# Recap : Protection des données de santé

## 1. Définitions

★ Donnée à caractère personnel = Toute information relative à **une personne physique** identifiée ou qui peut être identifiée, directement ou indirectement avec un ou plusieurs éléments qui lui sont **propres**

→ **Ces informations médicales personnelles intéressent beaucoup de monde qu'elles doivent donc être protégées**

→ les ordonnances de 1996 précisent qu'en dehors des soignants, seuls les inspecteurs de l'action sanitaire et social et les médecins conseils ont accès au **secret médical**

★ Fichier : tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés

★ La notion de traitement (Article 2) c'est des opérations ou un ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé…

★ Le ttt informatique = **centralise** et **interconnecte** les données, **augmentant leur puissance** et **leur exploitation**, mais aussi les **risques en cas de faille de sécurité**

Responsable : Il définit les **objectifs** et les **moyens** du traitement des données

→ **QUI ?** une personne, une autorité publique ou un organisme

→ **OÙ ?** en France ou utilise des moyens de traitement en France

Destinataire : Il reçoit les données pour les traiter, mais ce n'est **ni la personne concernée ni le responsable**

→ **QUI ?** On ne peut pas être à la fois responsable et destinataire. *Par exemple, un auteur d'article n'est pas destinataire, mais ses lecteurs le sont.* Les autorités exerçant un droit de communication ne sont pas des destinataires

★ Données médicales = toutes les données à **caractère personnel** relatives à la **santé** d'une personne

→Elle se réfère également aux **données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques**

★ Données de santé = *comme les données relatives aux origines raciales, à l'opinion politique, à la vie sexuelle*, sont des données sensibles dont le **traitement est en principe interdit** (***Article 8***)

→ Des **dérogations** sont prévues par la loi (**Art 8. II**)

## 2. Cadre légal

★ **Cadre légal FRANÇAIS :**

★ **Loi du 6/01/78 = Loi Informatique, Fichiers et Libertés (IFL)**

→ Institution de la **CNIL** = Autorité administrative **indépendante**

→ a subi plusieurs modifications mais seule la **modification de 2004** est **importante** = *droits de la personne renforcés, allègement des formalités déclaratives auprès de la* CNIL, *contraintes nouvelles pour les transferts de données hors UE, nouveaux pouvoirs de la* CNIL : *sanctions et labellisation, institution du « correspondant* CNIL »

★ **Textes : *Code de déontologie* = *Article 4* ; *Code pénal* = *Article 226-13* ; *Code de la santé publique***

A *bien différencier* +

★ **Cadre légal EUROPÉEN :**

★ **Directive du 24/10/95** : vise à réduire les divergences entre législations nationales sur la protection des données personnelles au sein de l'Europe.

★ **Règlement de la protection des Données (RGPD) du 25 mai 2018**

## 3. La loi IFL

★ **Les 5 points clés de la loi IFL**

★ **Finalité**

→ Les données sont recueillies dans un **but précis, préalablement défini.**

★ **Proportionnalité et pertinence**

→ Seules les informations **pertinentes et nécessaires** au regard des objectifs sont utilisés

★ **Durée de conservation**

→ Pas de conservation **indéfinie** des informations personnelles

★ **Sécurité**

→ **Prendre les** mesures nécessaires pour garantir la sécurité des données

★ **Droit des personnes**

→ Information, accès, rectification, suppression et opposition / consentement sur leurs **données**

★ **Principes**

★ **Protection :** Confidentialité, Intégrité, Disponibilité

★ **Déclaration** : Avec la **Loi IFL,** tout fichier informatisé nominatif de façon directe ou indirecte doit être déclaré à la **CNIL** +++

→ Le déclarant doit spécifier : **objectifs** de la banque de données, organisme de **conservation,** organisme de **production** (*qui contrôle le droit d'accès*), catégories d'informations traitées et les différents utilisateurs

→On y différencie 2 types de déclarations ; les **déclarations normales** et les **déclarations simplifiées**

★ **Finalité** : (*Article* 6-2) Elle doit être **déterminée**, **explicite, légitime**

→ Si détournement de finalité : des sanctions pénales existent

★ **Protection :** Le **responsable du traitement** doit assurer la **sécurité des données** en empêchant leur **altération**, leur **détérioration** ou **tout accès non autorisé** (Article 34)

→ Il est tenu de respecter leur intégrité et leur confidentialité

★ **Droit des personnes :**

**I. DROIT À L'INFORMATION PRÉALABLE ET CONSENTEMENT ÉCLAIRÉ | II. DROIT DE CURIOSITÉ | III. DROIT D'ACCÈS DIRECT ET INDIRECT | IV. DROIT DE RECTIFICATION | V. DROIT À L'OUBLI ++**

→ **Droit à l'oubli** = Une durée de conservation **limitée** en adéquation avec la **finalité** poursuivie par le traitement (*Article 6-5*)

## 4. Accès au dossier médical

★ **Mesures de protection**

★ **Propriété du dossier :** Le dossier appartient au patient (loi du 4 mars 2002 dite Kouchner)

→ Le médecin et l'établissement sont co-propriétaires du dossier médical.

