichiers sans l'autorisation du responsable informatique ;
- Interdiction d'utiliser des forums ou mailing-list sortant du cadre professionnel ;
- Interdiction de se connecter sur des sites abordant des sujets sensibles, par exemple :
  - duplication illégale de musique ou vidéo (ex. mp3, divx) ;
  - rencontres en ligne ;
  - pornographie, pédophilie ;
  - extrémismes politiques et religieux ;
  - terrorisme, racisme ;
  - drogues, substances illicites ;
  - piratage informatique, jeux en ligne ;
  - ...

i) Antivirus

- Interdiction de désactiver et/ou de désinstaller les logiciels antivirus ;
- Interdiction de modifier le paramétrage du logiciel antivirus.

j) Sauvegardes

- La sauvegarde des fichiers personnels (lorsqu'ils sont autorisés) est sous la responsabilité de l'utilisateur ;
- La sauvegarde des données situées sur le serveur est sous la responsabilité du responsable informatique ;
- Les autres sauvegardes (automates, poste de travail, ...) doivent être exécutées par des utilisateurs désignés. Ces utilisateurs devront s'assurer de l'intégrité des données sauvegardées et de leur conservation.

**Engagement de l'utilisateur**

Je soussigné(e) :

.....

Demeurant à :

.....

Exerçant la fonction de :

.....

Déclare avoir pris connaissance et approuver les dispositions de la présente charte énoncées sur les pages précédentes et m'engage à les respecter. Dans le cas contraire, je ne pourrais pas m'opposer à l'application des sanctions prévues au règlement intérieur du laboratoire.

Fait à : .....

En deux exemplaires dont un est remis à l'utilisateur et l'autre conservé par le laboratoire.

Signature de l'utilisateur :

Signature du responsable du laboratoire :

**9.4 Annexe 4 : exemples de formulaires de paramétrage**

**Exemple n°1 : Expression du besoin**

Partie réservée au demandeur	
Expression du besoin :	Date :
Biologiste demandeur ou autre avec fonction :	
Nom de l'examen ou du bilan :	
Sous-Domaine (ex Hématocytologie) / Famille (ex : Hémostase / COAGBM) :	
Code(s) nomenclature(s) :	
Commentaire(s) sur l'examen ou bilan :	

**Exemple n°2 : Liste de contrôle de paramétrage de la fiche examen**

Liste de contrôle : modification d'examen ► . . . . .	Traces	
	Visa	Date
<b>1 / Logiciel SIL</b>		
Fiche(s) du dictionnaire N° _____		
Tarifcation nombre de B + code de nomenclature		
Non cumuls, plafonds, profils, 100%		
Code de prélèvement et tarifs		
Format d'expression du résultat (nombre de décimales)		
Unités principale et secondaire		
Conversion unité SI / unités conventionnelles		
Valeurs de références + Bornes de contrôle biologiste		
Fiche de calcul N° _____		
Code analyse reflexe : _____		
Fichier des réponses N° _____		
Règle(s) d'expertise N° _____		
Mention de la technique employée		
Inscription dans le cahier de paillasse N° _____		
Documents secondaires (feuille de travail, liste de transmission, bordereau de transmission) _____		
Inscription sur une étiquette de prélèvement PRIMAIRE N° _____		
Inscription sur une étiquette de prélèvement SECONDAIRE N° _____		
Inscription dans une connexion automate ou liaison extérieure		
Impact sur le paramétrage d'un graphique		
Impact sur un code d'appel (profil et bilan) N° _____		
Impact sur les états statistiques N° _____		
Mention d'alerte ou « flag » : _____		
<b>2 / Logiciel expert d'aide à la validation : Vérification d'impact</b>		
<b>3 / Logiciel Manuel de prélèvement : Vérification d'impact</b>		
<b>4 / Logiciel(s) de diffusion de résultats : Vérification d'impact</b>		
<b>5 / Logiciel MW : Vérification d'impact</b>		
<b>6 / Logiciel(s) SIH : Vérification d'impact</b>		
<b>7 / Dossier(s) test (un ou plusieurs selon analyse de risque)</b>		
Vérification rapport d'analyse, Feuille de soins,		
Vérification étiquette de prélèvement primaire / secondaire		
Vérification feuille de travail et autres documents secondaires		
Vérification connexion(s)		
<b>8 / VALIDATION DU PARAMETRAGE</b>		
<b>J'atteste avoir réalisé une analyse de risque, une revue du paramétrage et une vérification du dossier(s) test. Bon pour mise en exploitation.</b>	Date	
Nom et signature du Biologiste Responsable		

**Exemple n° 3 : Liste de contrôle pour la création d'un examen ou d'un texte ou commentaire codé**

Question	Qui	Réponse	Validation / traçabilité
Demande	BIO	<input type="checkbox"/> Création <input type="checkbox"/> Modification	
Conservation de l'antériorité des résultats	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	si OUI Création d'un dictionnaire
Modification majeure des matrices des comptes rendus (CR) (traçabilité d'évolution)	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	Si OUI Création d'un dictionnaire
Besoin de transmission	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Evolution d'un Examen/ Élément/ CR simple	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	Duplication / Attention aux bilans qui devront être modifiés
Création d'un dictionnaire	SI		Attention : la tarification n'est pas historisée
<b>Demande</b>			
Site demandeur	BIO		
Biologiste demandeur	BIO		
Analyse transmise à un labo extérieur	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Cette analyse est effectuée sur quel site	SI BIO	Site : <input type="checkbox"/> Oui <input type="checkbox"/> Non Site 2 : <input type="checkbox"/> Oui <input type="checkbox"/> Non Site N : <input type="checkbox"/> Oui <input type="checkbox"/> Non	Avertir les responsables des sites concernés
Chapitre / Sous Chapitre concerné dans le SIL	BIO	Chapitre : Sous chapitre :	
<b>Identification</b>			
Code d'appel de l'examen	SI		
Code interne de l'examen	SI		
Nom de l'analyse pour libellé long dans le SIL	BIO		
Vérification si distinction de technique par site : « Code d'appel de production »	SI		
Code communication par défaut	SI		Ce code est communiqué au client + SUPPRESSION de l'ancien code

