# Systèmes de l’information au LBM et accréditation ISO 15189 version 2012

## Partie 1

**2017**

**Didier CHAMARD**

*Biologiste LBM ISIBIO (01)*

** Les formateur déclare ne pas avoir de conflits d’intérêt avec d’autres sociétés*

# PLAN DE LA JOURNEE

**A.Généralités sur le S.I - Définitions - Référentiels et documents de travail - S.I vs 15189**

B.Réseaux - Sécurité

C.Architectures réseaux d'un LBM - Hébergements données de santé

D.Aspects pratiques SI vs 15189

# Définition : Système d'information ?

- Un système d'information (SI) = ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, regrouper, classifier, traiter et diffuser de l'information sur un environnement donné.

- Composition des SI :

  a. Terminaux : postes « clients », tablettes…

  b. Réseaux : importance en LBM multisites - Ex :

     - connexion ADSL (informations non cryptées sauf si existence d'un VPN avec clé de cryptage personnelle (1 clé par utilisateurs autorisés)

     - lien SDSL : réseau dédié et sécurisé

     - etc.

c.Serveurs :

- **CRITIQUES** : SIL, MW, analyseurs, logiciels d'aide à la validation biologique, serveurs de résultats <=> **arrêt serveurs *impacte* la production + données médicales patients**
- NON CRITIQUES <=> arrêt serveurs sans impact sur production - pas de données médicales de patients

# Référentiels et documents de travail

- Loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 :
  - Article 1 : *L'informatique doit être au service de chaque citoyen... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*
- *Normes ISO 15189 et ISO 22870*
- *SH GTA 02*
- *SH REF 02*
- *LAB GTA 09*
- *Documents de l'ASIP*
- *Instruction n° DGOS/MSIOS/2013/281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins*

*Doc en italiques seront développés ultérieurement*

+ 2 Décrets de 2016

# Décret R6211-4 modifié le 26/01/2016

Le compte rendu des examens de biologie médicale est **structuré** conformément au référentiel d'interopérabilité dénommé " volet compte rendu d'examens de biologie médicale ", pris en application du quatrième alinéa de l'article L. 1111-8. L'identification et l'authentification du biologiste médical sont réalisées conformément aux référentiels mentionnés à ce même alinéa. Ce compte rendu structuré est produit, conservé et échangé par voie électronique conformément aux **référentiels d'interopérabilité et de sécurité** arrêtés par le ministre chargé de la santé après avis du groupement d'intérêt public chargé du développement des systèmes d'information de santé partagés mentionné à l'article L. 1111-24.

Lorsque le compte rendu des examens de biologie médicale est communiqué au prescripteur par voie électronique, l'échange se fait en utilisant une **messagerie électronique sécurisée de santé**. Dès lors qu'il contribue à la coordination des soins, le compte rendu des examens de biologie médicale est inséré dans le dossier médical personnel mentionné à l'article L. 1111-14.

## Article 6

I. L'article D. 62114 du code de la santé publique s'applique au plus tard le 31 octobre 2016. Avant cette date, les laboratoires de biologie médicale qui n'appliquent pas les dispositions de l'article D. 62114 du même code respectent, pour l'élaboration et la transmission d'un compte rendu d'examen de biologie médicale par voie électronique, les recommandations décrites par le guide technique d'accréditation pour l'évaluation des systèmes d'information en biologie médicale élaboré par le Comité français d'accréditation

=> Communiqué presse SFIL

# Décret 2016-1214 du 14/09/16 relatif au signalement des incidents graves des S.I

« II. – Sont considérés comme incidents graves de sécurité des systèmes d'information les événements générateurs d'une situation exceptionnelle au sein d'un établissement, organisme ou service, et notamment :

« – les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins ;

« – les incidents ayant des conséquences sur la confidentialité ou l'intégrité des données de santé ;

« – les incidents portant atteinte au fonctionnement normal de l'établissement, de l'organisme ou du service.

