Santé Publique

PROTECTION DES DONNÉES DE SANTÉ

PLAN

I) Concepts et champs d'application
II) Cadre légal
III) Principes de la loi IFL
IV) Accès au dossier médical
V) Autres dispositions
VI) Récapitulatif et évolution

I) CONCEPTS ET CHAMPS D'APPLICATION

1. Données à caractère personnel

↳ La notion de donnée à **caractère personnel** : *(Article 2 de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995)*

- Toute information relative à une **personne** physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
- Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

➔ Toute information relative à une personne identifiée ou susceptible de l'être

Exemples : numéro de sécurité sociale, numéro d'ordre renvoyant à une liste nominative même établie sur papier, prélèvement biologique identifiant, identification par recoupement

2. Utilisation des données

→ Ces **informations médicales personnelles** sont une **ressource essentielle** dans les domaines de l'épidémiologie, de la maîtrise des dépenses de santé, du commerce et des assurances.
➔ C'est parce qu'elle intéressent beaucoup de monde qu'elles doivent être **protégées**

→ Les épidémiologistes par exemple font des études pour l'intérêt de l'ensemble de la population, mais ils n'ont pas de malades et n'ont donc pas à savoir qui est qui ➔ c'est le principe du **secret médical**.

Ce **secret médical** peut être **partagé**, mais se pose alors la question de savoir avec qui.
Ce sont les **ordonnances de 1996** qui précisent qu'en dehors des soignants, ont accès au secret médical les inspecteurs de l'action sanitaire et social et les médecins conseils

3. Traitement des données

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

↳ **Notion de traitement** : *(Article 2)* Opération ou ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction

Exemples : Constitution de fichiers, de bases, toute procédure, de télétransmissions d'informations quel que soit le moyen de télécommunications (réseaux, cartes Vitale, Internet...)

↳ Traitement informatique

- **Catégorisation**
- **Concentration des données** plus importante
  si défaillance de la protection = danger +++ car accès à toutes les informations en même temps
- **Puissance** du traitement
- **Identification des personnes** par recoupement
- **Interconnexion et dispersion**
  Une donnée isolée est potentialisée si relation possible avec d'autres informations
- **Portabilité et appropriation**

4. Responsable et destinataire

Responsable *Article 3-I*

- La personne, l'autorité publique, le service ou l'organisme qui détermine les **finalités** et les **moyens nécessaires** à sa **mise en œuvre**, sauf désignation expresse par les dispositions législatives ou réglementaires.
- **Où ?** Établi sur le **territoire français** (installation stable, quelle que soit sa forme juridique, filiale, succursale...) ou recours à des moyens de traitement situés en zone française

Destinataire *Article 3-II*

- Toute personne **habilitée** à recevoir **communication des données** autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données.
  Astuce : *On ne peut pas être responsable et destinataire à la fois, par exemple, vous écrivez une article, vous êtes au courant du contenu de l'article ainsi que vos collaborateurs, vous n'êtes donc pas des destinataires. Lorsque l'article sera publié, les lecteurs seront des destinataires*
- Les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication ne constituent pas des destinataire

5. Données médicales

→ L'expression « **données médicales** » se réfère à 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**.

Annexe de la recommandation R (97) 5 du 13 février 1997 relative à la protection des données médicales, Conseil de l'Europe

6. Données de santé

→ Les **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 *(Art 8. II)* :

- consentement exprès des personnes sauf disposition contraire
- les traitements nécessaires aux fins de médecine préventive, des diagnostics, de l'administration de soins ou de traitements ou de la gestion de services de santé et mis en œuvre par un professionnel de santé ou par une personne tenue au secret
- les traitements de données de santé à des fins de recherche médicale
- les traitements de données sensibles susceptibles de faire l'objet à bref délai d'un procédé d'anonymisation reconnu conforme par la CNIL
- les traitements de données sensibles, justifiés par l'intérêt public et autorisé par la CNIL ou par décret en CE pris après avis de la CNIL, …

