

Code de Conduite sectoriel

Biologie Médicale



SFIL

SOCIÉTÉ FRANÇAISE
D'INFORMATIQUE DE LABORATOIRE



provadys

Introduction

Le présent code décline la mise en œuvre du RGPD à travers 11 Fiches pratiques.

Exigences pré analytiques

FICHE 1 : Information des patients

FICHE 2 : Enregistrement des patients

FICHE 3 : Réalisation des prélèvements

FICHE 4 : Transport et collecte des échantillons biologiques

Exigences analytiques

FICHE 5 : Réalisation des examens Biologiques

FICHE 6 : Externalisation des traitements

Exigences post analytiques

Fiche 7 : Validation et diffusion des examens de Biologie Médicale

Fiche 8 : Archivage, sauvegarde et destruction des DCP

Fiche 9 : Gestion de la Facturation

Fiche 10 : Réutilisation des DCP (validation de méthodes, étude épidémiologique, publication)

Exigences liées aux services supports

FICHE 11 : Mesure de sécurité à mettre en œuvre

Les encadrés bleus correspondent aux exigences auxquelles les laboratoires doivent se conformer, le présent code de conduite constituant le cadre de référence à suivre par les adhérents afin de se conformer à la réglementation sur la protection des données.

Exigences n° XX

Les encadrés verts correspondent à des moyens possibles pour répondre aux exigences.

Recommandation n°

FICHE N° 5 Réalisation des examens Biologiques

1	Introduction	4
2	Gestion des droits des patients	4
3	Mise en œuvre du principe de Minimisation.....	5
3.1	Transmission des DCP vers les outils de productions	5
3.2	Transmission des DCP vers les outils de gestion des réclamations et des non conformités.....	5
4	Conservation des traces.....	6
5	Gestion des accès aux outils de productions.....	6
5.1	Automates.....	6
5.2	Modalités d'accès aux applications de production et au système de management de la qualité	7
5.3	Maintenance des automates et du SIL.....	7
6	Validation biologique	7
6.1	Base réglementaire et normative	7
6.2	Authentification du biologiste	7
7	Réutilisation des DCP et des échantillons à des fins de recherche interne	7
8	Bibliographie	8
	ANNEXE A : Résumé des exigences et recommandations	9

1 Introduction

La réalisation des examens va englober l'ensemble des processus permettant à partir d'un échantillon biologique la production des résultats prescrits. Ces processus englobent la prise en charge de l'échantillon sur le site de production jusqu'à la mise à disposition des résultats d'examens pour validation avant diffusion.

Certains actes de biologie médicale sont soumis à autorisation ¹ :

- Les examens de biologie moléculaire ou de biochimie ou d'immunologie, concourant au diagnostic des maladies génétiques et qui ne sont pas exécutés en vue d'établir le diagnostic prénatal ;
- Le caryotype constitutionnel ;
- Le test de migration survie des spermatozoïdes ;
- Les examens d'immunologie suivants : détermination des antigènes d'histocompatibilité, recherche et identification des anticorps antileucocytaires et antiplaquetaires, identification des populations lymphocytaires.

Les examens biologiques qui nécessitent l'utilisation de radioéléments artificiels en sources non scellées et qui ne comportent pas l'administration au malade d'un radioélément sont réservés aux biologistes possédant la compétence des personnes autorisées à utiliser des radioéléments en source non scellées à des fins médicales ².

Les analyses de cytogénétique et de biologie en vue d'établir le diagnostic prénatal ne peuvent être pratiquées que dans des structures autorisées. Cette autorisation vaut inscription sur la liste des examens de biologie médicales réservés ³.

Les examens d'anatomie et de cytologie pathologiques peuvent être réalisés en laboratoire de biologie médicale s'ils sont effectués par un médecin spécialiste qualifié d'anatomie et cytologie pathologiques ⁴.

2 Gestion des droits des patients

L'ensemble des droits des patients (le droit de rectification, le droit d'accès, etc.) concernent le SIL mais également tous les applicatifs de gestion de la production à savoir :

- Les applicatifs de gestion des tubes (middleware, concentrateur...);
- Les applications de gestion de la qualité ;
- Les automates ;
- Tous les outils permettant de gérer les résultats (document bureautique, logiciel de consolidation des sauvegardes automates...);
- Les logiciels de gestion des biothèques.

Exigence n° 1

[EX1] Le LBM doit prévoir dans sa procédure de gestion des droits des patients pour l'exercice du droit d'accès et du droit à la rectification que ces droits s'appliquent non seulement au système de gestion du laboratoire mais également à tous les applicatifs de gestion de la production du laboratoire et de ses sous-traitants.

