SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

sfil Société Française d'Informatique de laboratoire

JOURNÉE SDB – RGPD

CODE DE CONDUITE – BIOLOGIE MÉDICALE

PIAF – PRIVACY IMPACT ASSESSMENT FRAMEWORK

MARDI 10 AVRIL 2018

LEXING ALAIN BENSOUSSAN AVOCATS

provadys

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

INTRODUCTION AU RGPD

RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES

- Texte européen et **de portée générale**
- Applicable en l'état en France avec **prise d'effet au 25 Mai 2018**
- Place au cœur **les droits nouveaux des personnes et de leurs données**
- Définit les exigences des **responsables de traitements , et ceux de leurs prestataires**
- **Renforce le pouvoir de sanction** des autorités de contrôle

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LE RGPD EN BIOLOGIE MÉDICALE

- Des **exigences renforcées** liée à la nature même des **données de santé**
  - **Les données de santé : des DPC - données à caractères personnel - sensibles**
  - **Les données de santé: des données à grande échelle… locale ou nationale**

- **Des Exigences d'organisation et de sécurité du Responsable de traitement**
  - Etablir un **PIA** – Privacy Impact Assessment: Une Analyse d'Impact des DCP
  - Définir un **DPO** - Data Privacy Officer: Un Délégué à la Protection des Données DPD
  - Tenir un **Registre de traitements**

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LA SFIL FACILITE LE RGPD
BIOLOGIE MÉDICALE

- **La SFIL produit les premiers outils RGPD en Santé en France**
- Un **Code de conduite Sectoriel** – Biologie Médicale qui a vocation à être **opposable**
  - **Le respect du Code de Conduite participe à la conformité au RGPD**
  - **Intègre les exigences et les référentiels légaux européennes et nationales : Code de Santé Public, CNIL, ANSSI, HFSI, PGSSI-S**
- **PIAF – Biologie Médicale: Un outil sectoriel d'Analyse d'Impact des DCP**
  - **Appliquer le PIAF permet de se limiter à un PIA – résiduel aux cas particuliers**

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LA SFIL FACILITE LE RGPD
CODE DE CONDUITE BIOLOGIE MÉDICALE

- **Exigences communes à toutes les activités métiers liées aux**
  - **principes relatifs au traitement de données à caractère personnel**
  - **droits des personnes concernées**
  - **mesures de sécurité**
  - **incidents de sécurité et violations de données**
  - **cas de sous-traitance**
  - **Transfert de données en dehors de l'union européenne**
- **Code de Conduite exclut de son champ les services supports généraux (RH, Comptabilité)**
- **Exigences spécifiques aux activités métiers de Biologie Médicale**
- **Annexes**

LE PRINCIPE DE MINIMISATION EN PRATIQUE

> *3° [les données] sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;*
>
> *4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;*

Article 6 de la loi Informatique et Libertés

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LE PRINCIPE DE MINIMISATION EN PRATIQUE

Article 5

Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être:

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

LE PRINCIPE DE MINIMISATION EN PRATIQUE

- **Le NIR**
  Le Numéro d'Inscription au Répertoire national d'identification des personnes physiques constitue une donnée particulièrement sensible. L'utilisation du NIR par le LBM contribue à un risque d'interconnexion généralisée ou d'utilisation détournée des fichiers. Son utilisation répond à deux finalités
  - l'identification univoque des patients pour l'échange et le partage de données de santé entre professionnel de santé
  - les besoins de facturation du laboratoire

  Toute autre utilisation notamment la diffusion vers les outils de production n'a pas lieu d'être. Un identifiant local est suffisant pour suivre les échantillons biologiques au sein d'une même structure

LE PRINCIPE DE MINIMISATION EN PRATIQUE EN PRÉANALYTIQUE

Zones bloc note et commentaires : les bons réflexes pour ne pas déraper

23 avril 2014

L'utilisation de zones de commentaires libres (dite également "zones bloc-notes") est une pratique courante au sein de nombreux organismes. Elle permet par exemple d'assurer le suivi d'un dossier client ou de de personnaliser la relation commerciale. Néanmoins, son usage comporte des risques au regard de la vie privée. La CNIL, qui a déjà sanctionné à plusieurs reprises des dérives, rappelle les réflexes à adopter.

https://www.cnil.fr/fr/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper

LE PRINCIPE DE MINIMISATION EN PRATIQUE ZONES BLOC NOTE ET COMMENTAIRES

Règle n° 4 : sensibiliser les utilisateurs

La sensibilisation du personnel à la protection de la vie privée est indispensable. Elle peut prendre la forme de notes d'information, de messages d'alerte en cas d'utilisation des zones commentaires ou de formation. Le Correspondant informatique et libertés peut aussi être un relais efficace en matière de formation en interne.

https://www.cnil.fr/fr/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper

LE PRINCIPE DE MINIMISATION EN PRATIQUE ZONES BLOC NOTE ET COMMENTAIRES

Règle n° 5 : utiliser des outils conformes à la loi Informatique et Libertés

La CNIL recommande de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives. La réalisation d'audits réguliers et le recours à des outils automatiques vérifiant les mots contenus dans les zones commentaires doivent également être envisagés. Enfin des extractions des commentaires peuvent être réalisées régulièrement pour s'assurer du respect de la loi Informatique et Libertés. Si ces extractions peuvent mener à des sanctions disciplinaires, une consultation des instances représentatives du personnel et une information individuelle des salariés est nécessaire.