« Rangement »																							
Ranger l'analyse dans le chapitre (ordre d'impression des examens sur le CR)	SI/ BIO																						
Contrôle d'accueil																							
Geste de prélèvement particulier	BIO	<input type="checkbox"/> Sang <input type="checkbox"/> Bactério <input type="checkbox"/> Autre : .....																					
Nombre de séances	BIO		(par défaut : 1)																				
Exécution																							
Labo exécutant (si transmis)	BIO																						
Contexte de réalisation	BIO	<input type="checkbox"/> Local <input type="checkbox"/> Autre : .....																					
Délai de réalisation	BIO	..... jours																					
Jours de réalisation	BIO	<input type="checkbox"/> Lu <input type="checkbox"/> Ma <input type="checkbox"/> Me <input type="checkbox"/> Je <input type="checkbox"/> Ve <input type="checkbox"/> Sa <input type="checkbox"/> Di																					
Facturation																							
Facturation immédiate	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non																					
Cotation extérieure (si transmis)	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non																					
Code nomenclature / nbre B	BIO	Acte : réf ..... Nombre de B .....																					
Détermination des différents éléments composants l'analyse	BIO	<table border="1"> <thead> <tr> <th>Nombre éléments : .....</th> <th>NOM élément</th> <th>CODE élément</th> <th>Numérique / Texte codé</th> </tr> </thead> <tbody> <tr> <td>1-</td> <td></td> <td></td> <td></td> </tr> <tr> <td>2-</td> <td></td> <td></td> <td></td> </tr> <tr> <td>3-</td> <td></td> <td></td> <td></td> </tr> <tr> <td>.....</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Nombre éléments : .....	NOM élément	CODE élément	Numérique / Texte codé	1-				2-				3-				.....				
Nombre éléments : .....	NOM élément	CODE élément	Numérique / Texte codé																				
1-																							
2-																							
3-																							
.....																							
Définition de l'ELEMENT n° : ..... (imprimer le s pages de 3 à 5)																							
Saisissable à l'accueil	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non																					
Recherche antériorité	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	Attention à la rupture liée au changement de technique																				
Code nature échantillon	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non N° ou libellé : .....																					

Type de résultat	BIO	Numérique texte codé calcul (Formule) : ..... autres : .....	
<b>Si élément de type « résultat numérique »</b>			
Bornes pathologiques extrêmes	BIO	Mini : Maxi :	Police 10 gras
Delta check : comparaison résultat du jour et résultat antérieur (si > à X%)	BIO	Relative : ..... % Absolue : ..... %	Police 10 gras
<b>Validation Biologique</b> (bornes propres au labo au delà desquelles <i>il y a demande</i> de validation biologique	BIO	Enfant : Min                      Max Femme : Min                    Max Homme : Min                    Max	
<b>Normes</b> Références (normales/ par sexe ou tranche d'âge ...)  Préciser les tranches d'âge si besoin pour chaque sexe	BIO	Normales ENFANT :  Normales FEMME :  Normales HOMME :	Il est obligatoire de mettre une ligne au moins pour gestion des attributs gras sur le CR médecin
Référence convertie si deuxième unité	BIO	Normales ENFANT :  Normales FEMME :  Normales HOMME :	
Technique <b>NON CONNECTEE</b>	BIO	Noter le libellé exact de la technique (avec nom de l'automate) : ..... .....	Recopier exactement le même libellé que celui mis au niveau de l'automate (obligatoire pour la saisie manuelle)
Nom du ou des automates	BIO	Nom de l'automate : ..... Transit via le MW : <input type="checkbox"/> Oui <input type="checkbox"/> Non <i>Si OUI :</i>  TRI MW : <input type="checkbox"/> Oui <input type="checkbox"/> Non – Code : .....	
Connexion concernée	BIO	Si transit MW : code ..... Si pas MW nom du driver : .....	Nom du driver à prendre dans l'interface « Connexion » du SIL
Code du test	BIO	Si transit par MW Code test : .....  Si (« nom automate » ...) : Code : ..... N° de la méthode dans le canal : .....	A décider avec le resp du MW (code identique dans le MW et dans ce champ) :  à demander au fournisseur de l'automate)

Technique	BIO	Noter le libellé exact de la technique (avec nom de l'automate) : ..... .....	Recopier exactement ce libellé au niveau de technique Technique <b>NON</b> <b>CONNECTEE</b>
Déclenchement de Texte codé	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non Si OUI : préciser les tranches numérique et le texte codé correspondant	
<b>Si élément de type « texte codé »</b>			
Description des libellés et textes codés voulus	BIO		
Orientation des maquettes (si bact) (référence interne)	SI		
examen à inclure sur une paillasse	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Feuille de bactério	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Avertir Référent automate si code connecté	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
<b>Si élément de type « Si élément de type « texte codé « Formule de calcul »</b>			
	BIO SI	Formule :	Faire contrôler la formule par excel ou calculette et garder la preuve de l'exactitude du calcul dans le SIL
<b>Exécution</b>			
Saisie obligatoire	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Double saisie	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Première unité	BIO		
Deuxième unité	BIO		
Facteur de conversion (si deuxième unité)	BIO		
<b>Compte-rendu</b>			
Résultats éditables au patient	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	reporter sur références éditables au patient
Résultats éditables au prescripteur	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	reporter sur références éditables au prescripteur
Nombre de décimales pour la première unité	BIO	.....	
Nombre de décimales pour la deuxième unité si besoin	BIO	.....	

