CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

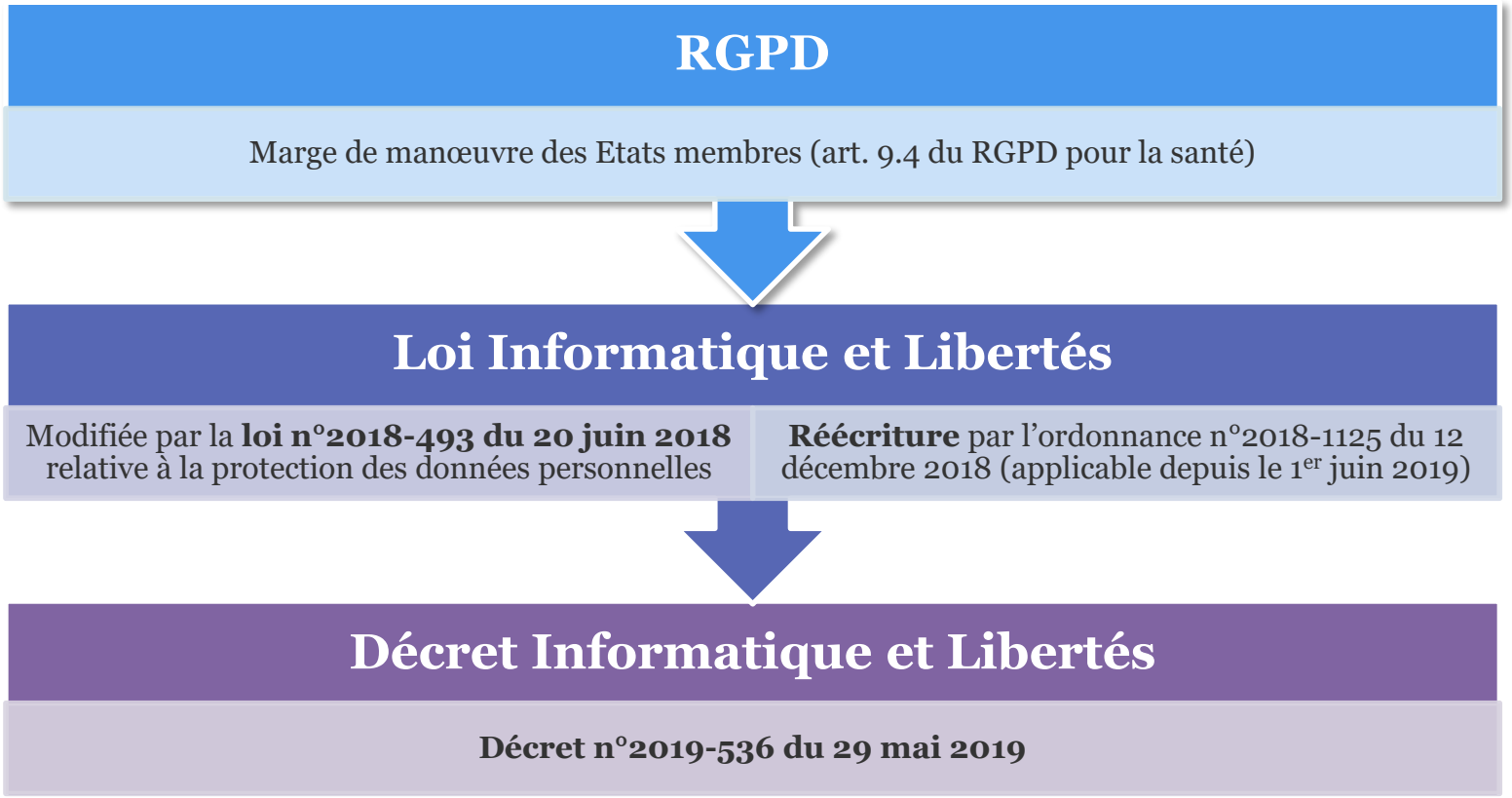
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Cadre légal de la protection des données de santé et le rôle du DPO

Axelle RACINOUX
Mathieu GINESTET

INTRODUCTION : CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES DE SANTÉ

Sur le traitement des données personnelles



Autres dispositions dans le domaine de la santé

- **Code de la santé publique :**

article L.1110-4 ; article L.1111-8 ; article L.1121-1 et suivants ; article L.1460-1 ;

