PROTECTION DES DONNES DE SANTE

I. Concepts et champs d'application

- ### Données à caractère personnel

Il s'agit de « **toute information concernant une personne physique identifiée ou identifiable** : est réputée identifiable, une personne **qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.** »

Article 2 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

La notion de donnée à caractère personnel (article 2)

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

- ### Utilisation des données

Ces informations médicales personnelles sont une **ressource essentielle dans les domaines de l'épidémiologie, de la maitrise des dépenses de santé, du commerce et des assurances**. C'est parce **qu'elles 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 dernier 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.**

- ### Traitement des données

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

La 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, carte vitale, internet…)*

Traitement informatique :

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

- ## Responsable des données

La notion de responsable (article 3-I) :

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

- ## Destinataires des données

La notion de 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.**
- **Les autorités légalement habilitées**, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication **ne constituent pas des destinataires.**

- ## 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.

- ## Données de santé

L'article 8 **: 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**.

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

- ## En France

Loi du 6/01/78 : loi informatique, fichiers et libertés, 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**

Modification en 92 : dispositions pénales
Modifications 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)

Code de déontologie médicale = article 4

Code pénal = article 226-13

Code de la santé publique

- **En Europe**

Recommandations du conseil de l'Europe du 3/01/81 relatives aux banques de données médicales automatisées

Directives 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

- **Protection des données**

La confidentialité des informations : sels 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.

- **Déclaration**

Avec la loi du 6/01/78, 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…

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 Etat non membre de la communauté européenne.

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…

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** (…)
- **Si le traitement envisagé correspond en tous points à une norme, un engagement de conformité suffit**

• La finalité

Une finalité déterminée, explicite et légitime correspond aux missions de l'organisme (art 6-2°).

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

Tout détournement de finalité est passible de sanctions pénales (art 226-32 c.pénal). 5 ans d'emprisonnement, 300 000 euros d'amende.

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

• L'obligation de sécurité

Article 34 de la loi modifiée : 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.

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)

L'identification : processus par lequel une « entité » informe le système distant de son identité

- Nom d'utilisateur, ou numéro d'utilisateur, ou de tout autre identifiant qui permet au système de savoir avec « qui » il va entrer en communication (login / carte à puce, carte vitale)

L'authentification : élément qui caractérise une personne ou une « entité » et autorise l'accès au système (mot de passe, empreinte 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 d'accès, tableau des habilitations.

Quelques précautions élémentaires s'imposent :

- **L'accès à l'application doit être protégé par des mots de passe** individuels, alphanumérique d'une longueur de 6/7 caractères au moins. Evitez les mots de passe trop courants (initiales, nom, prénom, SESAM…)
- **Eteindre le PC en cas d'absence**, déconnexion automatique, écran de veille protégé par un mot de passe
- En cas de connexion à Internet : **antivirus**, **pare-feu** (firewall) / séparation physique des réseaux

Effectuez régulièrement des sauvegardes 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 :

- Pare-feu
- **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

• 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**

Le droit d'être informé (article 32) :

- **L'identité de 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 Etat non membre de la communauté européenne**.

Le droit à l'oubli :

- Une **durée de conservation limitée** en adéquation avec la finalité poursuivie par le traitement (art 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** (art36)
- **Les traitements des archives publiques sont dispensés des formalités préalables**

IV. Accès au dossier médical

• 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

• Propriété du dossier

Le patient (loi du 4/3/2)

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

Le **patient** lui-même : avec la loi du 4/3/2 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.**

La loi du 4/3/2 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 la communication entre 48h et 8 j. Si les données remontent à plus de 5 ans, le délai est porté à 2 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.

• Communication des données

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

- 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 de séjour hospitalier.
- Informations formalisées établies à la fin du séjour
- 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 2°

V. Autres dispositions

• CIL

Défini **depuis la refonte de la loi du 6 janvier 1978 en 2004** : 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 Etat 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 ciblées et adaptée.

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 de manquements constatés.

Information : il dresse un bilan annuel qui est le reflet de son action (traitements examinés, recommandations émises…)

VI. Récapitulatif et évolution

- **Code de la santé publique**

- Obligation de confidentialité des données médicales
- Droit d'être informé
- Droit d'accéder aux données
- Obligation d'assurer la sécurité des données

- **Les 5 points clé de la loi IFL**

- **FINALITE :** les données personnelles sont recueillies pour un but précis, préalablement défini

- **PROPORTIONALITE & PERTINENCE :** Seules les informations pertinentes et nécessaires au regard des objectifs sont utilisées

- **DUREE DE CONSERVATION :** Pas de conservation indéfinie des informations personnelles

- **SECURITE :** Prendre des mesures nécessaires pour garantir la sécurité des données

- **DROIT DES PERSONNES :** Information, accès, rectification, suppression et opposition/consentement sur leurs données

- **Complété le 7.10.2016**

  ✓ 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 de la personne concernée
  ✓ Montant maximal des sanctions porté à 3millions 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 :

- Les recherches **impliquant la personne humaine**
- Les recherches, études et évaluations **n'impliquant pas la personne humaine**

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 caractères personnelles**
  Ex : celles issues de dossiers médicaux, de cohortes existantes ou de SNDS

- Les traitements de données à caractère personnel ayant pour finalité ces recherches sont soumis à **l'autorisation de la CNIL**

- **Les nouveautés RGPD**

  ✓ Formalités allégées → accountability
  Documentation prouvant les démarches

  ✓ Désignation d'un délégué à la protection des données par certaines entreprises
  Data Protection Officer (DPO)

  ✓ Garantir la protection des données par défaut ou dès la conception
  Privacy by design, Privacy by default

  ✓ Etude d'impact sur la vie privée
  Privacy Impact Assessment (PIA)

  ✓ Signalement des violations de données
  En cas de risques pour les personnes