Conservation			
Conservation de l'examen en échantillothèque	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non Si Oui : contexte de conservation Nom de l'échantillothèque :	
Matrice d'édition			
Matrice imprimable	SI BIO		Décrire ce qu'il faut écrire exactement sur le CR (ou citer un modèle d'examen)
Matrice texte (modèle)	SI		<b>Recopier toujours la matrice imprimable (pour rapport de fax)</b>
Matrice tableau	SI		Mettre dans la matrice tableau
Bilans			
Cette analyse appartient elle à un bilan ?	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non Si oui rajouter la nouvelle analyse dans le bilan concerné	Attention, les bilans ne sont pas historisés
Transmissions des résultats			
FAX analyse à faxer pour tous	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
analyse à faxer uniquement		Spécialité : .....	
Liaison extérieure	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non si oui : mettre à jour les requêtes d'exclusion	
Codage des éléments dans la liaison (LOINC)	SI	Supprimer la ligne correspondant à l'ancien code	Supprimer la ligne correspondant à l'ancien code
Avertissement des correspondants en connexion	SI	Envoyer mail à ..... pour avertir les partenaires par mail des nouveaux examens ou modif :  Liste des correspondants concernés : <ul style="list-style-type: none"> <li>• Corres 1</li> <li>• Corres 2</li> <li>• Corres N</li> </ul>	Attention : le code de communication par défaut est communiqué aux clients  Enlever le code de communication de l'ancienne analyse  Enlever dans la table connexion la ligne de l'ancien code
Paramétrage MW			
Généralités	Resp MW	Opérateur :	Date
code SIL reçu par MW ou autre automate	Resp MW		
examen reçu par le MW	Resp MW	<input type="checkbox"/> Oui <input type="checkbox"/> Non	

Examen traité par automate	Resp MW	<input type="checkbox"/> Oui <input type="checkbox"/> Non	Garder trace papier si possible
Résultat reçu par SIL du MW ou autre automate	Resp MW	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
<b>Dossiers tests de validation</b>			
	SI	Opérateur saisie : n° du dossier : ...../...../.....- .....- .....	
impression étiquettes	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Vérif : CR Médecin	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Vérif : CR patient	BIO	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Impr Cotation dans demande SIL	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Vérif Résultats FAX	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Vérif connexion/liaison	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Vérif : fiche identification patient	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Vérif feuille de sécu	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Vérif : bon de transmission si besoin	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Feuille de secteur si PAILLASSE / LECTEUR Bactério	SI	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Accord et signature de mise en service	SI		
Accord et signature du responsable du service	BIO		
Transmettre les infos pour le bio responsable du site internet et du guide des examens	BIO		
Transmettre un message aux biologistes et pour avertir tous les biologistes	BIO		
Nom du biologiste et signature du biologiste responsable demandeur	BIO		Date de mise en production de l'examen :

## 9.5 Annexe 5 : exemple de vérification de connexions par visualisation des fichiers transmis par l'analyseur

### Données brutes transmises par l'analyseur (non formatées)

Traces de traitement

Fichier

Fichier brut : 1263012

```
H|^~\&||130953^NETIKA||ORU||MPL||P|A2.2|201205111550|
P|1|A20071023-077||ESSAI^Connexion|20000101|F|||||||20120511||DC|
OBR|1|010320511245^A20120511-245|DIGO-OSTEO|R|201205111526|201205111526-201205111526||N|||201205111526|Serum|DC||
OBX|1|SI|DIGO||<0.150|||F|20120511|8||MPLauto|
OBX|2|NM|OSTEO||25.83|||F|20120511|8||MPLauto|
L|||1|6||
```

### Données formatées (lisibilité accrue)

Traces de traitement

Fichier

Fichier de traces : 1263012

Fichier de traces / Réception de résultats / Demande : A20120511-245

```
[0.1ms] [ Traitement du fichier 1263012_MPL676.AST le 11-05-2012 à 15:50:17 ]
[0.1ms] RECEPTION RESULTAT (idFichier=1263012)
[0.2ms] Connexion : - instrumentId : Array(8) - Tube : 010320511245
[0.7ms] Demande trouvée directement : A20120511-245 (idDemandeOrigine=235267)
[0.7ms] Référence matériel recherchée (array) : 8
[0.9ms] Référence matériel recherchée (array sup) : 8
[1.1ms] Matériel trouvé (instrumentId du fichier) : CE (id=300)
[2ms] Tube trouvé : 864930 - Lien : 960127
[2.4ms] Tube trouvé avec l'instrument ID (010320511245) : 864930 - Lien : 960127
[2.8ms] [235267] Patient trouvé : Connexion ESSAI / A20071023-077
[2.8ms] [235267] Demande trouvée : A20120511-245
[6.2ms] [235267] Analyse trouvée (sans tube) : DIGO => DIGO_ [1]
[7.4ms] [235267] Traitement du résultat (nombre) DIGO_ [1] : <0.150
[9.4ms] [235267] Conséquence sur résultat 1005 DIGO_ [1] : Remplacement par <0.15
[9.5ms] [235267] Après conséquence (1) : <0.150 => <0.15
[15.3ms] [235267] Résultat pour borne : 0.15
[16ms] [235267] Alarme trouvée : E => Dépassement limites alertes inf.
[17.5ms] [235267] Blocage de la validation technique détectée sur alarme S
[17.5ms] [235267] Validation technique bloquée par alarme
[26.6ms] [235267] Aucun lot trouvé pour cette demande
[29.3ms] [235267] Analyse trouvée (sans tube) : OSTEO => OSTEO[1]
[30.6ms] [235267] Traitement du résultat (nombre) OSTEO[1] : 25.83
[36.3ms] [235267] Résultat pour borne : 25.8
[41.5ms] [235267] Aucun lot trouvé pour cette demande
[42.7ms] [235267] Fichier au status : traite
[51.3ms] [ Fichier traité en 51.3 ms ]
[51.3ms]
```