https://www.cnil.fr/fr/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper

LE PRINCIPE DE MINIMISATION EN PRATIQUE TRANSMISSION DES MOUVEMENTS ENTRE UN ETS ET UN LBM

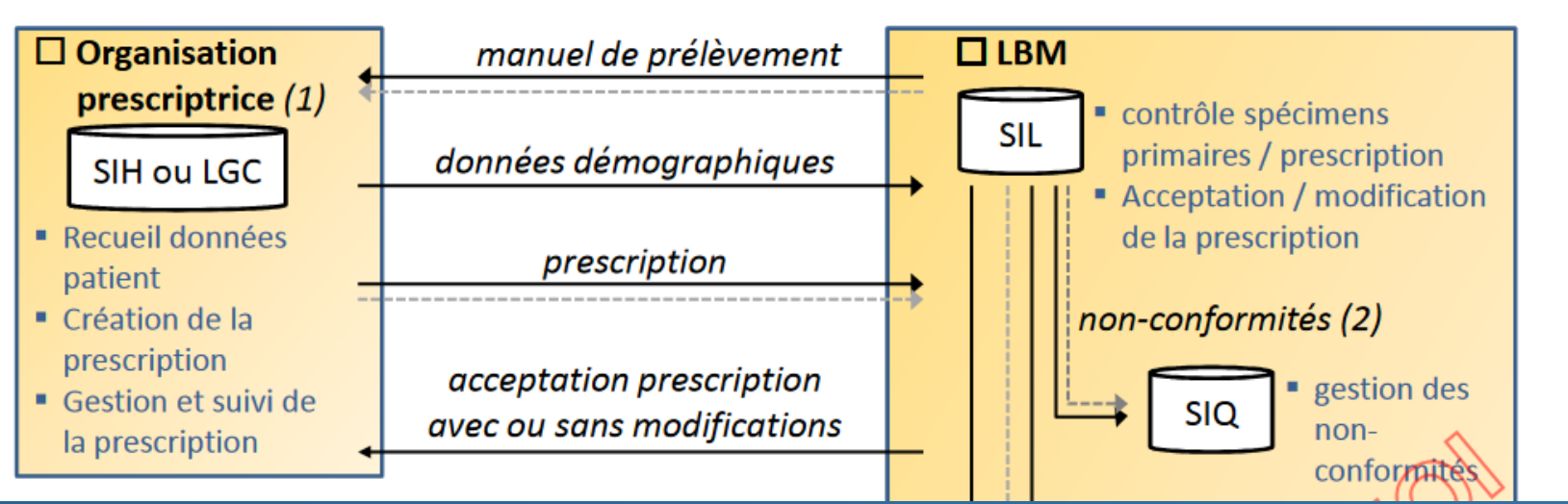


Figure 7 SH GTA 02

En cas de transmission de tous les mouvements le laboratoire devrait être certifié HDS

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LE PRINCIPE DE MINIMISATION EN PRATIQUE ANALYTIQUE : CONNEXION INFORMATIQUE

La transmission de données personnelles autres qu'un identifiant indirect différent du NIR ou de l'INS doit faire l'objet d'une étude d'impact en fonction de la finalité du traitement

LE PRINCIPE DE MINIMISATION EN PRATIQUE ANALYTIQUE : CONNEXION INFORMATIQUE

- Application de gestion des non-conformités ou des réclamations
  - En l'absence d'intégration dans le SGL on ne doit transmettre à ces outils qu'un identifiant indirect pour tous les événements concernant les patients
    - numéro de non-conformité et/ou de réclamation
    - Numéro de dossier
    - Numéro d'échantillon
  - En cas d'externalisation de ces plateformes, si elles hébergent des données sensibles, elles doivent être hébergées chez un tiers HDS.

LE PRINCIPE DE MINIMISATION EN PRATIQUE ANALYTIQUE : CONNEXION INFORMATIQUE

- Plateforme de gestion de ticket d'incident
  - si la demande concerne un patient ne transmettre que le numéro de dossier ou le numéro d'échantillon;
  - transmission des données de manière sécurisée;
    - Mails cryptés;
    - Déclaration sur un site web sécurisé
  - si elles hébergent des données sensibles, elles devraient être hébergés chez un tiers HDS ou à minima avoir mis en place des mesures de sécurités conformes au référentiel HDS.

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LE PRINCIPE DE MINIMISATION EN PRATIQUE ANALYTIQUE : CONNEXION INFORMATIQUE

- Connexion automate/middleware
  - Seul le numéro d'échantillon et les codes analyses sont nécessaires à la réalisation des examens de biologie médicale sauf cas particulier
    - Immunohématologie
    - calcul du risque de trisomie 21 par les marqueurs sériques par exemple
  - Tout autre élément présent dans la transmission doit-être évalué en fonction de la finalité ainsi pour les middlewares par exemple
    - Finalité
      - Boite noire
      - Gestion de la production
      - Backup du SGL et gestion de la Production

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LE PRINCIPE DE MINIMISATION EN PRATIQUE TESTS DE RESTAURATION DES SAUVEGARDES

- Dans le cas de la fourniture par un sous-traitant d'une prestation de test de restauration des sauvegardes, le sous-traitant s'engage à mettre en œuvre les mesures de sécurités suivantes
  - Le sous-traitant doit s'assurer que l'acheminement de la sauvegarde se fait dans des conditions permettant de préserver les données personnelles
    - Contractualisation avec le transporteur
    - Engagement de confidentialité
    - Traçabilité
    - ….
  - Les tests devraient être effectués dans un environnement agréé HDS, ou a *minima* dans un environnement cloisonné respectant le référentiel HDS
  - Les tests une fois effectués doivent donner lieu à un rapport et les restaurations supprimées sans possibilité de récupérer les données
  - Dans le cas ou le prestataire souhaite tester ces évolutions logicielles sur une sauvegarde
    - Le laboratoire doit donner son autorisation
    - La base de données doit être anonymisée

Disposer d'un serveur de test

LES NOUVEAUX DROITS DES PATIENTS

- **Droit à la rectification**

  Il s'agit du corollaire au principe général d'exactitude des données. Le patient peut exiger du LBM que soient rectifiées ou complétées les données à caractère personnel le concernant qui sont inexactes ou incomplètes.

  Ce droit concerne votre SGL mais aussi

  - Vos middlewares
  - Vos automates
  - Vos sous-traitants
  - La sérothèque
  - Les serveurs de résultats, le DMP
  - Les PS destinataires de vos comptes rendus

LES NOUVEAUX DROITS DES PATIENTS

- **Droit à l'effacement ou droit à l'oubli**

  Le patient a le droit d'obtenir l'effacement, dans les meilleurs délais, de ces données à caractère personnel lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles le LBM les a collectées ou traitées.

  Compte tenu de l'obligation de conservation des LBM, après échanges avec le patient ayant motivé sa demande, en parallèle de l'effacement, le LBM pourra conserver les données sur un support distinct, support papier ou support informatique amovible, de façon à assurer la conservation de l'information.

  Ce droit concerne votre SGL mais aussi

  - Vos middlewares
  - Vos automates
  - Vos sous-traitants
  - Les serveurs de résultats

LES NOUVEAUX DROITS DES PATIENTS

- **Droit à la portabilité**

Le droit à la portabilité apparaît comme un droit d'accès amélioré, auquel est associée une exigence d'interopérabilité. Pour ce faire, il permet à la personne concernée de recevoir les données qu'elle a fournies au responsable du traitement dans un *« format structuré, couramment utilisé et lisible par machine »*. Elle peut même exiger que les données soient transmises directement par le premier responsable au second, **lorsque cela est techniquement possible.**

Droit avec peu d'impact en LBM car cela ne concerne pratiquement que les données démographiques.