- **Code de l'action sociale et des familles**

- **Code pénal** ;

- Règlement n°536/2014 du 16 avril 2014 sur **les essais cliniques de médicaments à usage humain** ;

- Règlement 217/745 du 5 avril 2017 relatif aux **dispositifs médicaux ;**

- **Etc.**

1. Rappel des grands principes de la protection des données à caractère personnel

1.1. Quand s'applique la réglementation relative à la protection des données ? – critère matériel

1.2. Quand s'applique la réglementation relative à la protection des données ? – critère géographique

1.3. En pratique : quels sont les principes à respecter ?

1.1. Quand s'applique la réglementation relative à la protection des données ? – critère matériel

- Tout organisme public ou privé
- Deux types d'acteurs :

Le responsable de traitement

décide des finalités et des moyens du traitement

Par exemples:

- Secteur privé : la société pharmaceutique représentée par son président
- Secteur public : l'hôpital représenté par son directeur

Le sous-traitant

Traite les données personnelles pour le compte du responsable de traitement

Par exemple:

- l'hébergeur de données de santé

1.1. Quand s'applique la réglementation relative à la protection des données ? – critère matériel

Traitement

Toute **opération** portant sur des données personnelles, **quel que soit le procédé utilisé.**

Par exemples :
- enregistrer,
- organiser,
- conserver,
- modifier,
- transmettre,
- etc.

Données à caractère personnel

Toute information se rapportant à une **personne physique identifiée** ou **identifiable** directement ou indirectement.

- **Directement identifiante**
- **Indirectement identifiante**
- **Recoupement d'informations**

Focus : Données « anonymes » et données « pseudonymisées »

L'**anonymisation** vise à rendre impossible l'identification de la personne concernée, de manière irréversible et quels que soient les moyens utilisés.

La **pseudonymisation** consiste à remplacer des informations directement identifiantes par des données indirectement identifiantes.

➔Les données « pseudonymisées » restent des données à caractère personnel.

1.2. Quand s'applique la réglementation relative à la protection des données ? – critère géographique

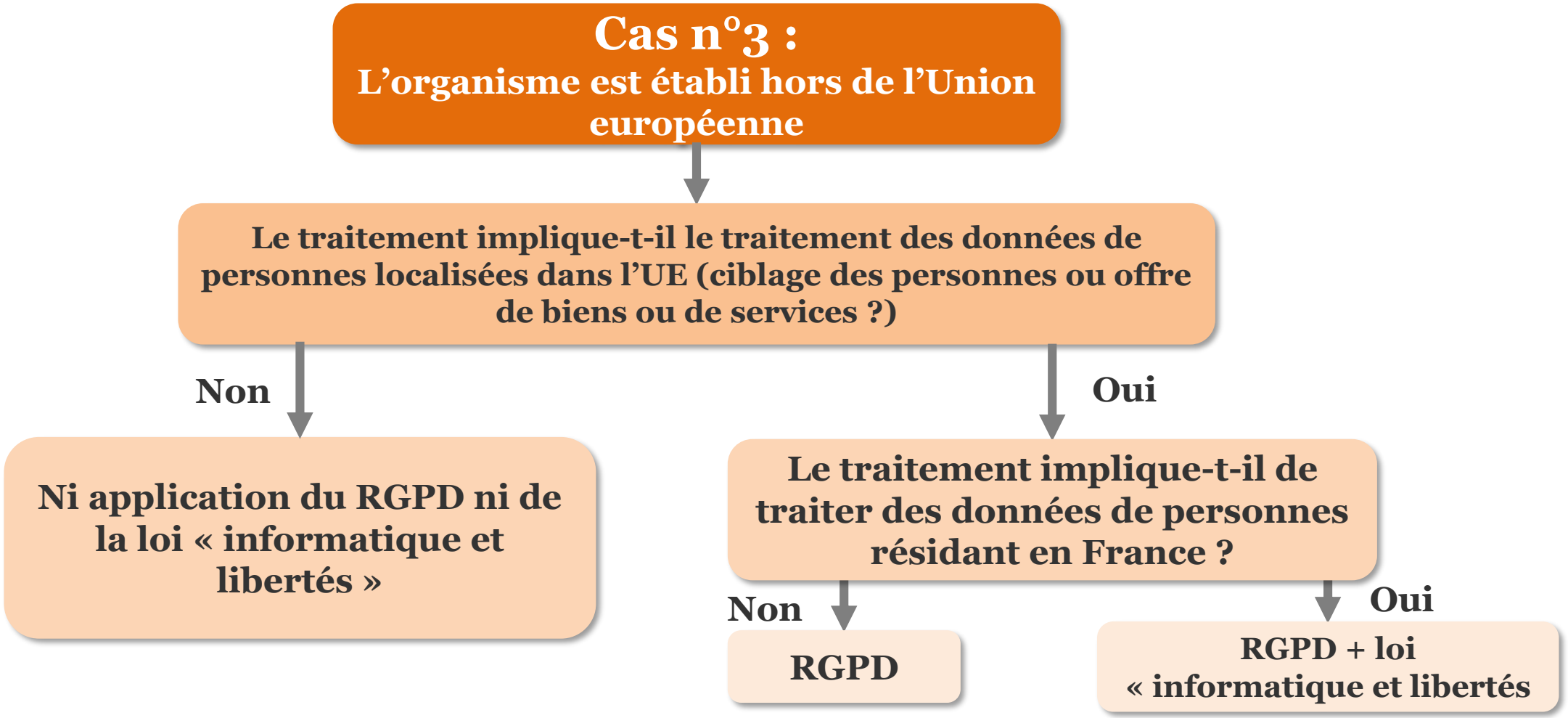
Cas n°1 :
L'organisme est établi en France