### Copie d'écran SIL : vérification concordance données brutes analyseur – données transmises par SIL

ESSAI Connexion A20120518-218 (Validée) | 10 / 99 | A20120511-245 | ESSAI Calcul Sil A20120510-195 (Validée)

Impressions | Impr. masse | Modification Demande | Visualisation Résultats (F7)

Val bio & technique & FQ & Scans / / Visu CR / / Infos demande / / Sérothèque & Traçabilité & Historique / / Trans. CR& Conseils & Impressions & Connexions

**M. ESSAI Connexion 25 ans** Né(e) le 17-12-1986 Prélèvement: reçu  
Adresse: Factorisation cabinet en référence 2  
 Dr DC Dossier du site LABORATOIRE

Analyses ▾

✓ Demande validée biologiquement par le 11-05-2012 à 18:00:15

Analyses	Résultats	T	B	Antériorités	Etat
HORMONOLOGIE					
OSTEO[1] : OSTEOCALCINE N-MID (C)	25.8 µg/l	KA	YY	-	
SEROLOGIE					
TPLA[2] : Sérologie TPLA	0.4 T.U.	KA	YY	-	
DOSAGES DE MEDICAMENTS					
DIGO_Cobas[1] : DIGOXINEMIE (C)	<math>< 0.15 \text{ ng/ml}</math> (0.90-2.00) ↓	IC	YY	67.00	
DIGO_Cobas[2] : Heure du prélèvement.	08:00	IC	YY	08	
DIGO_Cobas[3] : Posologie.	1 CP	IC	YY	1CP	

Scan

M. ESSAI Connexion 25 ans Né(e) le 17-12-1986

### Traçabilité de la vérification de la connexion

Date	Heure	Action	Statut	Code	Détails
11-05-2012	15:50:17	Saisie des résultats	SIL	OSTEO[1]	Résultat : - ► 25.8 Saisie par : - ► SIL Résultat identique à celui transmis par l'automate : connexion validée pour ce dossier test
11-05-2012	15:50:17	Saisie des résultats	SIL	DIGO_Cobas[1]	Résultat : - ► <math>< 0.15</math> Borne technique dépassée : Non ► Oui (inf) Borne biologique dépassée : Non ► Oui (inf) Saisie par : - ► SIL
11-05-2012	15:40:01	Infos carte vitale	SIL	010320511245	Intégration
11-05-2012	15:40:01	Saisie des résultats	SIL	TPLA[2]	Résultat : - ► 0.4 Saisie par : - ► SIL

## 9.6 Annexe 6 : exemple d'un test des règles d'un MW

Code	Texte abrégé	Nom /
CARBO2	CARBO	.B^High Turbidity Detected
O2SAT2	O2SAT	.B^High Turbidity Detected
THBGE2	THBGE	.B^High Turbidity Detected
METHB2	METHB	.B^High Turbidity Detected
CARBO	CARBO	.CARBO A^Absorbance Error
PCO37 I	PCO37 Interf	.interférence caillot
PCO2 I	PCO2 Interf	.interférence caillot
PH I	PH Interf	.interférence caillot
PH37 I	PH37 Interf	.interférence caillot
PO2 I	PO2 Interf	.interférence caillot
PO37 I	PO2 37 Interf	.interférence caillot
METHB	METHB	.METHB A^Absorbance Error
O2SAT	O2SAT	.O2SAT A^Absorbance Error
THBGE	THBGE	.THBGE A^Absorbance Error
BILGE < 5	BILGE < 5	:BILGE < 5
CAIGE < 0.1	CAIGE < 0.1	:CAIGE < 0.1
CAIGE > 5	CAIGE > 5	:CAIGE > 5
CARBO < 10	CARBO < 10	:CARBO < 10
CARBO > 110	CARBO > 110	:CARBO > 110
GLU < 0.2	GLU < 0.2	:GLU < 0.2
GLUGE > 41,6	GLUGE > 41,6	:GLUGE > 41,6
HTGE < 15	HTGE < 15	:HTGE < 15
HTGE > 75	HTGE > 75	:HTGE > 75
LACTGE < 0.3	LACTGE < 0.3	:LACTGE < 0.3
LACTGE > 20	LACTGE > 20	:LACTGE > 20
METHB < 10	METHB < 10	:METHB < 10
METHB > 110	METHB > 110	:METHB > 110
PCO37 < 6	PCO37 < 6	:PCO37 < 6
PCO37 > 150	PCO37 > 150	:PCO37 > 150
PH37 < 6,8	PH37 < 6,8	:PH37 < 6,8
PH37 > 8	PH37 > 8	:PH37 > 8
PO37 < 5	PO37 < 5	:PO37 < 5
PO37 > 800	PO37 > 800	:PO37 > 800
POTGE < 0.1	POTGE < 0.1	:POTGE < 0.1
POTGE > 0.2	POTGE > 0.2	:POTGE > 0.2
POTGE > 20	POTGE > 20	:POTGE > 20
SODGE < 100	SODGE < 100	:SODGE < 100
SODGE > 200	SODGE > 200	:SODGE > 200
THBGE < 3	THBGE < 3	:THBGE < 3
THBGE > 23	THBGE > 23	:THBGE > 23
CA	CA	:CA
COHB	COHB	:COHB
GLU	GLU	:GLU
HCT	HCT	:HCT
HTGE	HTGE	:HTGE
K	K	:K
LAC	LAC	:LAC
MCTH	MCTH	:MCTH
NA	NA	:NA
O2	O2	:O2
PCO37	PCO37	:PCO37
PH	PH	:PH
PO2	PO2	:PO2
TBIL	TBIL	:TBIL
THB	THB	:THB
THBGE	THBGE	:THBGE

Exemple de règles d'expertise

Comparaison d'écrans permettant la confirmation du transfert de données impliquant une ou plusieurs règles d'expertise

