TUTORAT NIÇOIS : UE 7 : PROTECTION DES DONNÉES DE SANTÉ

1) Concepts et champs d'application

a) Données à caractère personnel (DCP)

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

= « tte information concernant une **personne physique identifiée ou identifiable** » ou susceptible de l'être

- ➢ Personne identifiable = qui peut être identifiée
  - ***directement*** ou ***indirectement***
  - par référence à un **numéro d'identification**/**éléments spécifiques** propres à son identité :
- ⇨ physique, physiologique, psychique, économique, culturelle ou sociale
- ⇨ *n° de sécurité sociale, n° d'ordre renvoyant à une liste nominative (même établie sur papier), PV bio, identifiant, identification par recoupement*
- ➢ Déterminer si personne est identifiable : considérer les moyens auxquels on a accès

b) Utilisation et traitement des données

Informations médicales personnelles intéressent beaucoup de monde :

- ⇨ ressource ++ pour ***épidémiologie/maîtrise des DS/commerce/assurances***
- ⇨ devoir de les **protéger** (secret médical)

RAPPEL : Partage secret médical ?

Ordonnances (1996) : ont accès au secret médical :

- *les soignants*
- *les inspecteurs de l'action sanitaire et sociale*
- *les médecins conseils.*

Ex : études épidémiologistes pour l'intérêt population : ∅ nécessité de connaître l'identité des personnes = secret médical

FICHIER = ensemble structuré/stable de DCP accessibles selon des critères déterminés.

TRAITEMENT (TTT) = opération portant sur des données personnelles : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion, rapprochement, interconnexion, verrouillage, effacement, destruction…

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

TTT informatique :

- ➢ **catégorisation**
- ➢ **concentration données importantes ++**
- ⇨ *si défaillance protection = danger +++ car accès à ttes les infos en même temps*
- ➢ **puissance**
- ⇨ *identification des personnes par recoupement*
- ➢ **interconnexion et dispersion**
- ⇨ *une donnée isolée est potentialisée si relation possible avec d'autres informations*
- ➢ **portabilité et appropriation**

c) Responsable/Destinataire des données

Responsable	Destinataire
= **personne, autorité publique, service, organisme** ⇨ détermine **finalités / moyens** nécessaires à sa mise en œuvre *(sauf désignation expresse par dispositions législatives)* ⇨ Établi sur le **territoire français** = installation stable ++ (*sinon, recours à des moyens de TTT situés en zone française)*	= **personne** habilitée à recevoir communication des données autre que la personne concernée - le **responsable** du traitement - le **sous-traitant** - les personnes chargées de traiter données de par leur **fonction** ☛ *autorités légalement habilitées* (pour mission ou exercice droit de communication) ≠ *destinataires*

d) Données médicales / Données de Santé

Données médicales	Données de Santé *(Article 8)*
= toutes les **données à caractère personnel relatives à la santé** d'une personne = données ayant un **lien manifeste et étroit avec la santé** = **données génétiques** *(Annexe de la recommandation du 13/02/97 relative à la protection des données médicales, Conseil de l'Europe)*	= **données sensibles** dont le TTT est en principe interdit ⇨ idem données raciales, politiques, sexuelles Dérogations prévues (art 8. II) : ➢ **consentement exprès** des personnes sf disposition contraire ➢ TTT nécessaires aux fins de : - **médecine préventive** - **diagnostics** - **administration de soins/TTT** - **gestion services santé** + mis en œuvre par professionnel de santé (ou par une personne tenue au secret) - **recherche médicale** ➢ TTT susceptibles de faire l'objet d'une d'**anonymisation** *(reconnu conforme par la CNIL)* ➢ TTT justifiés par **l'intérêt public** et autorisé par la CNIL *(ou par décret en CE pris après avis de la CNIL)*

2) Cadre légal

a) En France (Loi du 6/01/78)

Loi informatique, fichiers et libertés, relative aux : développement/utilisation/protection fichiers informatiques et manuels

- institution de cette loi par la **CNIL (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*