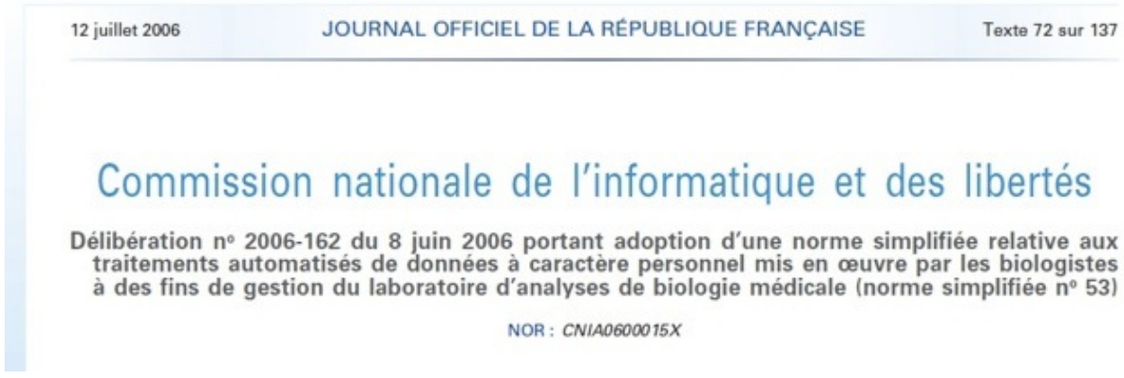
« III. – Parmi les incidents graves de sécurité des systèmes d'information, sont jugés significatifs les incidents ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé et les incidents susceptibles de toucher d'autres établissements, organismes ou services.

« *Art. D. 1111-16-3.* – La déclaration des incidents graves de sécurité des systèmes d'information, sans préjudice des autres déclarations obligatoires, est effectuée sans délai par le directeur de l'établissement de santé, de l'organisme ou du service exerçant des activités de prévention, de diagnostic ou de soins, ou la personne



déléguée à cet effet, auprès du directeur général de l'agence régionale de santé. L'agence régionale de santé est responsable de la qualification des incidents signalés.

# C.N.I.L



12 juillet 2006 JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE Texte 72 sur 137

Commission nationale de l'informatique et des libertés

Délibération nº 2006-162 du 8 juin 2006 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les biologistes à des fins de gestion du laboratoire d'analyses de biologie médicale (norme simplifiée nº 53)

NOR : *CNIA0600015X*

**Art. 1er. – *Champ d'application.***

Peuvent bénéficier de la **procédure de déclaration simplifiée** *(n° 53)* de conformité à la présente norme les traitements de données à caractère personnel mis en oeuvre au sein des laboratoires d'analyses de biologie médicale qui répondent aux conditions définies aux articles 2 à 7 ci-après.

La présente norme **ne s'applique pas** aux traitements mis en oeuvre au sein des laboratoires spécialisés dans la pratique des examens des caractéristiques génétiques d'une personne à des fins médicales définis à l'article R. 1131-2 du code de la santé publique ou de l'identification par empreintes génétiques dans le cadre de procédures judiciaires. Elle ne s'applique pas à ceux mis en oeuvre au sein des laboratoires qui pratiquent des activités d'assistance médicale à la procréation.

Elle ne s'applique pas non plus aux traitements mis en oeuvre au sein des laboratoires d'anatomo-cytopathologie.

- Documents de la SFIL (CCN, brochure accompagnement à l'accréditation)

Retour catégorie Rechercher Soumettre un fichier

# DOCUMENT D'ACCOMPAGNEMENT À L'ACCRÉDITATION - V2

## Documents

Trier par : Titre | **Date** | Clics [ Croissant ]