## 9.7 Annexe 7 : exemple de vérification de transmission des codes alarmes des analyseurs

### Paramétrage de la connexion dans le SIL

Correspondance des codes alarmes : XN 2000 L RET

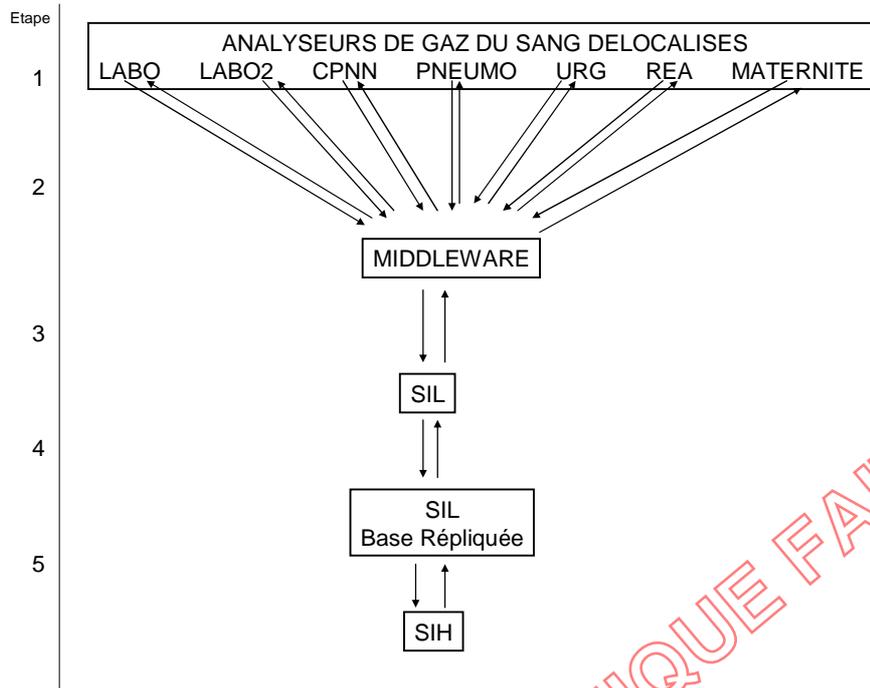
Code alarme automate	Texte de remplacement	Imp.	Alarme Tech	Bloquer Val T		Repasse	Impression CR			
				S-Analyse	Tube		P	M	C	
PLT_Clumps?	PLT_Clumps?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Non	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
@	linéarité dépassée	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Analyse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Abn_Lympho?	Abn_Lympho?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Non	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Anemia	Anemie	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Non	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Atypical_Lympho?	Atypical_Lympho?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Non	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Basophilia	Basophilia	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Non	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Blasts	Blasts	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Non	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

### Fichier de traces de la connexion

[196.1ms] [349885] Traitement du résultat (nombre) NF17 : 34.0  
 [204.6ms] [349885] Alarme trouvée : Positive\_Morph => Positive\_Morph  
 [205.4ms] [349885] Blocage de la validation technique de la sous-analyse détectée sur alarme Positive\_Morph  
 [205.6ms] [349885] Alerte sur demande déjà présente pour cette alarme  
 [205.7ms] [349885] Alarme trouvée : Atypical\_Lympho? => Atypical\_Lympho?  
 [206.1ms] [349885] Blocage de la validation technique de la sous-analyse détectée sur alarme Atypical\_Lympho?

⇔ Importance de la vérification de l'orthographe dans le paramétrage du SIL/MW : dans l'exemple, une saisie *Atypical\_Lympho* (sans ?) n'entraînerait pas un blocage de la validation

## 9.8 Annexe 8 : exemple de test de cohérence des données transmises



Cartographie du système (Étapes et connexions informatiques des gaz du sang)

Le bloc présente une comparaison de plusieurs interfaces utilisateur :

- Écran 'Rapport échantillon patient DUPLICATA' :** Affiche des informations de base du patient (Nom, Prénom, Sexe, Âge, Date de naissance) et des résultats de mesure (pH, pCO<sub>2</sub>, pO<sub>2</sub>, Hct).
- Écran 'Patient test 1' (Analyseur) :** Affiche des résultats de mesure à 37,0°C (pH, pCO<sub>2</sub>, pO<sub>2</sub>, Hct) et des calculs (TCO<sub>2</sub>, BE(B), sO<sub>2</sub>(c), HCO<sub>3</sub>(c)).
- Écran 'Saisie des résultats' :** Permet de saisir et valider les résultats des analyses.
- Écran 'Patient test 1' (Tableau) :** Affiche un tableau de résultats détaillés pour différents paramètres (pH, pCO<sub>2</sub>, pO<sub>2</sub>, Hct, TCO<sub>2</sub>, BE(B), sO<sub>2</sub>(c), HCO<sub>3</sub>(c), etc.) avec des valeurs de référence et des unités.
- Écran 'Patient test 1' (Tableau de résultats) :** Affiche un tableau de résultats pour différents tests (PH37, PCO37, PO37, HCO3, BE, O2SAT, TCO2, THGE, HTGE, TEMPS, PHG, PCO2, PO2, Hb, THGE) avec des valeurs de référence et des unités.

Comparaison des différents écrans des systèmes impliqués

## 9.9 Annexe 9 : exemple de vérification de non régression fonctionnelle

Les tests de non régression sont regroupés en scénario de non régression avec des scripts de test organisés par grandes étapes d'action utilisateurs. Pour chaque étape, il est précisé un résultat attendu et l'opérateur vérifie que le résultat attendu s'est bien reproduit preuve qu'il n'y a pas eu de régression.