1992	dispositions pénales
1994	TTT automatisés de données nominatives => but = recherche dans le domaine de la santé
1999	TTT données personnelles de santé => but = évaluation/analyse activités soins/prévention
2000	Collecte/enregistrement/conservation des informations nominatives
2004	- **droits de la personne** renforcés - allègement des **formalités déclaratives** auprès de la CNIL - nouvelles contraintes pour **transferts de données** hors UE - nouveaux pouvoirs CNIL : sanctions et labellisation, institution ***« correspondant CNIL »*** = CIL = Correspondant Informatique et Libertés

+ Code de déontologie médicale (*article 4*) + **Code pénal** *(article 226-13)* + **Code de la santé publique**

b) En Europe

Recommandations Conseil de l'Europe du 3/01/81 sur les banques de données médicales automatisées

Directive du 24/10/95 : vise à ↘ **divergences entre législations nationales** sur la protection DCP en Europe

3) Principes de la loi IFL

a) *Protection des données*

- **confidentialité des informations** : seuls les utilisateurs habilités dans les conditions normalement prévues doivent avoir accès aux informations
- **intégrité des informations** : les informations ne sont modifiables que par les utilisateurs habilités dans les conditions d'accès normalement prévues
- **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*

Loi du 6/01/78 : tout fichier informatisé nominatif de façon directe ou indirecte doit être déclaré à la CNIL

Déclaration normale : le déclarant doit spécifier :

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

Déclaration simplifiée : la CNIL peut adopter normes simplifiée pour TTT courants ++ si ne portent pas atteinte à vie privée/libertés *(54 normes : gestion cabinets médicaux et paramédicaux/pharmacies /LABM /centres d'optique/personnel/contrôle d'accès/gestion membres associations/utilisation services téléphonie au travail)*

⇨ si TTT envisagé = norme : engagement de conformité suffit

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
- protections des fichiers
- sauvegarde
- sécurité contre les virus et le piratage
- alimentation électrique constante et protégée

c) *Finalité*

- = **déterminée/explicite/légitime/correspondant aux missions de l'organisme**
- données **adéquates/pertinentes/non excessives** par rapport aux finalités
- détournement de finalité = sanctions pénales = 5 ans d'emprisonnement, 300 000€ amende

⇨ *fichiers obligatoires publics non utilisables à fins politiques/commerciales /commentaires/fichiers bancaires*

d) *Obligation de sécurité*

Respect intégrité et confidentialité des données	= empêcher données déformées/endommagées/accès tiers non autorisés ⇨ obligation qui pèse sur le ***responsable TTT*** ⇨ mesures de sécurité physique + logique adaptées à : - la nature des données - aux risques présentés par TTT *(ex: chiffrement des données sur internet)*
Identification	= **« entité »** informe le système distant de son identité ⇨ **identifiant = nom ou numéro utilisateur** ⇨ permet au système de savoir avec "qui" il communique *ex : login / carte à puce / carte vitale*
Authentification	= élément qui **caractérise une « entité»** + **autorise l'accès au système** *ex : mot de passe, emprunte digitale* = outil essentiel de la **confidentialité** ⇨ *celui qui accède à donnée est bien autorisé à le faire*
Gestion d'accès	tableau des habilitations
Précautions élémentaires	➢ Accès à application : - protégé par **mots de passe individuels / alphanumériques** /de **6-7 caractères** au moins / **peu courants** *(évitez initiales, nom, prénom, SESAM)/* **changés régulièrement** ➢ **Éteindre ordi** si absence/déco ou **écran veille protégé** par mot de passe ➢ **!!! si connexion à Internet** : antivirus/firewall/séparation réseaux ➢ **sauvegardes** régulières (CD-Rom) à conserver en lieu ≠ base données. ➢ !!! si numérisation/compression images (imagerie médicale), utilisation de **procédures normalisées** : garantir l'intégrité de ces données. ➢ Si données transférées via Internet : **dispositif chiffrement communicat°** (*ex: chiffrement SSL avec une clef de 128 bits, messagerie sécurisée)* ➢ **Protocoles transmission adaptés** : conformité données reçues /émises. ➢ Pour les applications en réseau : • *Par-feu (firewall)* • *Maintenance matériel* • *Limiter nb informaticiens « super-utilisateur »/ « administrateur sys »* • *Selon données traitées, traçabilité, journalisation des connexions*

e) *Les droits des personnes*

Droits : à l'information préalable et consentement éclairé + curiosité + accès direct/indirect + rectification + oubli + information