- Les applicatifs de gestion des tubes (middleware, concentrateur...);
- Les applications de gestion de la qualité ;
- Les automates ;
- Tous les outils permettant de gérer les résultats (document bureautique, logiciel de consolidation des sauvegardes automates...);
- Les logiciels de gestion des bibliothèques.

Recommandation n° 1

[REC1] Il est recommandé au laboratoire de prévoir une procédure pour informer l'ensemble des acteurs, correspondants, sous-traitants du laboratoire, en cas de modification d'une identité ou d'un résultat d'examen.

3 Mise en œuvre du principe de Minimisation

3.1 Transmission des DCP vers les outils de productions

Pour la réalisation d'un examen, seul l'identifiant local, le numéro des échantillons et les codes examens sont strictement nécessaires à la réalisation excepté dans certains cas particuliers comprenant notamment les examens d'immunohématologie et de calcul du risque de trisomie 21 par les marqueurs sériques, qui devront faire l'objet d'un traitement différent.

Toute transmission de données à caractère personnel supplémentaires doit être justifiée par le LBM et, au besoin, faire l'objet d'une étude d'impact préalable. Ainsi si le LBM utilise son middleware pour gérer la diffusion des résultats en cas de panne du SGL, la diffusion des données relatives au prescripteur et au patient sont justifiées par la continuité de service. Cette diffusion augmente le risque de corruption de données de sorte que le LBM doit mettre en place les mesures de sécurité sur son middleware conformes à l'état de l'art.

Exigence n° 2

[EX2] Toute transmission de données à caractère personnel vers un automate ou un logiciel de gestion de production, autre que le numéro de dossier, les codes examens, et l'identifiant local pour la réalisation d'un examen doit être justifiée par le laboratoire et au besoin faire l'objet d'une étude impact préalable.

3.2 Transmission des DCP vers les outils de gestion des réclamations et des non conformités

Si l'outil de gestion des réclamations et des non-conformités utilisées par le LBM n'est pas intégré au SGL, il est recommandé aux LBM de ne transmettre à ces applications que les données strictement nécessaires à la gestion de la non-conformité ou de la réclamation, idéalement seul le numéro de dossier ou l'identifiant local devrait être transmis.

En cas d'externalisation de ces applications, l'hébergeur va stocker des données de santé. Ces données n'ayant pas été recueillies à l'occasion de soins de diagnostic ou d'activité de prévention, elles n'entrent pas dans le champ d'application de l'activité hébergement de santé ⁵. Cependant le laboratoire devra s'assurer que l'hébergeur a mis en œuvre des mesures de protection conforme à l'état de l'art et notamment aux normes iso 27 000 relative à la sécurité..

Exigence n° 3

[EX3] En cas d'utilisation d'outil de gestion des réclamations et des non conformités non intégré au système de gestion du laboratoire, le LBM devra définir les DCP nécessaires et suffisantes à leurs traitements.

Recommandation n° 2

[REC2] En cas d'externalisation des outils de gestion des non conformités et des réclamations. Il est recommandé de privilégier les hébergeurs de données certifiés ou agréés HDS.

4 Conservation des traces

Ce paragraphe fait l'objet d'un développement spécifique dans la fiche 8

5 Gestion des accès aux outils de production

Le laboratoire doit appliquer le principe du moindre privilège ⁶ et les comptes administrateurs doivent être encadré et en nombre restreint ⁷.

Exigence n° 4

[EX4] Dans sa gestion des accès, le laboratoire doit appliquer le principe du moindre privilège afin d'assurer la sécurité et la traçabilité des données conformément aux exigences de la fiche sur la sécurité du présent code de conduite.

Si la machine et/ou le logiciel ne permet pas la mise en œuvre de ce principe, le laboratoire doit se doter d'une procédure permettant d'assurer une traçabilité.

5.1 Automates

On entend par automates tous systèmes analytiques permettant de produire un résultat d'examen de biologie médicale ou de gérer un échantillon biologique qu'ils soient connectés ou non au SIL. Ce terme regroupe les automates en « stand alone », les groupes d'automates en ilot, ou les chaînes de production.

Afin d'assurer la sécurité des données et la traçabilité, chaque utilisateur doit accéder aux automates avec son propre identifiant et son ou ses moyens d'authentification. Seules les personnes habilitées, selon la politique d'habilitation mise en œuvre par le LBM, peuvent accéder aux automates ^{8,9}.