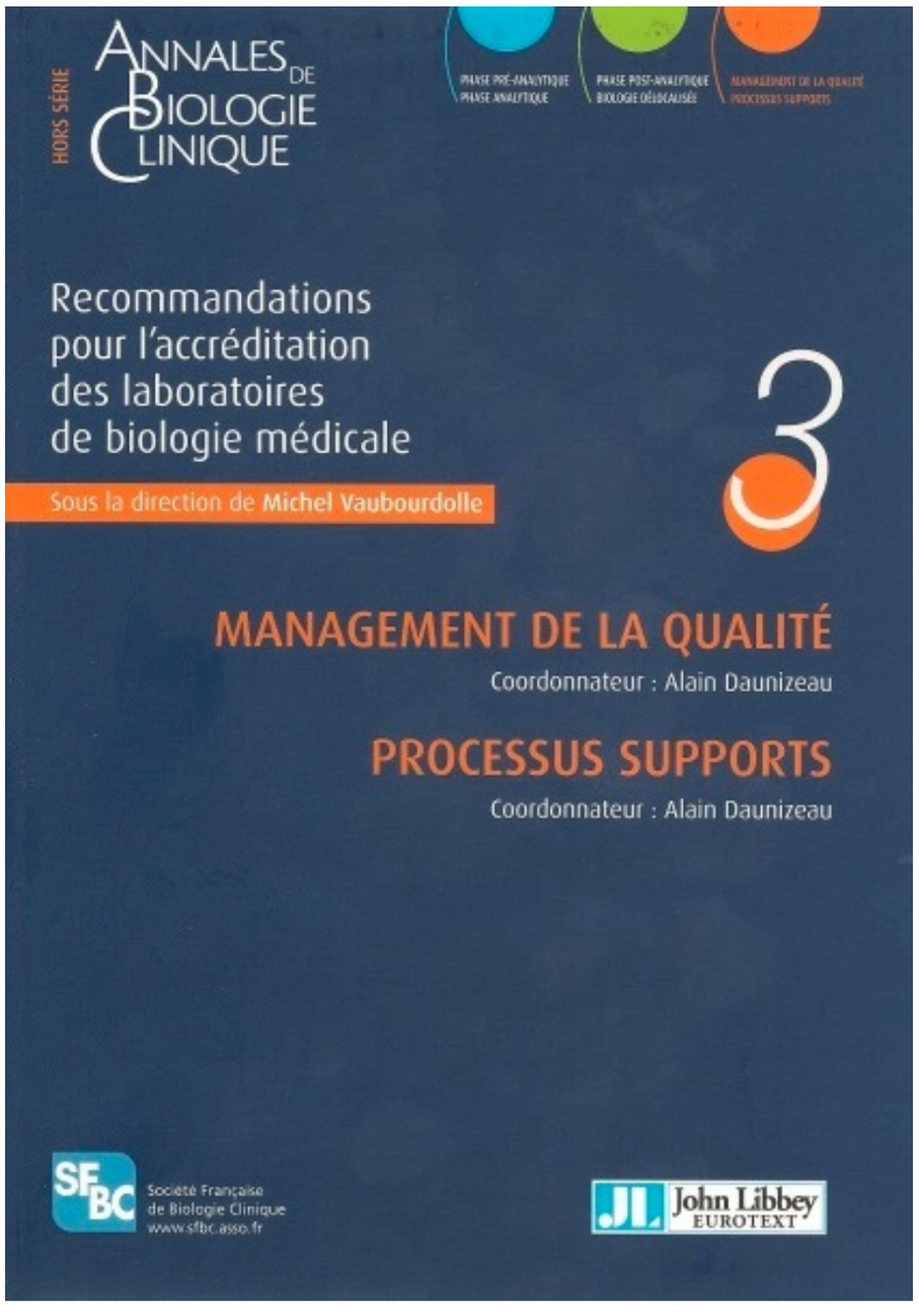
### Document d'accompagnement V2

**nouveau !**

| | |
|---|---|
| **Date de mise en ligne:** | 05/12/2014 |
| **Date de modification:** | 05/12/2014 |
| **Taille du fichier:** | 2.04 MB |
| **Téléchargements:** | 49 |

Télécharger Voir Propriétes

- A.B.C tome 3 : *Recommandations pour l'accréditation des laboratoires de Biologie Médicale* (SFBC)