II) CADRE LÉGAL

1. En France

Loi du 6 janvier 1978 dite loi IFL

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

→ **Loi du 6/01/78** : loi **Informatique, Fichiers et Libertés** (IFL), relative au développement, à l'utilisation et la protection des **fichiers informatiques** et **manuels** +++

➔ Institution de la **CNIL** par cette loi (Commission Nationale Informatique et Libertés) : +++

- Autorité administrative **indépendante** ++ chargée de veiller au respect de la loi
- Protège la vie privée et les libertés individuelles ou publiques

→ Cette loi a subi plusieurs modifications : *(seule la modification de **2004** semble importante)*

Modification en 92	*Dispositions pénales*
Modification en 94	*Traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé*
Modification en 99	*Traitements des données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins ou de prévention*

Modification en 2000	*Collecte, enregistrement et conservation des informations nominatives*
Modification en 2004	▪ 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 » (le **CIL** : correspondant Informatique et Libertés) +++

→ Textes :

- Code de déontologie = *Article 4*
- Code pénal = *Article 226-13*
- Code de la santé publique ♥

2. En Europe

- *Recommandations du conseil de l'Europe du 3/01/81 relatives aux banques de données médicales automatisées*
- *Directive du 24/10/95 : vise à réduire les divergences entre législations nationales sur la protection des données personnelles au sein de l'Europe*

III) PRINCIPES DE LA LOI IFL

A. Protection des données

❖ La confidentialité des informations

Seuls les utilisateurs habilités dans les conditions normalement prévues doivent avoir **accès** aux informations.

❖ L'intégrité des informations

Les informations ne sont **modifiables** que par les utilisateurs habilités dans les conditions d'accès normalement prévues.

❖ La disponibilité des informations

Les informations peuvent en permanence être **employées** par les utilisateurs habilités dans les conditions d'accès et d'usage normalement prévues

B. Déclaration

→ Avec la **loi du 6/01/78** (IFL), tout fichier informatisé nominatif de façon directe ou indirecte doit être déclaré à la **CNIL** +++

→ Le **déclarant** doit spécifier : +++

- les objectifs de la banque de données,
- l'organisme qui conserve,
- l'organisme qui produit les données et contrôle le droit d'accès,
- les catégories d'informations traitées et les différents utilisateurs, …

1. Déclaration normale

→ Contenu de la **déclaration** : *(Article 30)*

L'identité du responsable, la ou les finalités du traitement, les interconnexions éventuelles, les données traitées, leur origine, les catégories de personnes concernées,la durée de conservation, le ou les services chargés de mise en œuvre, les destinataires des données, le service auprès duquel s'exerce le droit d'accès, les dispositions prises pour assurer la sécurité des données, le cas échéant, les transferts de données vers un État non membre de la Communauté européenne

↳ Description des mesures

Des **mesures obligatoires** de protection des **fichiers informatiques** en découlent :

- **Identification et authentification** des utilisateurs
- Définition des **droits d'accès et d'utilisation**
- **Encryptage**
- Surveillance des **connexions**
- **Protection** des fichiers
- **Sauvegarde**
- **Sécurité** contre les virus et le piratage
- **Alimentation électrique** constante et protégée, …

2. Déclaration simplifiée *(Article 24)*

→ La **CNIL** peut adopter des **normes simplifiées** pour les traitements les plus **courants** dont la mise en œuvre n'est pas susceptible de porter atteinte à la **vie privée** ou aux **libertés**

- Il existe aujourd'hui 54 normes (les normes sont sur le site de la CNIL) : *gestion de cabinets médicaux et paramédicaux (n°50), gestion des pharmacies (n°52), gestions des LABM (n°53), gestion des centres d'optique (n°54), gestion du personnel (n°46), contrôle d'accès (n°42), gestion des membres des associations (n°23), utilisation de services de téléphonie fixe et mobile sur les lieux de travail (n°47), …*
- Si le traitement envisagé correspond en tous points à une **norme**, un **engagement de conformité** suffit

C. Finalité

→ Une **finalité** : *(Article 6-2)*

- **déterminée**
- **explicite**
- **légitime**, correspondant aux **missions** de l'organisme