↓

Application du RGPD
+
Loi « Informatique et libertés »

1.2. Quand s'applique la réglementation relative à la protection des données ? – critère géographique

1.2. Quand s'applique la réglementation relative à la protection des données ? – critère géographique



1.3. En principe, quels sont les principes à respecter ?

01

Licéité, loyauté & transparence du traitement

Finalité déterminée, explicite et légitime

02

03

Minimisation des données

Exactitude des données collectées

04

05

Durée de conservation limitée

Intégrité
Confidentialité
Disponibilité

06

07

Respect des droits des personnes

Conformité

La logique de responsabilisation des acteurs

Allègement des obligations en matière de formalités préalables

Obligation pour le RT de garantir et démontrer à tout moment sa conformité au RGPD

<u>En pratique :</u>

- Mise en œuvre **d'outils pour s'assurer de la conformité** :
  - Tenue d'un registre des activités de traitement
  - Obligation de mener des analyses d'impact (AIPD) pour les traitements présentant un risque élevé
  - Mise en place de procédures en cas d'exercice des droits et violations de données
- **Nécessité pour chaque traitement :**
  - D'assurer l'effectivité de l'information à délivrer aux personnes et de leurs droits
  - D'encadrer les cas de sous-traitance ou de responsabilité conjointe
  - De mettre en place de mesures de sécurité appropriées
- **Désignation d'un acteur pour s'assurer de la conformité : le DPO (lorsque cela est obligatoire)**

2. Spécificité de la protection des données de santé

2.1. Le traitement des données de santé
2.2. Secret médical et échange et partage d'information
2.3. L'hébergement des données de santé

2.1. LE TRAITEMENT DES DONNÉES DE SANTÉ

2.1.1. Qu'est-ce qu'une donnée de santé ?

Article 4 du RGPD « *données relatives à la **santé physique ou mentale**, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne* »

3 catégories de données de santé

Par nature

Par exemple : scanner, tension artérielle, disagnostic)

Par combinaison

Par exemple : l'association du poids et de la taille d'une personne pour déduire l'IMC

Par destination

Par exemple : la photographie d'une personne intégrée à son dossier médical en vue de la réalisation d'un acte de chirurgie réparatrice

2.1.2. A quelles conditions peut-on utiliser des données de santé ?

Attention : à ne pas confondre avec la base légale (art. 6 du RGPD)