- Politique Générale de Sécurité des Systèmes d'Information de Santé (**PGSSI-S**) <=> cf. sites SFIL et ASIP

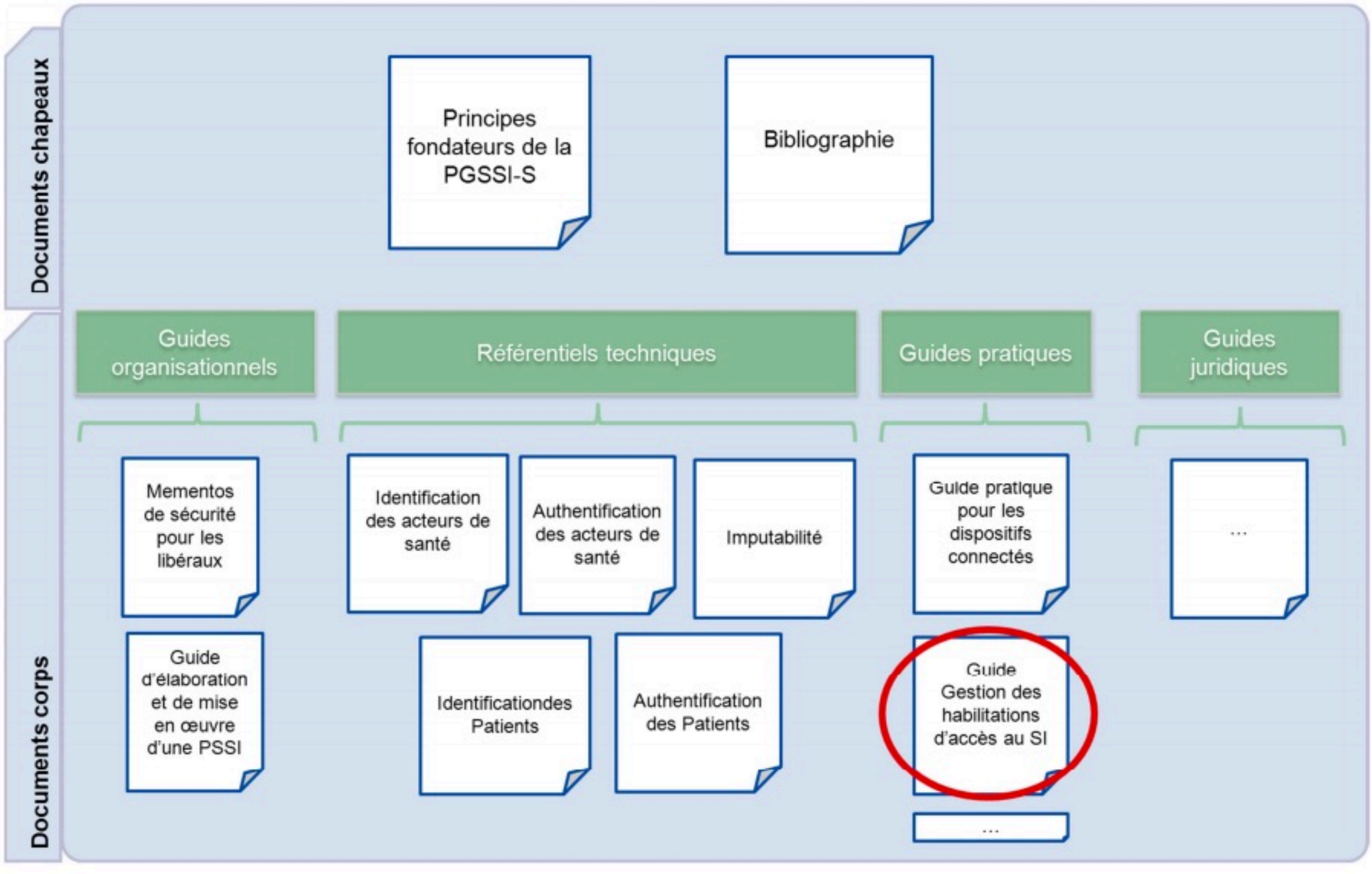



Figure 1 : Organisation du Corpus documentaire de la PGSSI-S

# S.I vs norme ISO 15189

**NF EN ISO 15189**

DÉCEMBRE 2012

www.afnor.org



**EXIGENCES POUR L'ACCREDITATION SELON LA NORME NF EN ISO 15189**

**SH REF 02**
Révision 05



cofrac

## 4.13 Maîtrise des enregistrements

Le laboratoire doit disposer d'une procédure documentée d'identification, de recueil, d'indexation, d'accès, de conservation, de mise à jour, de modification et d'élimination sûre des enregistrements qualité et des enregistrements techniques.

Les performances de chaque activité pouvant affecter la qualité du résultat doivent faire l'objet d'un enregistrement.

NOTE 1 Les enregistrements peuvent être dans n'importe quel format ou type de support à condition qu'ils soient facilement accessibles et protégés contre les modifications non autorisées.

NOTE 3 Pour certains enregistrements, plus particulièrement ceux stockés sur un support électronique, un stockage plus sûr peut impliquer d'utiliser des supports sécurisés et un site extérieur (voir 5.9.4).

### 4.14.6 Gestion des risques

Le laboratoire doit évaluer l'impact des processus de travail et défaillances potentielles sur la sécurité des résultats des examens et doit modifier les processus pour réduire ou éliminer les risques identifiés, et documenter les décisions et actions menées.

### 5.1.5 Formation

Le laboratoire doit assurer la formation pour l'ensemble du personnel, qui inclut les domaines suivants:

a) le système de management de la qualité;

b) les processus de travail et procédures attribuées;

c) le système d'information applicable au laboratoire;

### 5.3.1 Équipements

#### 5.3.1.1 Généralités

Le laboratoire doit disposer d'une procédure documentée pour la sélection, l'achat et la gestion du matériel.

