CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

Réglementation sur la protection des données à caractère personnel

Le BIG DATA en santé

De quoi parle-t-on?

- Création de données massives, ensemble de données ou « *Big data* »
  - Capacité à analyser divers ensembles de données provenant d'une multitude de sources
  - En santé, ensemble de données socio-démographiques et de santé collectées pour des finalités variées et disponibles auprès de différentes sources

- L'ère de la « médecine 4.0 »
  - Explosion de l'utilisation d'objets connectés (« *quantified self* »)
  - En 2020, on estime à 90% la proportion de données alimentant le *big data* via des objets connectés et capteurs personnels

Quels usages?

- Améliorer la prise en charge du patient
- Faciliter la recherche scientifique
- Mettre en place des mécanismes de vigilance sanitaire
- Mieux cibler la prévention
- Maîtriser les dépenses

Quels enjeux?

- Ethiques : équilibre à trouver entre les perspectives innovantes en santé (pratique médicale renouvelée et opportunités scientifiques) et le respect de la vie privée
- Economiques : les différents acteurs en présence (les anciens et les nouveaux)

La grille d'analyse de la CNIL

- La grille d'analyse de la CNIL ou les 5 règles d'or de la protection des données appliquées au *big data*
  - *Principe de finalité et de proportionnalité;*
  - *Pertinence des données traitées;*
  - *Conservation limitée des données;*
  - *Respect des droits des personnes concernées: loyauté et transparence (droit à l'information, consentement, droit d'opposition, d'accès et de rectification).*

Le traitement de données de santé

- Le principe : l'interdiction du traitement de données relatives à la santé (article 8-I de la LIL)

- Les exceptions :

  - 8-II-1°: consentement exprès ;
  - 8-II-6° : les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;
  - 8-II-8°: les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX ;
  - 8-IV : les traitements justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25.

Le traitement de données à des fins de recherche dans le domaine de la santé

- Avant la LMSS de 2016, deux chapitres de la loi Informatique et Libertés étaient consacrés à la recherche en santé :
  - Chapitre IX : traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé;
  - Chapitre X : traitements de données à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention.

- Après la LMSS de 2016 : fusion des chapitres IX et X
  - Nouveau chapitre IX: traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.
    - Modification du chapitre IV du décret d'application de la LIL (décret n°2016-1872 du 26 décembre 2016).

Les catégories de recherches dans le domaine de la santé

- Recherches impliquant la personne humaine :
  - Recherches interventionnelles;
  - Recherches interventionnelles à risques et contraintes minimes;
  - Recherches non interventionnelles.

  →Compétence CPP + CNIL

- Études, évaluation et recherches n'impliquant pas la personne humaine :

  → Compétence CEREES (*via* INDS) + CNIL

Un renforcement du pouvoir de simplification de la CNIL par la LMSS 2016

- **Maintien des méthodologies de référence (article 54-IV)**

- **Deux nouvelles mesures de simplification**
  - **L'homologation par la CNIL de conditions d'accès à des jeux de données agrégées ou des échantillons (article 54-V)**

  - **Les décisions uniques (article 54-VI)**
    - même demandeur
    - même finalité
    - mêmes catégories de données
    - mêmes catégories de destinataires

Focus sur les méthodologies de référence

- Fondement juridique : Article 54 de la loi Informatique et Libertés (alinéas 5, 6 et 7) (article 54-IV depuis la loi de 2016)
  - Pour les catégories les plus usuelles de traitements;
  - Homologation après concertation avec le CEREES et les organismes représentatifs des acteurs concernés.

Les méthodologies de référence existantes

- **MR 001 :** décision du 5 janvier 2006 portant homologation d'une méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales
  - Modifiée par la délibération n°2016-262 du 21 juillet 2016 portant modification d'une méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales

- **MR 002 :** délibération n° 2015-256 du 16 juillet 2015 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro

- **MR 003 :** délibération n° 2016-263 du 21 juillet 2016 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement exprès ou écrit de la personne concernée

A VENIR

- Mise à jour des MR 001 et 003 (périmètre CPP)
- Création d'une MR 004 (périmètre CEREES)
- Création de MR sur le PMSI

Les entrepôts de données

- Bases de données de santé utilisées à des fins de recherche ultérieure;
- Pose la question de la réutilisation, dans l'intérêt public, de données de santé, à des fins de recherche ultérieure avec la problématique liée au respect des droits des personnes concernées et celle de la finalité.

Illustrations au travers des autorisations de la CNIL

- Délibération du 10/11/2016 autorisant la mise en œuvre du centre d'étude et de recherche national dédié au traitement des images cérébrales (« CATI ») par le CEA
- Délibération du 19/01/2017 autorisant la mise en œuvre de l'entrepôt de données de santé (EDS) de l'AP-HP
- Fixe le cadre applicable pour la création de ce type d'entrepôt

Exemple de l'EDS – Finalités

- Finalités :
  - Faciliter la réalisation de recherche dans le domaine de la santé et d'études relatives au pilotage hospitalier en regroupant dans une base unique l'ensemble des données de soins recueillis auprès des patients hospitalisés dans l'un des 39 établissements de l'AP-HP
    - Recherches non interventionnelles par les personnels de l'AP-HP, éventuellement associés à des partenaires extérieurs;
    - Réalisation d'études de faisabilité d'essais cliniques;
    - Réalisation d'études relatives au pilotage médical et stratégique visant à optimiser l'organisation des soins.