Si l'automate ne permet pas de gérer les habilitations et les accès aux données à caractère personnel, une procédure doit être mise en place afin d'assurer la traçabilité des actions sur

l'automate.

Recommandation n° 3

[REC3] Si l'automate ne permet pas de gérer les accès, le laboratoire peut s'appuyer sur le logiciel de gestion de temps pour assurer la traçabilité de personnes au poste et de la fiche de vie de l'appareil pour suivre toutes les actions réalisées sur l'automate

Les accès à distance seront décrits dans la Fiche n° 6 sur l'externalisation des traitements du LBM.

5.2 Modalités d'accès aux applications de production et au système de management de la qualité

Les exigences et recommandations s'appliquant aux automates s'appliquent également aux systèmes de gestion de la production et au système de management de la qualité.

Les contraintes liées à la téléassistance sont décrites dans la fiche n°6.

Les accès à distance seront décrits dans le chapitre « Maintenance des automates et du SIL » figurant ci-dessous.

5.3 Maintenance des automates et du SIL

Les exigences et recommandations concernant ce chapitre sont développés la fiche n°6 sur l'externalisation des traitements du LBM.

6 Réutilisation des DCP et des échantillons à des fins de recherche interne

Ce chapitre fait l'objet d'un développement spécifique dans la fiche n°10 sur la réutilisation des données et des échantillons.

7 Bibliographie

¹ [Arrêté du 6 juillet 1994 fixant la liste des actes réservés à certains laboratoires et à certaines catégories de personnes](#)

² [Arrêté du 29 avril 1988 fixant la réglementation et la liste des diplômes d'études spécialisées complémentaires de biologie médicale](#)

³ [CSP, art. L. 2131-1](#)

⁴ [CSP, art. L. 6212-2](#)

⁵ [CSP, art. L. 1111-8](#)

⁶ ANSSI [Gestion des identités et des accès](#)

⁷ CNIL, [Guide relatif à la sécurité des données personnelles, édition 2017, Sécuriser les serveurs](#)

⁸ [PGSSI-S, Guide gestion des habilitations d'accès au SI, janvier 2017, V1.0, §2.1](#)

⁹ [ASIP Santé, Référentiel de certification HDS V.1.1](#) (Norme ISO 27001:2013 A.9)

CONFIDENTIEL

ANNEXE A : Résumé des exigences et recommandations

[EX1] Le LBM doit prévoir dans sa procédure de gestion des droits des patients pour l'exercice du droit d'accès et du droit à la rectification que ces droits s'appliquent non seulement au système de gestion du laboratoire mais également à tous les applicatifs de gestion de la production du laboratoire et de ses sous-traitant

- Les applicatifs de gestion des tubes (middleware, concentrateur...);
- Les applications de gestion de la qualité ;
- Les automates ;
- Tous les outils permettant de gérer les résultats (document bureautique, logiciel de consolidation des sauvegardes automates...);
- Les logiciels de gestion des bibliothèques.

[REC1] Il est recommandé au laboratoire de prévoir une procédure pour informer l'ensemble des acteurs, correspondants, sous-traitants du laboratoire, en cas de modification d'une identité ou d'un résultat d'examen.

[EX2] Toute transmission de données à caractère personnelle vers un automate ou un logiciel de gestion de production, autre que le numéro de dossier, les codes examens, et l'identifiant local pour la réalisation d'un examen doit être justifié par le laboratoire et au besoin faire l'objet d'une étude impact préalable.

[EX3] En cas d'utilisation d'outil de gestion des réclamations et des non conformités non intégré au système de gestion du laboratoire, le LBM devra définir les DCP nécessaires et suffisantes à leurs traitements.

[REC2] En cas d'externalisation des outils de gestion des non conformités et des réclamations. Il est recommandé de privilégier les hébergeurs de donnée certifiés ou agréés HDS.

[EX4] Dans sa gestion des accès, le laboratoire doit appliquer le principe du moindre privilège afin d'assurer la sécurité et la traçabilité des données conformément aux exigences de la fiche sur la sécurité du présent code de conduite. Si la machine et/ou le logiciel ne permet pas la mise en œuvre de ce principe, le laboratoire doit se doter d'une procédure permettant d'assurer une traçabilité et une protection des données.

[REC3] Si l'automate ne permet pas de gérer les accès, le laboratoire peut s'appuyer sur le logiciel de gestion de temps pour assurer la traçabilité de personnes au poste et de la fiche de vie de l'appareil pour suivre toutes les actions réalisées sur l'automate