### 5.3.1.2 Essais d'acceptation de l'équipement

Le laboratoire doit vérifier, lors de l'installation et avant utilisation, que le matériel est capable d'atteindre la performance nécessaire et qu'il est conforme aux exigences relatives aux examens concernés (voir aussi 5.5.1)

NOTE Cette exigence s'applique au matériel utilisé dans le laboratoire, au matériel prêté ou au matériel utilisé dans des locaux associés ou mobiles par des tiers autorisés par le laboratoire.

Chaque élément du matériel doit être étiqueté, marqué ou identifié d'une façon univoque.

### 5.3.1.5 Maintenance et réparation du matériel

Le laboratoire doit disposer d'un programme documenté de maintenance préventive qui, au minimum, observe les instructions du fabricant.

### 5.3.1.6 Compte rendu des événements indésirables

Les incidents et accidents défavorables qui peuvent être attribués directement à du matériel spécifique doivent être étudiés et signalés au fabricant et aux autorités appropriées, si nécessaire.

## 5.10 Gestion des informations de laboratoire

### 5.10.1 Généralités

Le laboratoire doit avoir accès aux données et informations nécessaires pour fournir un service qui répond aux besoins et exigences de l'utilisateur.

Le laboratoire doit disposer de procédures documentées pour garantir la confidentialité permanente des informations des patients.

NOTE Dans la présente Norme internationale, les «systèmes d'information» comprennent la gestion des données et informations contenues dans les systèmes informatiques et non informatisés. Certaines exigences peuvent être davantage applicables aux systèmes informatiques qu'aux systèmes non informatisés. Les systèmes informatisés peuvent comprendre ceux qui sont intégrés au fonctionnement du matériel de laboratoire et des systèmes autonomes à l'aide de logiciels génériques (par exemple applications de traitement de texte, de feuille de calcul et de base de données qui génèrent, assemblent, communiquent et archivent les informations des patients et les comptes rendus).