Scénarii de test de non régression			
N° scénario	Description		
1	Saisie d'un dossier patient avec une numération et rendu de résultat au laboratoire		
2	Saisie d'un dossier patient avec une numération et rendu de résultat dans son DMP		
...			
Script de test du scénario 1		Date d'exécution : 01/03/2013	
Opérateur	John Doe		
N° étape	Description	Résultat attendu	Résultat réel
1	Saisie du dossier patient avec analyse de numération	Le dossier est enregistré et en attente de résultat	OK
2	Saisie manuelle du résultat de la numération	Le dossier passe en validation biologique	OK
3	Consultation du résultat en prévisualisation	Le dossier est prévisualisé dans un format CDA avec les résultats saisis	OK
4	Validation biologique du résultat	Le statut du dossier passe à validé	OK
5	Visualisation du fichier CDA généré sur le serveur	Après clic, il s'ouvre ddans un navigateur et et parfaitement lisible avec les résultats saisis	OK
6	Visualisation du message envoyé dans la boîte d'envoi de la messagerie	Un mail est envoyé et contient un fichier crypté	OK

A noter que contrairement aux tests d'intégration, les tests de non régression peuvent être automatisés avec des logiciels « robots » qui reproduisent toujours les mêmes séquences utilisateur.



## 9.12 Annexe 12 : Analyse de risques appliquée aux systèmes informatiques des LBM

L'analyse de risques tel que décrite ci-après est un processus que l'on met en œuvre lors de l'organisation ou la réorganisation d'un service informatique. Dans la pratique courante, la conduite du changement ne fait intervenir que certains des outils proposés, de façon plus ou moins allégés en fonction des situations (les interventions sur le SI n'ont pas les mêmes impacts lors d'une maintenance régulière ou lors d'une mise à jour « importante » du système).

La gestion des risques est définie par le guide 73 de l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La finalité de la gestion de risque peut se décomposer en trois étapes :

- Améliorer la sécurisation des systèmes d'information ;
- Justifier le budget alloué à la sécurisation du système d'information ;
- Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Le guide 73 de l'ISO évalue un risque par la combinaison de la probabilité d'un événement et de ses conséquences. Une équation « **RISQUE = MENACE \* VULNÉRABILITÉ \* IMPACT** » est couramment reconnue dans ce domaine, les termes de cette équation étant définis ainsi :

- **La menace** est la source du risque (par exemple l'attaque possible d'un élément sensible du système) ;
- **La vulnérabilité** est la caractéristique d'une partie du système constituant une faiblesse ou une faille au regard de la sécurité ;
- **L'impact** représente la conséquence du risque sur l'organisme et ses objectifs.

Il existe de nombreuses méthodes utilisées pour estimer et maîtriser les risques lié aux systèmes d'information.

Exemples :

- **AMDEC = Analyse des Modes de Défaillance et de leurs Effets Critiques**
- **EBIOS = Expression des Besoins et Identification des Objectifs de Sécurité (ANSSI)**
- **OCTAVE = Operationally Critical Threat, Asset, and Vulnerability Evaluation**
- **MARION = Méthode d'Analyse de Risques Informatiques Orientée par Niveau**
- **MEHARI = Méthode Harmonisée d'Analyse des Risques**

Globalement, elles proposent de :

### 1) Définir le périmètre de l'analyse de risques

Il s'agit d'identifier les activités métier, les intervenants, les éléments technologiques et d'infrastructure du LBM et éventuellement les patients, qui doivent être prises en compte. Cette étape initiale définit aussi les biens essentiels à protéger, par exemple les données patients, les traitements ayant une influence directe sur la qualité du service rendu par le LBM à ses patients et à ses prescripteurs, les données de production, de paramétrage, ...

La cartographie est un point de départ essentiel à l'identification de « failles potentielles » du système :

- matérielles (locaux, serveurs ou terminaux critiques, réseau, ...) ;
- logicielles (BDD, hébergement, protections, redondances, interfaces, réseau, sécurité, ...) ;
- humaines (opérateurs, utilisateurs, gestionnaires, protection, hiérarchisation accès, ...) ;
- organisationnelles.

## **2) Identifier les risques**

Les données de l'étape précédente sont analysées et associées à des écueils : pannes, mésusages, ou toute autre « menace possible ».

La décomposition en processus/sous-processus et la méthode des 5M (matières, matériel, milieu, main d'œuvre, méthodes) sont des moyens efficaces.

Le niveau de détail des sous-processus détermine le temps consacré à cette analyse et doit donc être dimensionné en fonction de la criticité du processus que l'on souhaite étudier.

### **Exemple 1 :**

L'analyse de la gestion du réseau peut nécessiter une cartographie minutieuse du matériel, des accès VPN, des fournisseurs, des utilisateurs et de l'ensemble des points d'entrée du VPN.

Une telle analyse approfondie se fait au démarrage ou lors d'une modification profonde du réseau pour ne revêtir qu'une forme simplifiée ou une revue sommaire lors d'évolution mineure.

### **Exemple 2 :**

Lors d'un changement de logiciel sur un automate connecté à la chaîne d'information SIL <=> MW <=> AUTOMATE les investigations se focaliseront sur les modifications nécessairement annoncées par le fournisseur. Si le LBM délègue cette tâche à un prestataire, une traçabilité des actions réalisées est à assurer.

## **3) Estimer la probabilité de la réalisation d'un risque et son niveau d'impact**

Il est d'usage d'affecter une cotation à chacun des critères identifiés précédemment afin de les combiner avec un indicateur facilitant la prise de décision. Même s'il existe dans la littérature des seuils décisionnels pour ce type d'indicateur, ils sont spécifiques à la méthode employée. En pratique ils sont le plus souvent fixés empiriquement par le LBM.

## **4) Consolider les éléments de l'analyse et élaborer le plan d'actions**

Une vue synoptique des éléments collectés lors des phases 1, 2 et 3 ci-dessus est obtenue en construisant un tableau du type « matrice risque/criticité » (Cf. tableaux ci-dessous).

Le plan d'action résulte finalement d'un arbitrage entre les coûts potentiels et le bénéfice attendu en matière de maîtrise des risques. Cet arbitrage est du ressort de la direction qui en garde la trace.

Le plan de continuité d'activité résulte de l'analyse de risques ou intègre celle-ci.