LES NOUVEAUX DROITS DES PATIENTS

- **Droit d'opposition**

Le patient peut s'opposer, pour des motifs légitimes, aux traitements mis en œuvre par le LBM

Le patient, dont un membre de la famille exerce au sein du LBM, refuse que ses données à caractère personnel soient traitées dans le SIL, à des fins de confidentialité

Mise en place d'une procédure de pseudonymisation
Afin de permettre au patient de faire réaliser ses examens de biologie.

LES NOUVEAUX DROITS DES PATIENTS

- **Droit de définir des directives sur le sort de ses données après son décès**

Les patients peuvent également définir des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès, étant précisé que toute communication des données de santé des patients doit être réalisée dans le respect des règles du Code de la santé publique et notamment l'article L. 1110-4 de ce code.

Ce nouveau droit comme tous les autres doit faire l'objet d'une information éclairée, précise et concise au patient

PRÉCISIONS SUR LE DROIT D'INFORMATION

- Le LBM doit s'assurer que la collecte des données à caractère personnel ne puisse être effectuée sans information des patients
- Le LBM doit s'assurer que l'information est délivrée avant la collecte des données personnelles
  - Pour les prélèvements réalisés à domicile, l'information doit être fournie au patient par le préleveur
  - En cas d'examens de biologie médicale réalisés en établissement de santé, cette information devra être fournie par ce même établissement au moment de l'admission ou de la préadmission

L'HÉBERGEMENT DE DONNÉES DE SANTÉ

- Art. R. 1111-9.-Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L. 1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R. 1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes :
  - 1° La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
  - 2° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
  - 3° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
  - 4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
  - 5° L'administration et l'exploitation du système d'information contenant les données de santé ;
  - 6° La sauvegarde des données de santé.
- Art. R. 1111-8-8 – I …

  Toutefois, ne constitue pas une activité d'hébergement au sens de l'article L. 1111-8, le fait de se voir confier des données pour une courte période par les personnes physiques ou morales, à l'origine de la production ou du recueil de ces données, pour effectuer un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données.

L'archivage n'est pas couvert par la certification HDS

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

L'HÉBERGEMENT DE DONNÉES DE SANTÉ

- Art. L. 1111-8. …
  - II.-L'hébergeur de données mentionnées au premier alinéa du I sur support numérique est titulaire d'un certificat de conformité. S'il conserve des données dans le cadre d'un service d'archivage électronique, il est soumis aux dispositions du III.
    …
  - III.-L'hébergeur de données mentionnées au premier alinéa du I est agréé par le ministre chargé de la culture pour la conservation de ces données sur support papier ou sur support numérique dans le cadre d'un service d'archivage électronique.
    Les conditions d'agrément sont fixées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé.
    L'agrément peut être retiré, dans les conditions prévues par les articles L. 121-1, L. 121-2 et L. 122-1 du code des relations entre le public et l'administration, en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

CERTIFICATION HDS
QUI EST CONCERNÉ ?

- Les structures qui hébergent des données de santé pour des tiers
  - Dès lors que la structure héberge les données de santé à caractère personnel de tiers (toute personne morale distincte de la structure, y compris une société du même Groupe), il est considéré comme un hébergeur de données de santé et doit se conformer au référentiel de certification et être certifié hébergeur de données de santé.
    - Concerne l'infrastructure matérielle et applicative
    - Concerne toutes les applications susceptibles de contenir des données de santé
      - SGL
      - Middleware
      - Logiciel de Gestion de la qualité

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

CERTIFICATION HDS
QUI EST CONCERNÉ ?

- Les éditeurs de SGL
  - Dès lors qu'ils ont un lien ouvert permanent vers l'infrastructure du laboratoire afin d'assurer la maintenance applicative et matérielle
  - Dès lors que leur plateforme de gestion de ticket d'incident traite des données de santé
  - Dès lors qu'ils proposent des prestations de test de restauration à l'extérieur du laboratoire
- Les fournisseurs d'automates (si l'automate contient des données de santé)
  - Dès lors qu'ils ont un lien ouvert permanent vers l'infrastructure du laboratoire afin d'assurer la maintenance applicative et matérielle de l'automate.
  - Dès lors que leur plateforme de gestion de ticket d'incident traite des données de santé
  - Dès lors qu'ils hébergent l'environnement applicatif d'un automate d'un laboratoire pour des besoins de maintenance

HÉBERGEMENT DE DONNÉES DE SANTÉ QUEL RÉFÉRENTIEL ?

- L'hébergement des données de santé doit être réalisé dans des conditions assurant leur sécurité c'est-à-dire leur protection en matière de confidentialité, intégrité et disponibilité .

- Quel est l'état de l'art: le référentiel HDS

Toute structure hébergeant des données de santé doit mettre en œuvre ce référentiel HDS

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

PRIVACY BY DESIGN, PRIVACY BY DEFAULT QUEL IMPACT POUR LE LABORATOIRE ?

PARAGRAPHE 71

- protection dès la conception :
  le LBM doit mettre en œuvre, en amont et lors de la détermination des moyens du traitement, des mesures techniques et organisationnelles destinées à mettre en œuvre les principes relatifs à la protection des données du patient, notamment au regard des risques dont la probabilité et la gravité varient, que présente le traitement pour les droits et libertés des patients …
- protection par défaut :
  le LBM doit garantir la protection des données par défaut c'est-à-dire garantir que, par défaut, seules les données nécessaires à la finalité spécifique du traitement sont traitées. Ces principes s'appliquent à la quantité des données, l'étendue de leur traitement, leur durée de conservation et leur accessibilité.

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

PRIVACY BY DESIGN, PRIVACY BY DEFAULT QUEL IMPACT POUR LE LABORATOIRE ?