### 5.10.2 Autorités et responsabilités

Le laboratoire doit garantir que les autorités et responsabilités concernant la gestion du système d'information sont définies, y compris la maintenance et la modification des systèmes d'information qui peuvent affecter les soins délivrés aux patients.

Le laboratoire doit définir les autorités et responsabilités de l'ensemble du personnel qui utilise le système, en particulier ceux qui

a) ont accès aux données et informations de patients,

b) saisissent les données des patients et les résultats,

c) modifient les données des patients ou les résultats, et

d) autorisent la diffusion des résultats et comptes rendus.

### 5.10.3 Gestion du système d'information

Le ou les systèmes utilisés pour la collecte, le traitement, l'enregistrement, le compte rendu, le stockage ou la récupération des données et informations doivent être

a) validés par le fournisseur et vérifiés en termes de fonctionnement par le laboratoire avant application, avec les changements apportés au système autorisés, documentés et vérifiés avant mise en œuvre,

NOTE La validation et la vérification comprennent, si applicable, le bon fonctionnement des interfaces entre le système d'information du laboratoire et les autres systèmes (par exemple avec l'instrumentation du laboratoire, les systèmes d'administration des patients hospitaliers et des systèmes de soins primaires).

b) documentés, et la documentation (y compris celle pour le fonctionnement au jour le jour du système) facilement accessible aux utilisateurs autorisés,

c) protégés contre tout accès non autorisé,

d) sauvegardés en cas d'accès non autorisés ou de perte,

e) utilisés dans un environnement conforme aux spécifications du fournisseur ou, dans le cas de systèmes non informatisés, offre des conditions protégeant l'exactitude de l'enregistrement manuel et de la transcription,

f) conservés de manière à garantir l'intégrité des données et informations et comprennent l'enregistrement des défaillances du système et des actions immédiates et correctives appropriées, et

g) sont en conformité avec les exigences nationales ou internationales concernant la protection des données.

Le laboratoire doit vérifier que les résultats des examens, les informations associées et les commentaires sont reproduits avec précision, au format électronique et papier si pertinent, par les systèmes d'information externes au laboratoire destinés à recevoir directement les informations (par exemple systèmes informatiques, télécopieurs, courriel, site internet, équipements Web personnels). Lorsqu'un nouvel examen ou des commentaires automatisés sont mis en œuvre, le laboratoire doit vérifier que les modifications sont reproduites avec précision par les systèmes d'information externes au laboratoire destinés à recevoir directement les informations du laboratoire.

Le laboratoire doit disposer de plans de contingence documentés pour maintenir les prestations en cas de défaillances ou de panne des systèmes d'information qui affectent la capacité du laboratoire à fournir une prestation.

Si le ou les systèmes d'information sont gérés et entretenus hors site ou sous-traités à un autre fournisseur, la direction du laboratoire doit être chargée de s'assurer que le fournisseur ou l'opérateur du système satisfait à toutes les exigences applicables de la présente Norme internationale.

# SH REF 02 v5

5.10. Gestion des informations de laboratoire

e) - Le laboratoire met en œuvre une vérification des saisies manuelles des données électroniques/informatisées (saisie des demandes d'examens, données liées aux patients, données brutes (résultats), paramétrage des CIQ, des valeurs des étalons, ...) réalisée systématiquement ou à fréquence définie, selon une analyse bénéfice/risque, en fonction des types d'opération.

# Approche processus

Nouveauté de la version 2012 de la norme 15189 :

- Cartographie des processus
- Fiches de processus - *ex : gestion des accès distants*
- Vérification du bon fonctionnement du processus (audit interne, indicateurs, présentation en RD)

# Principaux messages

- Notion serveur critique
- Penser à faire la déclaration à la CNIL
- 5.10 = nouveauté de la version 2012 de la 15189
- L'informatique n'est pas concerné que par le 5.10 (importance 4.14.6, 5.1, 5.9, etc.)
- SH GTA 02 = guide…
- Importance croissante des documents/référentiels liés à la sécurité informatique