→ Les données traitées doivent être **adéquates**, **pertinentes** et **non excessives** par rapport aux finalités pour lesquelles elles sont collectées *(Article 6-3°)*

→ Tout **détournement de finalité** est passible de **sanctions pénales** *(Article 226-21 code pénal)* : 5 ans d'emprisonnement, 300 000 euros d'amende *(retenez qu'on peut être sanctionné)*

Exemples : Les fichiers obligatoires (publics) ne peuvent être utilisés à des fins politiques ou commerciales / zones commentaires (« timide, menteur », …), fichiers bancaires, …

D. Obligation de sécurité

→ Il appartient au **responsable du traitement** de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la **sécurité des données** et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès *(Article 34 de la loi modifiée)*

→ **Respect de l'intégrité et de la confidentialité des données** : empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès

➔ Une **obligation** qui pèse sur le **responsable du traitement** +++

→ Les mesures de **sécurité physique et logique** doivent être adaptées à la nature des données et aux risques présentés par le traitement *(ex: chiffrement des données sur Internet)* :

Identification	→ Processus par lequel une « entité » informe le système distant de son identité → Généralement l'identifiant se compose du nom de l'utilisateur, ou d'un numéro d'utilisateur, ou de tout autre identifiant qui permet au système de savoir avec « qui » il va entrer en communication *(ex : login / carte à puce, carte vitale*
Authentification	→ Élément qui caractérise une personne ou une « entité » et autorise l'accès au système *(ex : mot de passe, emprunte digitale, …)* → L'authentification est un **outil essentiel de la confidentialité** : celui qui accède à une donnée est bien celui qui est autorisé à le faire
Gestion des accès	Tableau des habilitations
Précautions élémentaires	▪ L'accès à l'application doit être protégé par des mots de passe individuels, alphanumérique d'une longueur de 6/7 caractères au moins. Évitez les mots de passe trop courants (évitez initiales, nom, prénom, SESAM etc.). Changez les régulièrement ▪ Éteindre le PC en cas d'absence, déconnexion automatique, écran de veille protégé par un mot de passe ▪ En cas de connexion à l'Internet : antivirus ; « pare-feu » (firewall) / séparation physique des réseaux ▪ Effectuez régulièrement des sauvegardes (CD-Rom, disquettes) et conservez-les dans un lieu différent de la base de données ▪ Lors de la numérisation et de la compression des images (imagerie médicale), utilisation de procédures normalisées permettent de garantir l'intégrité de ces données. ▪ Lorsque des données de santé sont transférées via Internet, il convient de recourir à un dispositif de chiffrement de la communication (ex.: chiffrement SSL avec une clef de 128 bits, messagerie sécurisée...) ▪ Mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises. ▪ Pour les applications en réseau : ➢ Par-feu (firewall) ➢ Maintenance des matériels : ne pas laisser emporter le disque dur si les données sont en « clair » ➢ Limiter à tout prix le nombre d'informaticiens ayant le profil « super-utilisateur » ou « administrateur système » ➢ En fonction des données traitées, traçabilité, journalisation des connexions

E. Les droits des personnes

- Droit à **l'information préalable et consentement éclairé**
- Droit de **curiosité**
- Droit **d'accès direct et indirect**
- Droit de **rectification**
- Droit à **l'oubli**

Droit à l'information

Article 32

L'Information
➔ Délivrée pour un **consentement éclairé**

Le **droit d'être informé** : +++

- de l'identité du **responsable**
- de la **finalité** poursuivie par le traitement
- du **caractère obligatoire ou facultatif** des réponses, des conséquences à leur égard d'un défaut de réponse
- des **destinataires** des données
- de l'existence d'un **droit de s'opposer** pour des raisons légitime au traitement, un **droit d'accès** et de **rectification**
- et le cas échéant, des **transferts** à destination d'un État non-membre de la Communauté européenne

↳ ***Modalités d'information***

- *Affichettes dans les **établissements de santé**, à l'accueil des caisses,*
- *Note d'information sur le site web de l'organisme,*
- *Lettre de présentation de l'étude, …*