SECURITE DES MOTS DE PASSE

- Le LBM doit protéger l'accès aux données par la mise en œuvre d'une politique de mots de passe conforme aux exigences de la Cnil et de l'Anssi.
  - Les mots de passe doivent être nominatifs et associés à des comptes nominatifs. Les comptes génériques sont à proscrire ;
  - S'agissant des modalités de création d'un mot de passe requis pour l'authentification à un compte, la taille minimale et la complexité de ce mot de passe doivent être imposées par le LBM
- Les mots de passe doivent être régulièrement renouvelés, une fois tous les six mois. Si les utilisateurs n'ont pas modifié leur mot de passe avant la date limite, les postes de travail doivent être verrouillés dans le but de forcer le changement de mot de passe

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

PRIVACY BY DESIGN, PRIVACY BY DEFAULT QUEL IMPACT POUR LE LABORATOIRE ?

DUREE DE CONSERVATION

- **Principe de limitation**. Les données sont conservées pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Chaque LBM doit disposer d'une politique de durée de conservation des données en application de son obligation d'« accountability »
- Lorsque la durée de conservation n'est pas définie par un texte, il appartient à chaque gestionnaire de LBM de définir la durée, notamment en fonction de la finalité du traitement et du risque contentieux
- Le corollaire au principe de limitation du traitement est l'obligation de **suppression des données**

PRIVACY BY DESIGN, PRIVACY BY DEFAULT QUEL IMPACT POUR LE LABORATOIRE ?

SUPPRESSION DES DONNEES

- il convient de prévoir un système de purge automatique ou manuelle des données dont la durée de conservation est atteinte, au moins une fois par mois, c'est-à-dire que chaque mois, à date fixe, les données qui ont été conservées un certain temps (ex. 10 ans glissant) sont supprimées.
- Les LBM doivent s'assurer que les fichiers « flaggés » comme supprimés, mais qui peuvent être restaurés, sont régulièrement supprimés par l'applicatif. Cette vérification peut être effectuée par le biais d'un rapport annuel sur la taille des bases de données ou d'un audit.

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

PRIVACY BY DESIGN, PRIVACY BY DEFAULT QUEL IMPACT POUR LE LABORATOIRE ?

ARCHIVAGES DES DONNEES

- L'archivage numérique, pour être, probant doit permettre d'assurer, comme indiqué à l'article « Exigences liées aux mesures de sécurité » du présent code de conduite :
  - l'intégrité de la donnée, en stockant des données figées (fichiers FEC en comptabilité, fichier scellé ou signé électroniquement), en assurant la confidentialité (gestion des droits d'accès) et en assurant la traçabilité des consultations et l'historique de toute action
  - l'authenticité du document, grâce à l'horodatage et le scellement voire la signature électronique
  - l'intelligibilité des documents en utilisant des formats standards pour permettre leur lisibilité dans le temps : TIFF, PDF/A, CDA R2

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

PRIVACY BY DESIGN, PRIVACY BY DEFAULT QUEL IMPACT POUR LE LABORATOIRE ?

PLAN DE CONTINUITE D'ACTIVITE/PLAN DE REPRISE D'ACTIVITE

- Le LBM doit:
  - rédiger un plan de reprise d'activité et un plan de continuité d'activité informatique, mentionnant tous les intervenants
  - informer les utilisateurs, les prestataires et les sous-traitants concernant les personnes du LBM à alerter en présence d'un incident
  - effectuer régulièrement des tests de restauration, au moins un test de restauration annuel de l'ensemble des données doit être
  - effectué et, en fonction de l'étude de risques du laboratoire, des tests de restauration partiels peuvent être réalisés à une fréquence plus élevée. A ce titre, les tests de restauration peuvent être réalisés de manière systématique, ponctuelle, ou de manière générale pour une restauration entière du SIL
- **Même en cas de situation dégradée**, les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

Société Française d'Informatique de laboratoire

SFIL – La réglementation sur la protection des données et le principe d'accountability

Journée SFIL/SDB – **RGPD** –10 avril 2018

1. NOTION

Article 24

Définition de l'accountability

- L'accountability désigne l'obligation pour les acteurs de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données (Cnil, Accountability).
- L'efficacité des mesures prises doit également être démontrée (considérant 74 du RGPD).

L'accountability implique pour le responsable du traitement

- de prendre des mesures appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD (art. 24 du RGPD).

1. NOTION

Article 24

Les mesures doivent tenir compte

- De la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques que celui-ci présente pour les droits et libertés des personnes physiques (considérant 74, art. 24 du RGPD)

La mise en œuvre d'un code de conduite participe au respect de ce principe

- L'application d'un code de conduite approuvé comme le prévoit le RGPD peut servir d'élément pour démontrer le respect des obligations incombant au responsable de traitement (art. 24 du RGPD).

Lien avec le référentiel de certification HDS

- Cette obligation documentaire fait partie du Système de management de la Sécurité de l'Information (SMSI) visé par la norme ISO 27001 dont la mise en place facilite le respect du principe d'accountability.