**Proposition des tableaux permettant de formaliser l'analyse par sous-processus, l'évaluation et la cotation du risque et de la criticité, ainsi que les éventuels moyens de maîtrise envisagés dans le cadre de la structuration des moyens de maîtrise (cellule informatique, politique de gestion, ...) :**

🌀 Guide Technique d'Accréditation – Evaluation systèmes informatiques Biologie Médicale

Processus concerné	Cause potentielle de défaillance	Effet indésirable de la défaillance	Mode de défaillance - M -	Fréquence d'occurrence - F -	DéTECTABILITÉ - D -	Gravité / Criticité de l'impact - C -	Criticité globale de la défaillance - R -	Moyen de maîtrise envisagé	Efficacité / commentaires
Chaque ligne du tableau reprend un sous processus issu de la cartographie	Description des éventuelles causes pouvant entraîner une défaillance	Description du type d'impact attendu concernant le sous processus envisagé	Défaillance permettant de fonctionner en mode dégradé => cotation 2  Défaillance Bloquante => cotation 4	Inexistant = 1  Rare = 2  Fréquent = 3  Systématique = 4	Toujours = 1  Facilement = 2  Difficile = 3  IndéTECTABLE = 4	Absence = 1  Faible = 2  Moyenne = 3  Elevée = 4	Combinaison des colonnes précédentes  $R=M \cdot F \cdot D \cdot C$  donc compris entre 2 et 256	Permet de n'avoir qu'un seul document	Idem
<p><i>Exemples de processus concerné par la <b>méthode MARION</b></i>                      la sécurité organisationnelle                      la sécurité physique                      la continuité de service                      l'organisation informatique                      la sécurité logique et l'exploitation                      la sécurité des applications</p>					<p><i>Exemples de processus concerné par la <b>méthode MEHARI</b></i>                      l'entité                      le site                      les locaux                      les applicatifs                      les services offerts par les systèmes et l'infrastructure                      le développement                      la production informatique                      les réseaux et les télécoms</p>				
<p><i>Exemples de cause de défaillance par la <b>méthode MARION</b></i>                      Accidents physiques / Malveillance physique                      Panne du SI                      Carence de personnel / Carence de prestataire                      Interruption de fonctionnement du réseau                      Erreur de saisie / Erreur de transmission                      Erreur d'exploitation                      Erreur de conception / développement                      Vice caché d'un progiciel                      Indiscrétion / détournement d'information / Attaque logique du réseau</p>					<p><i>Exemples de cause de défaillance par la <b>méthode MEHARI</b></i>                      une seule cause :                      =&gt; erreur                      =&gt; malveillance                      =&gt; accident                      une seule conséquence :                      =&gt; atteinte à la disponibilité                      =&gt; intégrité,                      =&gt; confidentialité                      =&gt; service</p>				
<p><b>Dans tous les cas, il faut lister les processus et sous-processus, puis envisager les causes et conséquences potentielles avant d'en estimer le risque et de décider des moyens à mettre en œuvre pour ramener ce risque à un niveau acceptable en fonction des possibilités et de la politique du LBM</b></p>									

**Exemple de mise en œuvre dans le cadre de la structuration du « système de gestion des SI »**

Processus concerné	Cause potentielle de défaillance	Effet indésirable de la défaillance	Mode de défaillance - M -	Fréquence d'occurrence - F -	DéTECTABILITÉ - D -	Gravité / Criticité de l'impact - C -	Criticité globale de la défaillance - R -	Moyen de maîtrise envisagé	Efficacité / commentaires
Gestion fichiers sensibles ou dictionnaires critiques	Panne du SI ou du réseau	Arrêt « Prod »	4	2	1	4	32	Redondances (serveurs, VPN, ...)	/
			4	1	1	4	16		Action OK
	Accidents / Malveillance physique	Indisponibilité matériel / logiciel	4	1	2	4	32	Sécurisation locaux	/
			4	1	1	1	4		Action OK
	Erreur d'exploitation / saisies param. (Accès ouvert)	Invalidation paramétrage	2	2	3	4	48	Log / MDP	/
			2	1	1	4	8		Action OK
	Carence de personnel / de prestataire (Incompétence)	Mauvais paramétrage	2	4	3	4	96	Formation RI	/
2			1	1	4	8	Action OK		
Vice caché	NA								
Etc...									

**Analyse basée sur la méthode MARION**

Processus « organisation de l'informatique », sous processus « maîtrises des paramétrages », voire « gestion des fichiers sensibles » avec un « cut off » choisi à 24 par le LBM => un plan d'action est mis en place au-dessus de 24, et il est considéré que les actions sont efficaces si l'estimation repasse en dessous du « cut off ». Le LBM s'attachera à hiérarchiser les différents processus et sous-processus en fonction des modes de défaillances envisagés et inversement.

Exemple de mise en œuvre dans le cadre de la structuration du « système de gestion des SI »									
Processus concerné	Cause potentielle de défaillance	Effet indésirable de la défaillance	Mode de défaillance - M -	Fréquence d'occurrence - F -	DéTECTABILITÉ - D -	Gravité / Criticité de l'impact - C -	Criticité globale de la défaillance - R -	Moyen de maîtrise envisagé	Efficacité / commentaires
Organisation générale	Panne du SI ou du réseau	Arrêt « Prod »	4	2	1	4	32	Redondances (serveurs, VPN, ...)	/
			4	1	1	4	16		Action OK
	Accidents / Malveillance physique	Indisponibilité matériel / logiciel	4	1	2	4	32	Sécurisation locaux	/
			4	1	1	1	4		Action OK
	Erreur d'exploitation	Estimer dans un ou plusieurs autres processus moins généraux (comme ci-dessous par exemple)							
Vice caché	NA								
Etc...									
Gestion fichiers sensibles ou dictionnaires critiques	Erreur d'exploitation / saisies param. (Acces ouvert)	Invalidation paramétrage	2	2	3	4	48	Log / MDP	/
			2	1	1	4	8		Action OK
	Carence de personnel / de prestataire	Mauvais paramétrage	2	4	3	4	96	Formation RI	/
			2	1	1	4	8		Action OK
	MAJ logicielle	Modif comportement	2	2	2	3	24		Cf. autres sous processus
Vice caché	NA								
Etc...									
Gestion des transferts de données	MAJ SIL, MW, ...	Modif comportement	4	3	3	3	108	Gestion des versions et traça des MAJ	Etc....
Fusion de structures et harmonisation des outils	Fusion BDD	Mélanges données	4	3	3	4	144	Procédure +++ Accès restreints +++	Etc...