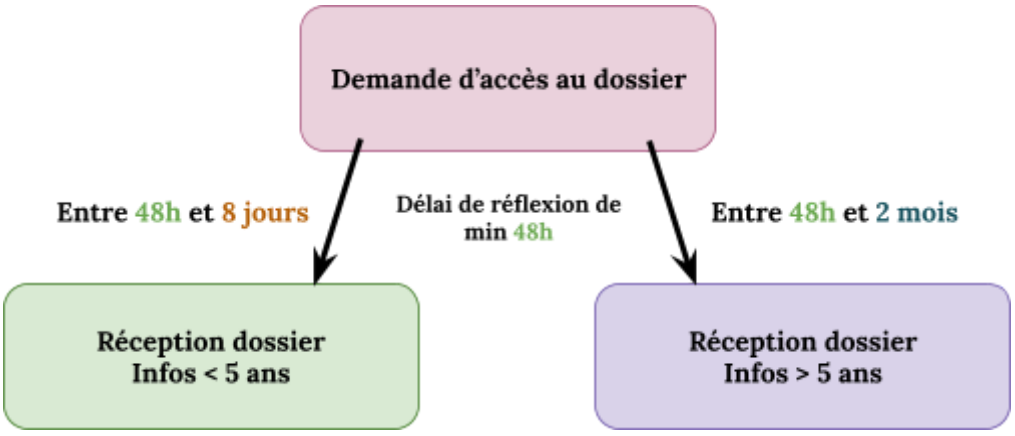
→ Le médecin et l'établissement qui établissent et conservent le dossier en sont les dépositaires

★ **Accès au dossier :**

→ Les personnes suivantes ont accès au dossier (les informations du dossier) :

**Le patient lui-même** (loi du 4 mars 2002 +++) ; La personne de confiance ; Les ayants droits d'un patient décédé sous certaines conditions ; Le médecin libéral et les médecins du service public hospitalier qui soignent le malade (en continuité des soins)

→ (Loi 4/03/2002) Pose le principe d'accès direct du patient à l'ensemble des informations de santé le concernant repris dans **l'article 43 de la loi IFL.**




★ **Communication des données :** Seules sont **communicables** les informations recueillies lors des consultations, admissions et séjours hospitaliers, ainsi que celles établies en fin de séjour.

*Les informations provenant de tiers extérieurs à la prise en charge ne le sont pas.*

## 5. Autres dispositions

★ **Le CIL**

→ Le correspondant tient un registre des traitements de l'organisme
→ Il assure localement et de manière **indépendante**, une meilleure application de la loi et ainsi diffuse la culture informatique et libertés. ++
→ Il permet de disposer de **relations privilégiées** avec la CNIL : service dédié, information ciblée et adaptée. ++

→ **Le CIL a un rôle de : Conseil, Recommandation, Médiation, Alerte, Information**

## 6. Récap et évolutions

★ **Code de la santé publique**

→ Obligation de **confidentialité des données médicales**
→ Droit d'être **informé**
→ Droit d'**accéder aux informations**
→ Obligation d'assurer la **sécurité du stockage des données**

★ **COMPLÉTÉ 7.10.2016 (RÉPUBLIQUE NUMÉRIQUE)**

→ **Droit à l'oubli** pour les mineurs,
→ **Mort numérique** : directives de la personne sur ses données et droits des héritiers,
→ **Portabilité des données**,
→ En cas de violation des données, obligation d'information des personnes concernées,
→ **Montant maximal des sanctions porté à 3 millions d'euros**.

★ **CHAPITRE IX DE LA LOI IFL**

→ S'applique aux recherches en santé, en complément de la loi Jardé.
→ Distingue les recherches impliquant la personne humaine et celles reposant uniquement sur la réutilisation de données de santé
→Ces traitements de données nécessitent une **autorisation de la CNIL**

**LES NOUVEAUTÉS RGPD (2018)**

→ Formalités allégées –> Accountability
→ Désignation d'un délégué à la protection des données pour certaines entreprises
→ Garantir la protection des données par défaut ou dès la conception
→ Étude d'impact sur la vie privée
→ Signalement des violations de données

**Attention** : Même avec la mise en œuvre du RGPD, il faut toujours déclarer !

**RGPD**

En cas de violation de données, il y a obligation de la personne concernée
➔ Il n'y a aucune nuance entre le RGPD et la loi du 7 octobre 2016 puisque le RGPD prévaut comme il est plus récent *(confirmé par le prof)*