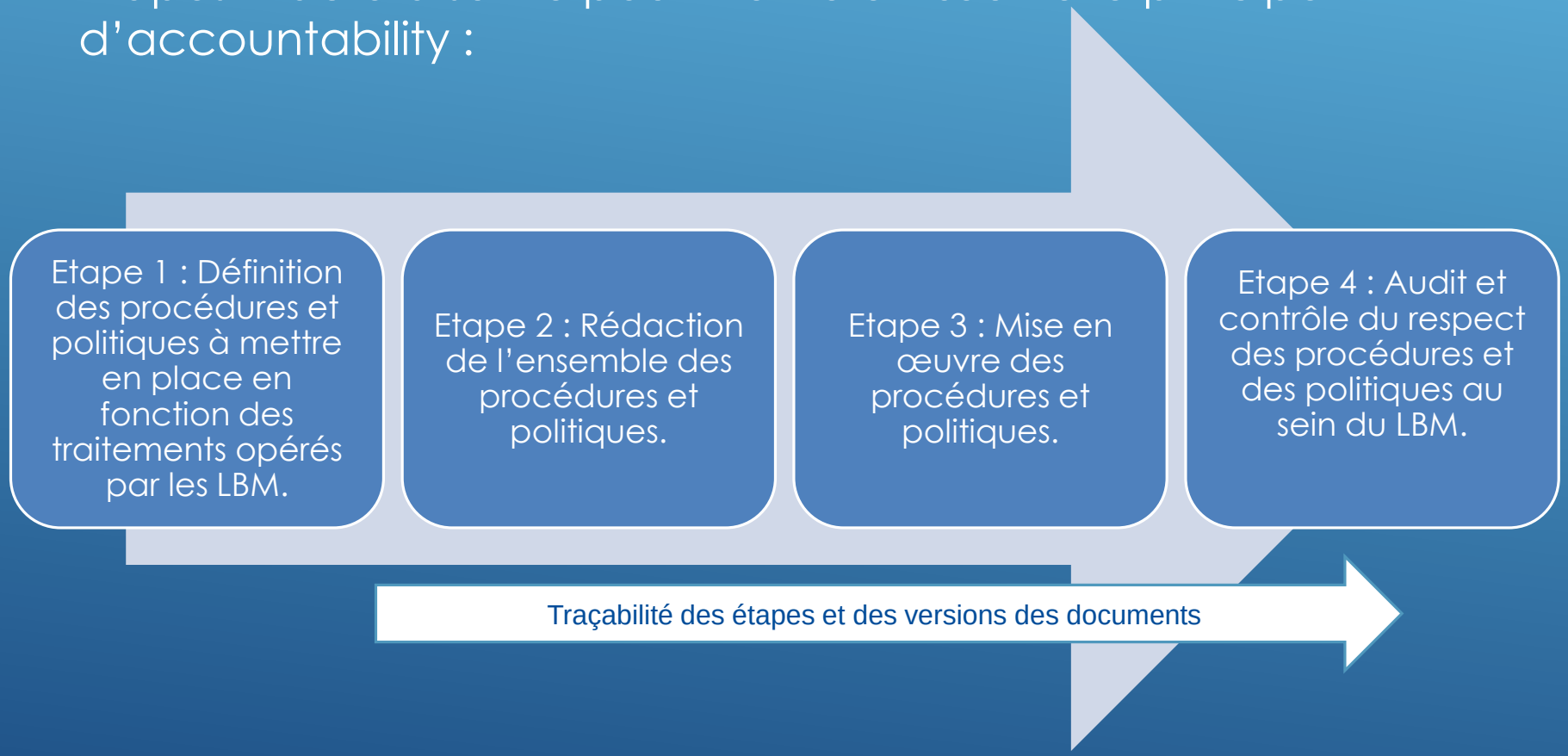
2. MISE EN CONFORMITÉ

Mise en œuvre du principe d'accountability

Exemples de documents d'accountability annexés au code de conduite

2.1 MISE EN ŒUVRE DU PRINCIPE D'ACCOUNTABILITY

- Etapes macro à suivre pour mettre en œuvre le principe d'accountability :



2.1 MISE EN ŒUVRE DU PRINCIPE D'ACCOUNTABILITY

- La Cnil recommande de constituer un dossier comportant les éléments suivants (Cnil, Documenter la conformité) :

Documentation sur les traitements de données	Documentation sur l'information des personnes	Documentation contractuelle ayant pour objet de définir les rôles et les responsabilités des acteurs
• Registre des traitements ; • Analyses d'impact sur la protection des données pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes ; • Encadrement des transferts de données hors de l'UE (clauses contractuelles types, BCR, etc.).	• Mentions d'information ; • Modèles de recueil de consentement, le cas échéant ; • Procédures de mises en place pour l'exercice des droits	• Contrats avec les sous-traitants ; • Procédures internes en cas de violations de données ; • Preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

2. MISE EN CONFORMITÉ

Mise en œuvre du principe d'accountability

Exemples de documents d'accountability annexés au code de conduite

2.2 EXEMPLES DE DOCUMENTS D'ACCOUNTABILITY ANNEXÉS AU CODE DE CONDUITE

Modèle d'information des patients

- Ce document permet d'informer les patients sur les traitements de données qui le concernent, l'utilisation des fonds de tube et, le cas échéant, l'hébergement de leurs données.

Procédure de délivrance de l'information des patients

- Ce document a pour objet de présenter la procédure à suivre pour informer les patients du LBM et notamment : le contenu de l'information et les modalités de fourniture de l'information.

Charte de protection des données

- Ce document a pour objet de formaliser les règles de déontologie et de sécurité que s'engagent à respecter tous les utilisateurs du système d'information du LBM.

2.2 EXEMPLES DE DOCUMENTS D'ACCOUNTABILITY ANNEXÉS AU CODE DE CONDUITE

Procédure de gestion des droits d'accès des patients

- Ce document a pour objet de présenter la procédure à suivre pour répondre aux demandes d'exercice de droits d'accès formulées par les patients du LBM.

Modèle de CGU de serveur de résultats

- Ce document a pour objet de définir les conditions d'accès et les modalités d'utilisation du serveur de résultats par le patient.

Charte d'utilisation du Wifi au sein d'un LBM

- Ce document a pour objet de définir les conditions dans lesquelles les utilisateurs peuvent bénéficier de la fourniture du Wifi par le LBM.

2.2 EXEMPLES DE DOCUMENTS D'ACCOUNTABILITY ANNEXÉS AU CODE DE CONDUITE

Modèle de registre des traitements

- Ce document a pour objet de recenser l'ensemble des traitements mis en œuvre par le LBM.

PIAF

- Ce document a pour objet d'apporter une aide aux LBM dans la réalisation de leurs rapports d'analyse d'impact.

Politique de sécurité du LBM

- Ce document a pour objet de présenter les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information du LBM.

2.2 EXEMPLES DE DOCUMENTS D'ACCOUNTABILITY ANNEXÉS AU CODE DE CONDUITE

Procédure de réaction et de notification des incidents de sécurité et des violations de données

- Ce document a pour objet de présenter les aspects stratégiques et juridiques relatifs aux incidents de sécurité mettant en cause des données.

Modèle de registre des violations de données

- Ce document a pour objet de documenter toute violation de données, en indiquant les faits concernant la violation des données, ses effets et les mesures prises pour y remédier. Il permet à l'autorité de contrôle de vérifier le respect de l'article 33 du RGPD.

Lettre de mission du délégué à la protection des données

- Ce document a pour objet de nommer le DPO et de présenter l'ensemble de ses missions.

2.2 EXEMPLES DE DOCUMENTS D'ACCOUNTABILITY ANNEXÉS AU CODE DE CONDUITE

Modèles de clauses obligatoires du contrat de sous-traitance :

- Pour les contrats liant le LBM et un éditeur de logiciel de gestion (intégration, gestion, extension du SIL).
- Pour les contrats liant le LBM avec un fournisseur d'automate (intégration et maintenance de l'automate).
- Pour les contrats liant le LBM avec un autre LBM.