2.1.2. A quelles conditions peut-on utiliser des données de santé ?

Cas dans lesquels des données de santé peuvent être traitées

voir : article 9.1 du RGPD

- la personne concernée a donné son **consentement explicite**
- le traitement est nécessaire aux fins de **l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail**, de la sécurité sociale et de la protection sociale
- le traitement est nécessaire à la **sauvegarde des intérêts vitaux de la personne** concernée ou d'une autre personne
- le traitement est effectué, dans le cadre de leurs **activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif** et poursuivant une finalité politique, philosophique, religieuse ou syndicale
- Les données ont été **manifestement rendues publiques par la personne concernée**
- le traitement est **nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice**
- le traitement est nécessaire pour des **motifs d'intérêt public important**
- Le traitement est **nécessaire à la prise en charge médicale ou à la protection sociale**
- le traitement est nécessaire pour des **motifs d'intérêt public dans le domaine de la santé publique**
- le traitement est **nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique** ou historique ou à des fins statistiques

2.1.3. Dois-je réaliser des formalités préalablement au traitement ?

Traitements pour lesquels aucune formalité auprès de la CNIL n'est nécessaire

voir article 65 de la LIL

<u>Attention :</u>
Inscription au registre de traitement
+
AIPD (si obligatoire)

- traitements nécessaires aux fins de médecine préventive, de diagnostics médicaux, de l'administration des soins ou de la gestion de services de santé et mis en œuvre par un professionnel de santé ou une personne à laquelle s'impose l'obligation de secret professionnel ;
- traitements auxquels la personne concernée a donné son consentement explicite ;
- traitements nécessaires à la sauvegarde des intérêts vitaux de la personne, dans le cas où la personne concernée est dans l'incapacité physique ou juridique de donner son consentement ;
- traitements portant sur des données à caractère personnel manifestement rendues publiques par la personne concernée
- traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ou à chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle

2.1.3. Dois-je réaliser des formalités préalablement au traitement ?

Traitements pour lesquels aucune formalité auprès de la CNIL n'est nécessaire

voir article 65 de la LIL

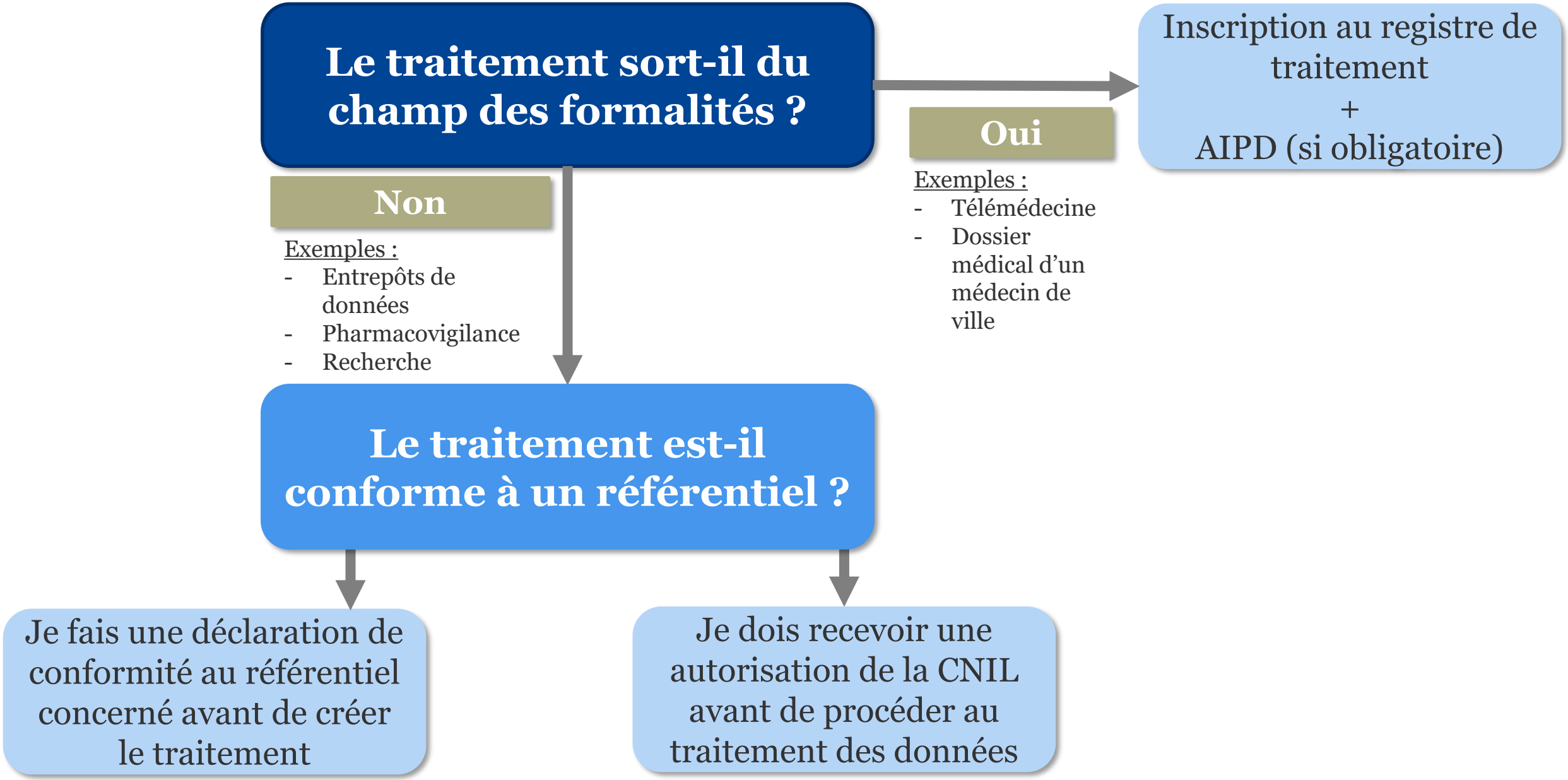
Attention :
Inscription au registre de traitement
+
AIPD (si obligatoire)