Exemple de tableau destiné à évaluer l'impact d'une modification de version logicielle (utilisable par le LBM ou le fournisseur)					
Date:	N°version	O/N	descriptif	Utilisation	Impact potentiel et Suivi à envisager
Exécutable installé	1.1		SIL	Gestion Patients	
Nouvel exécutable	1.2		SIL	Gestion Patients	
Fonctionnalités	Nouvelles	O	Gestion renseignements cliniques	Données cliniques intégrées au dossier patient utilisables en validation biologique et intégrable dans le SAVB	Connexion et gestion SAVB Revalidation des règles et commentaires automatisés
	Modifiées	N	NA		
	Débuguée	N			
Champs dans la base	Ajout	N			
	Suppression	N			
	Modification	N			
Tables dans la base	Ajout	O	Table GEST_CLIN_PAT	Gestion du dossier clinique du patient	Connexion et gestion SAVB Commentaires automatisés
	Suppression	N			
	Modification	N			
Relations / Liaisons Tables	Modification	O	DOSS_PAT et GEST_CLIN_PAT		
Gestion "multi CLEUNIK"	Modification	O	Combine clé unique DOSS_PAT et GEST_CLIN_PAT à la création du dossier patient du jour		Création du dossier patient à l'accueil à vérifier (bonne prise en compte des RC dans les dossiers et les résultats vus en VB)
Connexions automatées	Ajout	N			
	Suppression	N			
	Modification	N			
Liaison HPRIM/MED/WEB	Ajout	N			
	Suppression	N			
	Modification	O			
Utilisation "briques externe"	Windows	N			
	Linux	N			
	Mac	N			
	Autres (tablettes)	N			
	Post Script Imp.	N			

## 10 BIBLIOGRAPHIE

### Références réglementaires

Directive [98/79/CE](#) du parlement européen et du conseil du 27 octobre 1998, relative aux dispositifs médicaux de diagnostic *in vitro*, JOCE du 7 décembre 1998.

Ordonnance n°2010-49 du 13 janvier 2010 relative à la biologie médicale : J.O. du 15 janvier 2010.

### Références normatives générales

Laboratoires d'analyses de biologie médicale – Exigences particulières concernant la qualité et la compétence. NF EN ISO 15189 ([AFNOR](#)).

Analyses de biologie délocalisées (ADBD) – Exigences concernant la qualité et la compétence. NF EN ISO 22870 ([AFNOR](#)).

### Documentation Cofrac

[Document Cofrac SH REF 02](#), "Recueil des exigences spécifiques pour l'accréditation des laboratoires de biologie médicale".

### Publications

#### **Descriptif standardisé "Robotique et automatisation du laboratoire" - Annales de Biologie Clinique - Volume 68 - Numéro spécial Janvier 2010**

Anne Gruson (Arras) Coordonnateur et les membres du groupe de travail : Bernard Capolaghi, Pierre Carayon, Annette Chamson, Philippe Chatron, Geneviève Dedieu, Philippe Derache, Gérard Desch, Franck Fernandez, Anne Gruson, Damien Gruson, Dominique Khenfer, Jean-Claude Maury, Bernard Poggi, Michel Sorel, Jean-Jacques Taris.

#### **Descriptif standardisé "Middleware" - Annales de Biologie Clinique - Volume 70 - Supplément 1 - Novembre 2012**

Anne Gruson (Arras) Coordonnateur et les membres du groupe de travail : Thierry Blanchard, Bernard Capolaghi, Pierre Carayon, Régine Cartier, Philippe Chatron, Geneviève Dedieu, Philippe Derache, Gérard Desch, Bruno Gauthier, Anne Gruson, Jean-Claude Maury, Yvan Monneret, Bernard Poggi, Michel Sorel, Jérôme Soucheleau, Jean-Jacques Taris.

**CI-SIS : Cadre d'Interopérabilité des Systèmes d'Information de Santé.** Version approuvée en accès libre sur le site internet de l'ASIP Santé

**Position Paper « Les fournisseurs de DM DIV et la norme NF EN ISO 15189 », SIDIV édition mai 2011**

### Sites internet

AFNOR, Association Française de Normalisation : [www.afnor.fr](http://www.afnor.fr)

ASIP Santé, Agence des systèmes d'information partagés de santé : [www.esante.gouv.fr](http://www.esante.gouv.fr)

CNIL, Commission nationale de l'informatique et des libertés : [www.cnil.fr](http://www.cnil.fr)

DMP, Dossier médical personnel : [www.dmp.gouv.fr](http://www.dmp.gouv.fr)

IHE, Integrating the Healthcare Enterprise : [www.ihe.net](http://www.ihe.net)

MSSanté, les messageries sécurisées de santé : [www.mssante.fr](http://www.mssante.fr)

SFBC, Société Française de Biologie Clinique : [www.sfbc.asso.fr](http://www.sfbc.asso.fr)

SFIL, Société Française d'Informatique de Laboratoire : [www.sfil.asso.fr](http://www.sfil.asso.fr)

SIDIV, Syndicat de l'Industrie du Diagnostic In Vitro : [www.sidiv.fr](http://www.sidiv.fr)

LA VERSION ELECTRONIQUE FAIT FOI