Guide de négociation des contrats d'hébergement de données de santé

- Ce document a pour objet de guider les LBM dans le cadre de la négociation des contrats HDS et notamment :
  - identifier les clauses qu'il est recommandé de négocier ;
  - présenter le contenu des négociations recommandées aux LBM.

Convention de preuve entre LBM et professionnels de santé

- Ce document a pour objet de définir les conditions dans lesquelles le professionnel donne son accord au LBM à l'usage du procédé de dématérialisation et de communication électronique des CR d'examens et l'admet comme preuve.

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

Société Française d'Informatique de laboratoire

SFIL – Réglementation sur la protection des données – PIAF

Journée SFIL/SDB – **RGPD** –10 avril 2018

SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

QU'EST-CE QU'UN PIA ?

Privacy Impact Assessment

Risques sur la vie privée des personnes
Atteintes aux droits et libertés individuelles

Qui

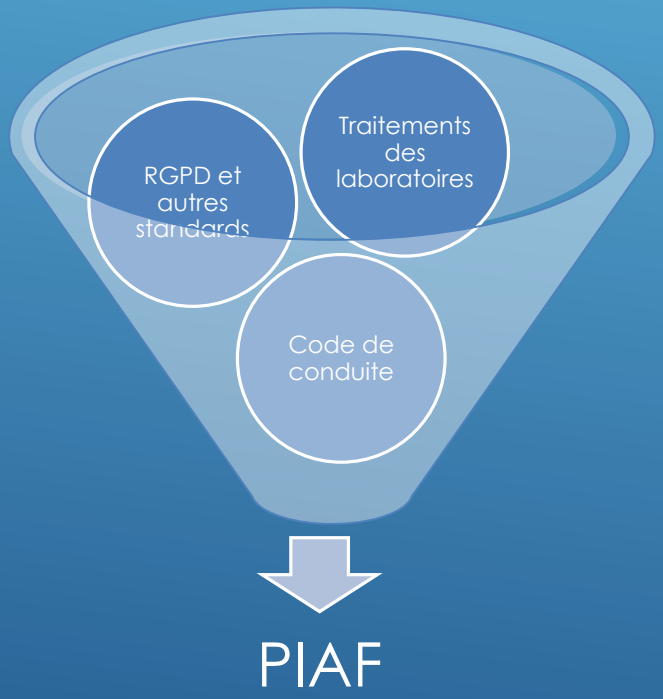
Responsable du traitement est en charge de réaliser le PIA.
Délégué à la Protection des Données (DPO) peut être sollicité pour contribution, à minima, il doit donner son avis.
Acteurs du traitement peuvent être mis à contribution du fait de leur connaissance du traitement. Ils doivent, à minima, être informés des décisions.
Direction valide les résultats et décisions suite au PIA.

Quels traitements ?

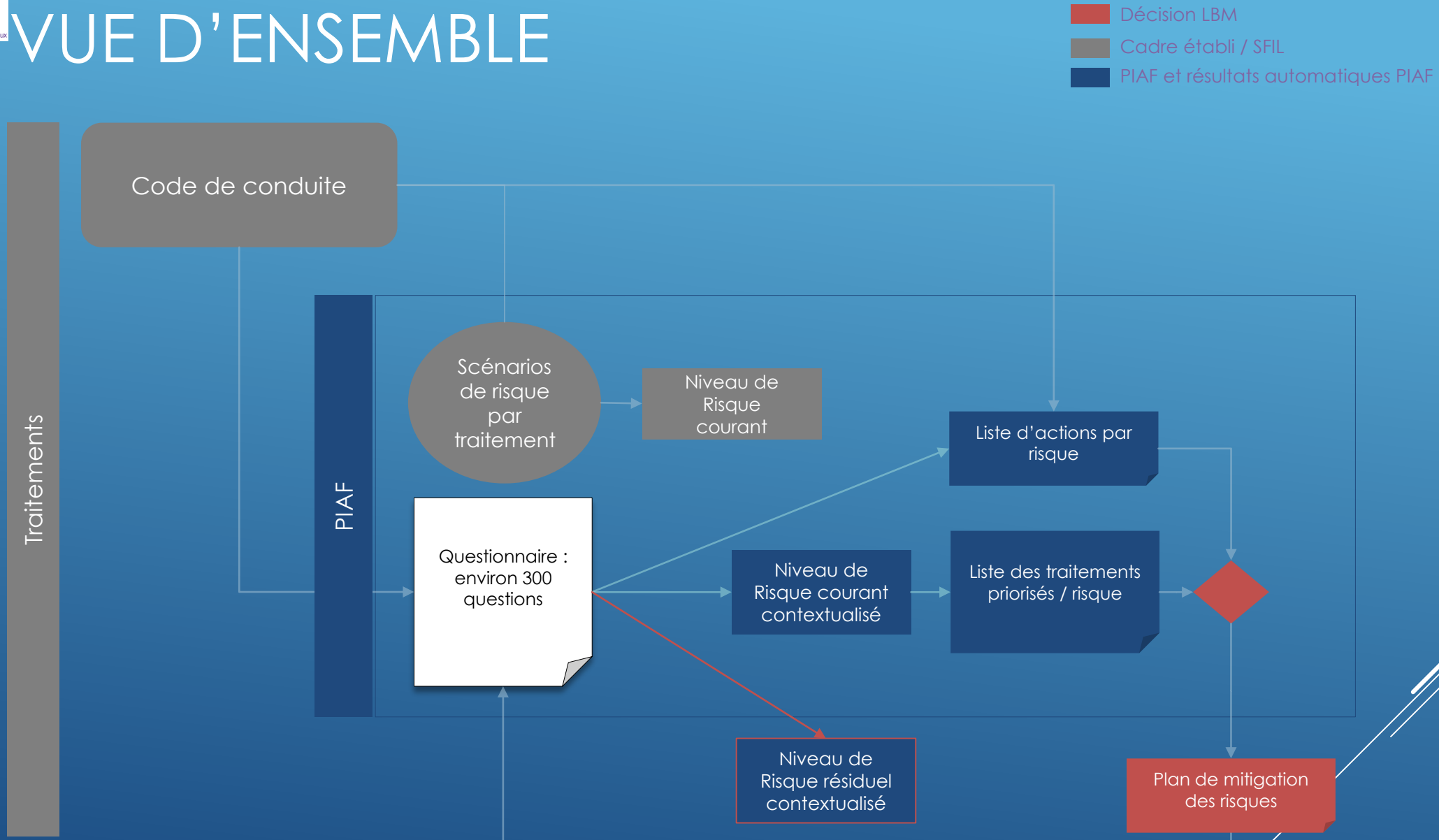
Volume de données important
Données d'individus vulnérables
Données de santé

LA RÉPONSE DE LA SFIL : LE PIAF !