Droit d'opposition

- Pour des raisons légitimes (art. 38), sauf si le traitement répond à une obligation légale
- Discrétionnaire en matière de recherche médicale (art. 56) et d'utilisation des données à des fins de prospection commerciale

Droit de rectification

Article 40

Droit à l'oubli

→ Une durée de conservation **limitée** en adéquation avec la **finalité** poursuivie par le traitement *(Article 6-5)*

→ La durée de conservation doit être **mentionnée** dans le dossier de formalité et limitée

→ **Distinction** entre la conservation en ligne des données et l'archivage

→ Au-delà de cette durée les données ne peuvent être conservées qu'en vue de leur traitement à des fins historiques, statistiques ou scientifiques *(Article 36)*
Les traitements des archives publiques sont dispensés des formalités préalables

IV) ACCÈS AU DOSSIER MÉDICAL

1. Mesures de protection

- Protection des **données médicales**
  Ex : suppression des feuilles de température et des prescriptions au lit du malade, …
- Mesures de protection des **informations nominatives** au niveau du circuit et du stockage du dossier médical
  Ex : suppression des éléments nominatifs ou distinctifs
- Procédures de **destruction** des documents nominatifs

2. Propriété du dossier

- Le **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

3. Accès au dossier

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

- Le **patient lui-même** : avec la **loi du 4 mars 2002** qui garantit l'accès direct du patient à son dossier médical +++
- La **personne de confiance** (parent, proche, médecin, …)
- Les **ayants-droits** d'un patient décédé sous certaines conditions
- Le **médecin** libéral et les **médecins du service public hospitalier** qui soignent le malade (continuité des soins)

Attention :

En fait comme accès au dossier = accès aux informations du dossier, le Pr. Staccini ne fait pas la distinction entre l'accès au dossier en lui-même et les informations, retenez donc les deux versions (en éthique, la personne de confiance ou les ayants-droits n'ont pas accès au dossier mais plutôt aux informations) mais gardez en tête que cela relève plus du Pr. Quatrehomme que Staccini !

→ La loi du **4 mars 2002** a posé le **principe de l'accès direct du patient** à l'ensemble des informations de santé le concernant, ce principe a été repris dans l'article 43 de la loi « informatique et libertés ». Le décret du 29 avril 2002 a organisé cet accès.

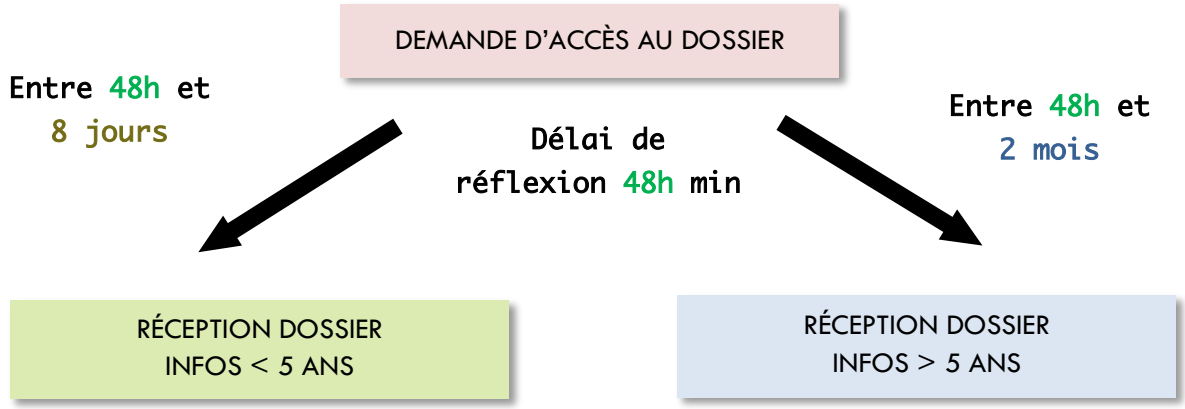
- Délai de communication entre **48h** et **8 jours**
- Si les données remontent à **plus de cinq ans**, le délai est **porté à deux mois**

→ La présence d'une **tierce personne** peut être recommandée.