- traitements permettant d'effectuer des études dites « internes »à usage interne
- traitements mis en œuvre par les organismes chargés de la gestion d'un régime de base d'assurance maladie ainsi que la prise en charge des prestations par les organismes complémentaires d'assurance maladie (OCAM)
- traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale
- traitements effectués par les agences régionales de santé, par l'Etat et la personne publique désignée pour l'élaboration et la révision du projet régional de santé, la détermination des ressources, l'évaluation de la qualité des soins, la veille et la vigilance sanitaires, le contrôle de l'activité de soins et de la facturation des établissements de santé
- traitements mis en œuvre par l'Etat aux fins de conception, de suivi ou d'évaluation des politiques publiques dans le domaine de la santé ainsi que ceux réalisés aux fins de des statistiques dans ce domaine

2.1.3. Dois-je réaliser des formalités préalablement au traitement ?

Traitements pour lesquels une formalité auprès de la CNIL est nécessaire

- Les traitements qui ne sont pas exemptés de formalités
- Les traitements automatisés dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention


Le traitement sort-il du champ des formalités ?
Oui
Inscription au registre de traitement
+
AIPD (si obligatoire)
Exemples :
- Télémédecine
- Dossier médical d'un médecin de ville
Non
Exemples :
- Entrepôts de données
- Pharmacovigilance
- Recherche
Le traitement est-il conforme à un référentiel ?
Je fais une déclaration de conformité au référentiel concerné avant de créer le traitement
Je dois recevoir une autorisation de la CNIL avant de procéder au traitement des données

2.2. LE SECRET MÉDICAL ET L'ÉCHANGE ET LE PARTAGE D'INFORMATIONS

2.2.1. Le secret médical

« ***Toute personne prise en charge par un professionnel de santé***, *un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins […], le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social […]* ***a droit au respect de sa vie privée et du secret des informations la concernant***. » (article L.1110-4 du Code de la santé publique)

2.2.1. L'échange et le partage d'informations

- **Echange** : deux professionnels ou plus identifiés par le patient (nominativement ou a minima par leur fonction) se communiquent de l'information.

- **Partage** : l'information relative au patient est placée dans un dossier papier ou électronique pour être rendue disponible au profit de professionnels que le patient ne peut pas identifier a priori.