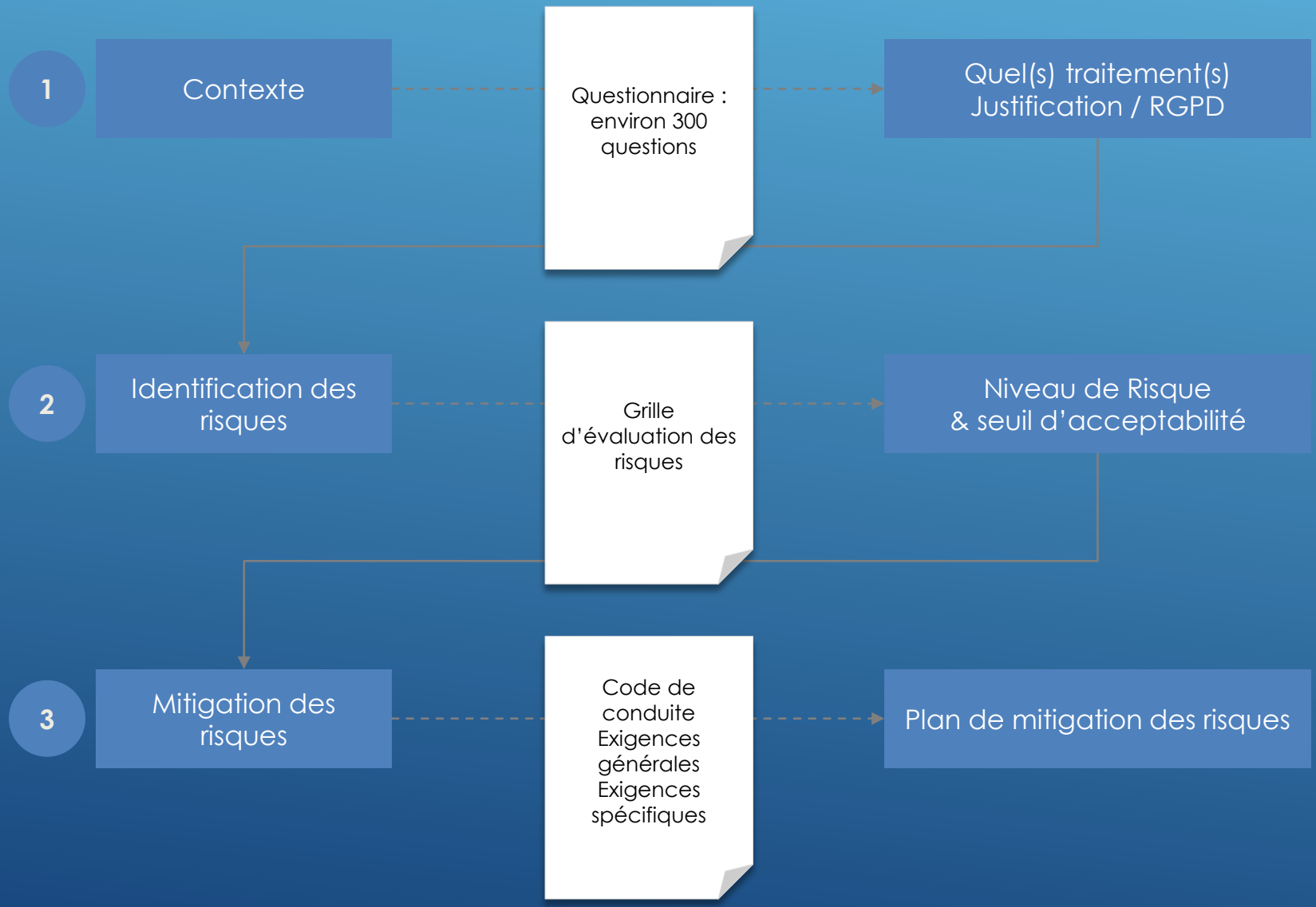
- Objectifs
  - Apporter une aide aux Laboratoires de Biologie Médicale dans la réalisation de leurs PIA
    - Identification les traitements nécessitant de conduire un PIA
    - Sélection des solutions de mitigation du risque (issues du code de conduite)
    - Traçabilité des décisions
  - Faciliter les prises de décisions
    - Quels risques sur les droits et libertés fondamentales des individus (patients en particulier) ?
    - Quels dispositifs de prévention et de protection à mettre en œuvre ?



VUE D'ENSEMBLE



UN PROCESSUS CLASSIQUE



LES RISQUES SUR LA VIE PRIVÉE

- Deux critères d'impact : perte de chance et impacts moraux
  - Perte de chance

Mesure d'impacts sur la vie privée : perte de chance		
Niveau	**Perte de chance**	**Exemple**
1	Mineure	Gêne faible pour le patient : Indisponibilité des données pour le remboursement ou la prise en charge
2	Modérée	Gêne modérée pour le patient : Geste invasif ou nouveau prélèvement nécessaire Retard de mise à disposition d'un résultat sans conséquence sur son état de santé Report de consultations
3	Majeure	Gêne majeure pour le patient : Aggravation de l'état de santé du patient Altération de prise en charge Retard ou absence de prise en charge dans un processus PMA Description : Mauvaise interprétation diagnostique qui induit une mauvaise prise en charge clinique
4	Irrémédiable	Décès du patient Retard sur une urgence vitale (ex : numération) Donnée produite mais retard de transmission

LES RISQUES SUR LA VIE PRIVÉE

- Deux critères d'impact : perte de chance et impacts moraux
  - Impacts moraux

Mesure d'impacts sur la vie privée : impacts moraux

Niveau	Moraux	Description
1	Mineurs	Impact strictement personnel sans conséquence sur l'environnement social ou familial du patient Exemple : Cholestérol divulgué à un tiers
2	Modérés	Impact sur l'environnement familial et social proche durant une période limitée Exemple : divulgation à un tiers d'un résultat de test de grossesse
3	Majeurs	Impact sur l'environnement familial et social étendu durant une période prolongée Exemple : Divulgation à un tiers d'un résultat de sérologie, hépatite C ou VIH avec risque de perte d'emploi ou de refus de prêt
4	Irrémédiables	Impact affectant la survie du patient Exemple : divulgation à un tiers d'un résultat concernant une maladie génétique, dégénérative ou incurable