→ **L'accès aux données** se fait, au choix du demandeur :

- soit par **consultation** sur place,
- soit par **l'envoi des documents**.
  ➔ Les frais de délivrance de ces copies ne sauraient excéder le coût de la reproduction et, le cas échéant, de l'envoi des documents

Schéma :



(Schéma récap fait par mes soins dans la ronéo 2 sur le Dossier médical*)*

4. Communication des données

→ Ce dossier contient au moins les éléments suivants, ainsi classés :

1. Informations **formalisées recueillies** lors des consultations externes dispensées dans l'établissement, lors de l'accueil au service des urgences ou au moment de l'admission et au cours du séjour hospitalier
2. Informations **formalisées établies à la fin du séjour**
3. Informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant de tels tiers

➔ Seules sont **communicables** les informations énumérées au 1 et au 2

V) AUTRES DISPOSITIONS

Le CIL

→ Défini depuis la refonte de la loi du 6 janvier 1978 en 2004 : CIL (Correspondant Informatique et Libertés) +++

→ Sa nomination permet un **allègement des formalités** : dispense de déclaration des traitements :

- sauf les traitements relevant du régime de l'autorisation ou de la demande d'avis
- sauf lorsqu'il existe un transfert de données à destination d'un État non membre de la Communauté européenne

➔ La désignation est **facultative** et **ouverte à tout responsable de traitement**

→ Le correspondant est chargé d'inscrire sur le registre qu'il tient à jour les traitements mis en œuvre par l'organisme

→ Assure localement et de manière **indépendante**, une meilleure application de la loi et ainsi diffuse la culture informatique et libertés ++

→ Permet de disposer de **relations privilégiées** avec la CNIL : service dédié, information ciblée et adaptée +++

Le CIL a un rôle de : +++

- **Conseil** : il est saisi pour avis avant la mise en œuvre de tout nouveau traitement, prépare les dossiers de formalités pour les traitements à risque
- **Recommandation** : il traduit les termes de la loi en règles internes ou codes de conduite propres au secteur d'activité
- **Médiation** : il reçoit les plaintes et requêtes des personnes concernées par les traitements (droit d'accès notamment)
- **Alerte** : il informe le responsable de traitement des manquements constatés
- **Information** : il dresse un bilan annuel qui est le reflet de son action (traitements examinés, recommandations émises, …

Attention : *Le CIL ne sanctionne pas +++*

VI) RÉCAPITULATIF ET ÉVOLUTION

❖ 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**

❖ Les 5 points clés de la loi IFL

1) Finalité

Les données sont recueillies pour un **but précis, préalablement défini**

3) Durée de conservation

Pas de conservation **indéfinie** des informations personnelles

2) Proportionnalité et pertinence

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

4) Sécurité

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

5) Droits des personnes

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

❖ Complété le 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

→ Désormais applicable en matière de **recherche, d'étude ou d'évaluation** dans le domaine de la santé (en complément de la loi Jardé) ++

→ 2 grandes **catégories de recherches** : +++

- d'une part, les recherches **impliquant** la personne humaine
- d'autre part, les recherches, études et évaluations **n'impliquant pas** la personne humaine

→ Sont en particulier visées les recherches nécessitant exclusivement la **réutilisation de données de santé à caractère personnel** (par exemple celles issues de dossiers médicaux, de cohortes existantes ou du SNDS).

➔ Les traitements de **données à caractère personnel** ayant pour **finalité** ces recherches sont soumis à **l'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**

Documentation prouvant la démarche : Data Protection Officier (DPO), Privacy by design, default, Privacy Impact Assessment (PIA), en cas de risques pour les personnes

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)*

Voilà pour votre dernière fiche de SP aux couleurs de Nissa la bella ! Ce cours paraît indigeste surtout vers la fin, c'était pas mon préféré mais il reste plus abordable que les ronéos de philo je pense mdrr, mais ne négligez rien dans votre TC ! Bon confinement et je vous dis à bientôt pour les fiches récap ! La SP vous love !

PS. On n'est pas en fac de droit, donc n'apprenez surtout pas le nom des articles sauf si vous aimez vous la péter ou étaler votre culture !