Droit d'être informé	⇨ identité du ***responsable*** ⇨ ***finalité*** poursuivie par le TTT ⇨ caractère oblig/facultatif des : ***réponses/conséquences*** (si ⃠ réponse) ⇨ ***destinataires*** des données ⇨ **droit de s'opposer** pour raison légitime au TTT ⇨ **droit d'accès et de rectification** et cas échéant : ***transfert vers État non membre*** Communauté europ *Modalités d'information : affichettes dans établissements santé, accueil des caisses, note d'info sur site web de l'organisme, lettre présentation de l'étude...*
Droit d'opposition	!!! QUE pour des raison légitimes sauf si TTT = obligation légale ⇨ discrétionnaire en matière de recherche médicale/utilisation données pour prospection commerciale
Droit de rectification	X
Droit à l'oubli	**Durée de conservation :** - **limitée** (adéquation avec finalité poursuivie par TTT) - **mentionnée dans le dossier** de formalité ⇨ conservation en ligne ≠ archivage - > à cette durée : données pour TTT historiques, statistiques, scientifiques - *(TTT archives publiques sont dispensés des formalités préalables)*

4) Accès au dossier médical

a) *Propriétaire*

- protection des **données médicales** *(ex : suppression feuilles de T° et prescriptions au lit du malade)*
- protection des **infos nominatives** au niveau du circuit et du stockage du dossier médical
- procédures de **destruction des documents nominatifs**

Qui sont les propriétaires ?

- 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**

b) Accès

- le **patient**
- 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

Loi du 4/3/2 : **accès direct du patient à l'ensemble des informations de santé le concernant** *(repris dans art 43 de la loi « informatique et libertés »)*
Décret du 29/04/02 : a organisé cet accès : - délai de communication **entre 48h et 8j** - si données remontent à + 5 ans : délai est porté à **2 mois** - présence d'une **tierce personne** peut être recommandée - accès aux données se fait : o au **choix du demandeur** o **consultation sur place** o **envoi des documents** *(frais de délivrance copies < coût reproduction et envoi des documents)*

c) Communication

Ce dossier contient :

- **infos formalisées** recueillies lors : -**COMMUNICABLES-**
  - des ***consultations externes*** dispensées dans l'établissement
  - de l'accueil au ***service des urgences***
  - de l'admission et au cours du ***séjour hospitalier***
- **infos formalisées** établies : -**COMMUNCABLES-**
  - à la ***fin du séjour***
- infos mentionnant qu'elles ont été recueillies : -**NON COMMUNICABLES-**
  - auprès de tiers n'intervenant pas dans prise en charge ttt

5) CIL

Loi du 06/01/78 revue en 2004 : correspondant **Informatique et Libertés**

⇨ **allègement des formalités** : dispense de déclaration des traitements :
- ¤ *sauf TTT relevant du régime de l'autorisation/demande d'avis*
- ¤ *sauf si transfert de données à destination d'un État non membre Communauté européenne*

⇨ **désignation = facultative = ouverte à tout responsable de TTT**

⇨ correspondant : chargé d'inscrire sur **registre** les TTT mis en œuvre par l'organisme

⇨ meilleure application loi + **diffusion culture info et libertés** (localement + indépendante)

⇨ relations privilégiées avec la CNIL : **service dédié, information ciblée et adaptée**

Rôle de conseil	• saisi pour avis avant mise en œuvre de tout nouveau TTT • prépare dossiers de formalités pour les TTT à risque
Recommandation	• traduit les termes de la loi en règles internes/codes de conduite propres au secteur d'activités
Médiation	• reçoit les plaintes/requêtes personnes concernées par TTT (droit d'accès ++)
Alerte	• informe le responsable de TTT des manquements constatés
Information	• dresse bilan annuel = reflet de son action (TTT examinés, recommandations)