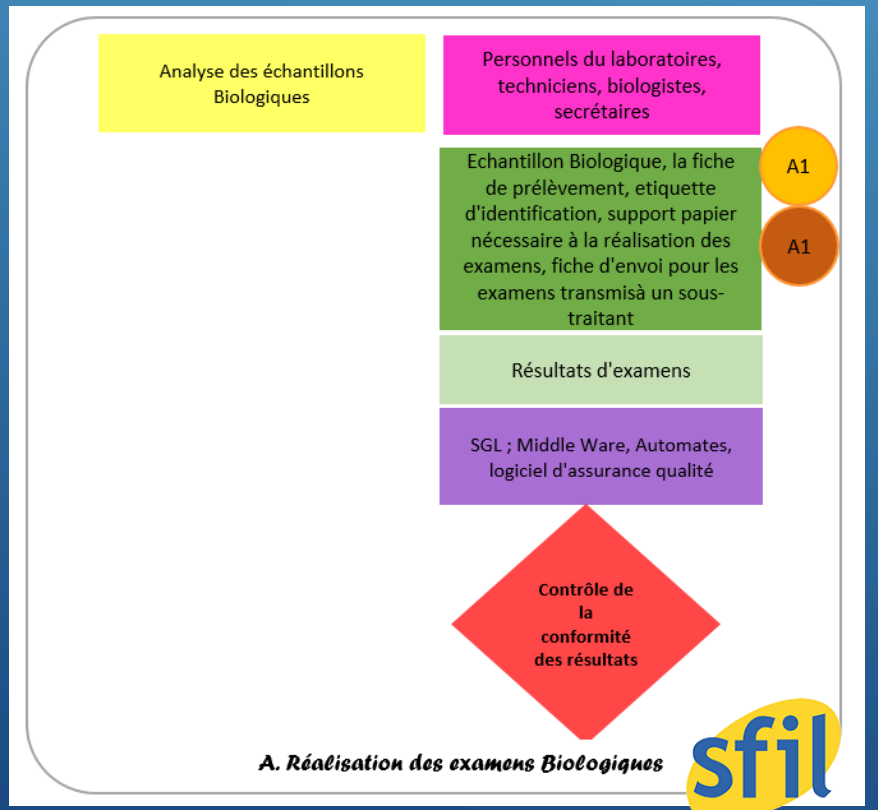
SYNDICAT DES BIOLOGISTES
Le syndicat de tous les biologistes médicaux

LA COTATION DU RISQUE

EXEMPLE

1 Contexte → Questionnaire : environ 300 questions → Quel(s) traitement(s) Justification / RGPD

- Hypothèse
  - Analytique – réalisation des examens biologiques
  - Traitement : Analyse des échantillons
  - Données concernées
    - Démographique de patients et acteurs de santé
    - Données de santé de patients



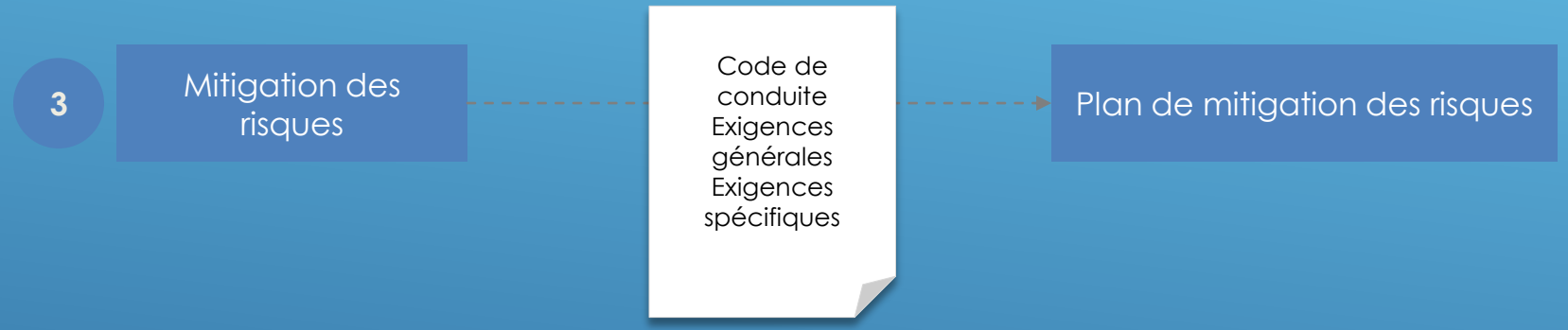
EXEMPLE

2 Identification des risques → Grille d'évaluation des risques → Niveau de Risque

- Risque identifié automatiquement

Evénements redoutés	Menaces	Scénario de menaces	Vraissemblance	Impacts vie privée		Impacts vie privée	NR
				Perte de chance	Moraux		
Divulgation de données	Erreur de transmission (Mauvais destinataire)	Un destinataire illégitime reçoit des données d'autres patients, suite à l'inscription d'une mauvaise adresse sur le courrier ou une inattention quand au bon choix du destinataire légitime, pour des personnes ayant un nom et un prénom identique.	4	1	2	2	8
Impossibilité de prendre en charge le patient	Suppression ou vol du document patient (Accès au support par une personne malveillante)	Une personne non habilitée et/ou malveillante peut accéder aux documents patients s'ils ne sont pas scellés ou que le local est en accès libre.	2	2	1	2	4

EXEMPLE



- Sélection des dispositifs à partir du code de conduite et des exigences

Evénements redoutés	Menaces	Scénario de menaces	Vraissemblance	Impacts vie privée		NR
				Perte de chance	Moraux	
Divulgation de données	Erreur de transmission (Mauvais destinataire)	Un destinataire illégitime reçoit des données d'autres patients, suite à l'inscription d'une mauvaise adresse sur le courrier ou une inattention quand au bon choix du destinataire légitime, pour des personnes ayant un nom et un prénom identique.	2	1	2	4
Impossibilité de prendre en charge le patient	Suppression ou vol du document patient (Accès au support par une personne malveillante)	Une personne non habilitée et/ou malveillante peut accéder aux documents patients s'ils ne sont pas scellés ou que le local est en accès libre.	1	2	1	2

www.sfil.asso.fr

rgpd@sfil.asso.fr

SFIL – LinkedIn