EDS – information

- L'information des personnes: patients et professionnels de santé

- L'information générale relative à l'entrepôt pour les patients
  - remise d'un document écrit **pour les patients pré-admis ou admis** postérieurement à la constitution de l'EDS
  - **En tout état de cause**, livret d'accueil, affichage dans les locaux des établissements et site web de l'AP-HP précisant que tout patient pris en charge par l'AP-HP, y compris avant constitution de l'EDS, est inclus dans cette base unique et peut s'opposer à l'utilisation de ses données dans le cadre de recherches.
- Qui ne se substitue pas à l'information individuelle prévue par les dispositions de l'art. 57 de la LIL à réaliser pour chaque projet de recherche.

- L'information des professionnels de santé

EDS - Autres

- Intervention d'un **comité scientifique et éthique** de l'AP-HP ayant une mission d'évaluation des projets de recherche et d'autorisation des accès aux données de l'entrepôt

- La CNIL a rappelé la distinction entre le traitement de l'entrepôt de données (article 25) et les traitements mis en œuvre ultérieurement à des fins d'études/recherches en santé **soumis à des formalités distinctes** (chap. IX)

L’anomymisation

- Si une donnée est anonymisée, elle n’est « rattachable » à aucune personne et n’est donc pas une donnée à caractère personnel au sens de la LIL;
- Une donnée/un jeu de donnée ne permet pas d’identifier, ni directement, ni indirectement un individu. Cette identification doit être impossible pour le détenteur du jeu de données ou toute autre personne;
- Conséquence: si la donnée est anonyme, pas d’application de la LIL.

L’anonymisation

- Procédé **d’anonymisation**: traitement de données consistant en un semble de techniques par lesquelles des données personnelles sont rendues anonymes. Si le procédé n’est pas appliqué de façon suffisamment poussée, les données conservent leur caractère personnel ;

- Procédé **de pseudonymisation**: traitement de données consistant en un procédé par lequel des données directement identifiantes sont rendues indirectement identifiantes.

L’anonymisation

- Critères du G29 relatifs à l’anonymisation
  - L’individualisation;
  - La corrélation;
  - L’inférence.

- Analyse de risque en ré-identification qui doit être nul ou pratiquement nul à l’issue du processus pour reconnaitre le caractère anonyme de la donnée/jeu de données

Le RGPD

- La philosophie générale du RGPD s'articule autour de 3 idées :
  - Crédibiliser les CNILs européennes (système de coopération pour les traitements transfrontaliers, augmentation très sensible du montant des amendes : 20 millions ou 4% de son chiffre d'affaires annuel mondial);
  - Renforcer les droits des personnes dont les données sont traitées;
  - Responsabiliser les acteurs.

Le RGPD

- Les principes de la protection des données sont presque identiques à ceux qui existent en France depuis 1978 :
  - Licéité, loyauté et transparence dans l'utilisation des données;
  - Limitation des finalités (finalités déterminées, explicites et légitimes);
  - Minimisation des données (données adéquates, pertinentes et limitées à ce qui est nécessaire);
  - Exactitude des données (données exactes, et tenues à jour);
  - Limitation de la conservation (données conservées sous une forme permettant l'identification des personnes pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées);
  - Le RGPD ajoute un nouveau principe qui concerne la sécurité des données et le principe de responsabilisation des acteurs.

Le RGPD - responsabilisation

- Que signifie le principe de responsabilisation?
  - Il impose qu'un responsable de traitement est en mesure de démontrer qu'il respecte les principes posés par le RGPD;
  - Il s'agit de passer dans une démarche de **conformité dynamique** : c'est-à-dire de s'assurer tout au long de la « vie » du fichier que les principes sont respectés (pas de collecte de données excessives, une fois inutiles, les données sont effacées ou anonymisées, les mesures de sécurité sont respectées, etc.);
  - La CNIL a publié une méthodologie en 6 étapes pour se préparer à l'entrée en vigueur du RGPD en mai 2018.

Le RGPD

- Etape 1 : **désigner un pilote**
  - le délégué à la protection des données (DPO)
- Etape 2 : **cartographier les traitements de données personnelles**
  - recenser de façon précise les traitements de données personnelles (utilité d'un registre des traitements)
- Etape 3 : **prioriser les actions à mener**
  - Sur la base du registre:
    - **identifier** les actions à mener pour se conformer aux obligations actuelles et à venir;
    - **Prioriser** les actions au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées.

Le RGPD

- Etape 4 : **gérer les risques**
  - Si des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées ont été identifiés, mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).
- Etape 5 : **organiser les processus internes**
  - Pour assurer un haut niveau de protection des données personnelles en permanence, procédures internes garantissant la prise en compte de la protection des données à tout moment à mettre en place, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).
- Etape 6 : **documenter la conformité**
  - Pour prouver la bonne conformité au règlement, constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

- Et le projet de loi …?

Merci pour votre attention !