2.2.1. L'échange et le partage d'informations

	Au sein de l'équipe de soins	En dehors de l'équipe de soins
Echange de données de santé	Information + **Droit d'opposition**	Information + **Droit d'opposition**
Partage de données de santé	Information + **Droit d'opposition**	Information + **Consentement requis**

2.2.1. L'échange et le partage d'informations

L'outil informatique utilisé pour le partage ou l'échange de données doit répondre aux « grands » principes applicables aux traitements des données à caractère personnel, en particulier :

- Les informations de santé sont partagées ou échangées pour des finalités déterminées, explicites et légitimes
- Elles sont strictement nécessaires à l'organisation de la prise en charge
- Elles sont conservées pour une durée n'excédant pas celle nécessaire à l'échange ou au partage
- Les destinataires des informations doivent être des professionnels identifiés et habilités
- Une information claire doit être délivrée concernant les modalités d'échange et de partage des données et les modalités d'exercice des droits de l'usager
- L'outil informatique utilisé doit être conforme au niveau de sécurité

2.3. L'HÉBERGEMENT DE DONNÉES DE SANTÉ (HDS)

2.3.1. Qu'est-ce que l'hébergement de données de santé ?

L'hébergement est une prestation de dépôt, de conservation et de restitution de ces données, de manière à en assurer la disponibilité, l'intégrité et la confidentialité pour le compte de certains acteurs.

Dans le secteur de la santé, la réglementation impose dans certains cas, le recours à un prestataire spécifique : l'hébergeur de données de santé ayant obtenu une certification.

2.3.2. Quand dois-je recourir à un HDS ?

L'hébergeur de données que je sollicite doit-il certifié ?

Oui, si ces trois conditions cumulatives sont remplies

Je collecte des données de santé à caractère personnel identifiantes ou indirectement identifiantes

+

Les données de santé que je collecte sont recueillies à l'occasion d'une activité de prévention, de diagnostic, de soins ou de suivi social et médico-social

+

Les données de santé collectées sont stockées / conservées par un prestataire :
- pour mon compte en tant que personne morale
- pour mon compte en tant que personne physique
- pour mon compte en tant que patient

Non, si l'une des conditions suivantes est remplie

Aucune donnée de santé à caractère personnel directement ou indirectement identifiantes n'est collectée

OU

Les données de santé collectées ne sont pas recueillies à l'occasion d'une activité de prévention, de diagnostic, de soins ou de suivi social ou médical social

OU

Les données de santé collectées sont conservées par le responsable de traitement lui-même ou par le patient lui-même: l'hébergement n'est pas externalisé.

RÉFÉRENCES UTILES

Les sources d'informations disponibles

- **Site web de la CNIL - Fiches pratiques :**

➢ Thématique santé : données de santé, télémédecine, recherche, formalités …
➢ Rubrique ma conformité au RGPD : RGPD par ou commencer, etc.
➢ Rubrique besoin d'aide

- **Site web de la CNIL - Outils à disposition des acteurs :**

➢ Logiciel « Analyse d'impact », modèles d'AIPD, modèle de « registre d'activités de traitements », infographie, MOOC, etc.

- **Charte d'accompagnement des professionnels**

Les guides spécifiques

- **Les guides :**

➢ Référentiel des durées de conservation dans le domaine de la santé hors recherche
➢ Référentiel des durées de conservation dans le domaine de la recherche en santé
➢ Référentiel pour la gestion des traitements courants des cabinets médicaux et paramédicaux

➢ A venir : Référentiel pharmacies d'officine, référentiel opticien lunetier / audioprothésiste

➢ Guide sur les modalités de circulation du NIR pour la recherche en santé aux fins d'appariement de données avec le SNDS
➢ Guide pratique sur les durées de conservation
➢ Guide du sous-traitant
➢ Guide pratique sur les mesures de sécurité élémentaires à mettre en œuvre

Les référentiels spécifiques

- **Les référentiels relatifs à des traitements soumis à autorisation (déclaration de conformité) :**

➢ Référentiel pour la gestion des vigilances sanitaires
➢ Méthodologies de référence (recherche médicale - MR 001 à MR 006)
➢ Référentiel entrepôts de données de santé

➢ Mise à jour du référentiel (AU 41) relatif aux accès précoces et compassionnels
➢ Mise à jour des méthodologies de référence

Pour poser une question

Par téléphone au 01 53 73 22 22

Permanence juridique

- Du lundi au vendredi (sauf le mercredi)
- De 10h à 12h et de 14h à 16h

Permanence service santé

- Tous les lundi de 9h30 à 12h

Permanence DPO

- Du lundi au vendredi (sauf le mercredi)
- De 10h à 12h

Permanence service international

- Tous les mercredi
- De 14h à 16h