PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL
COLLECTE ET CONSERVATION DES DONNÉES

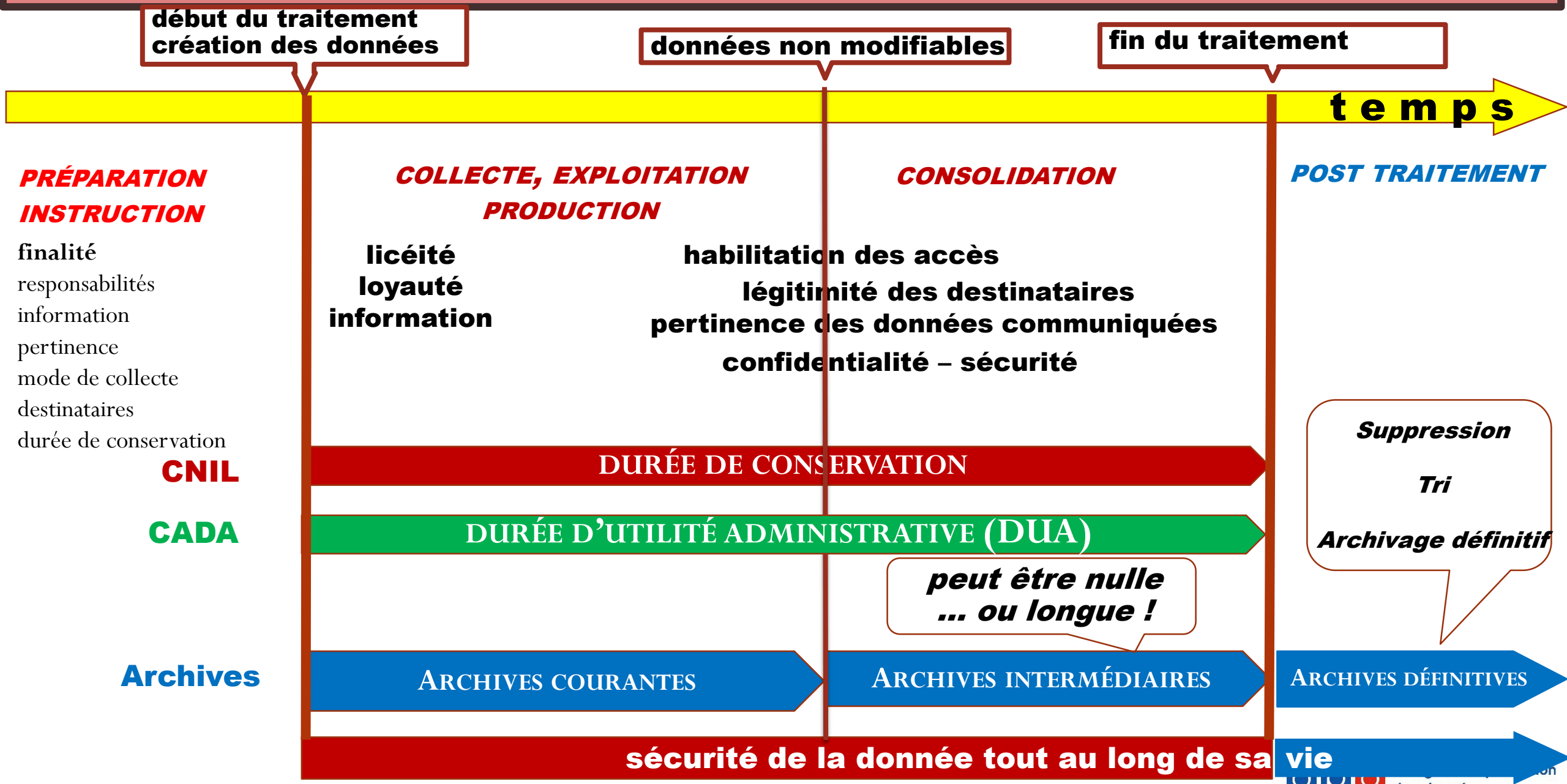
une approche « RGPD »

en amont et tout au long du projet

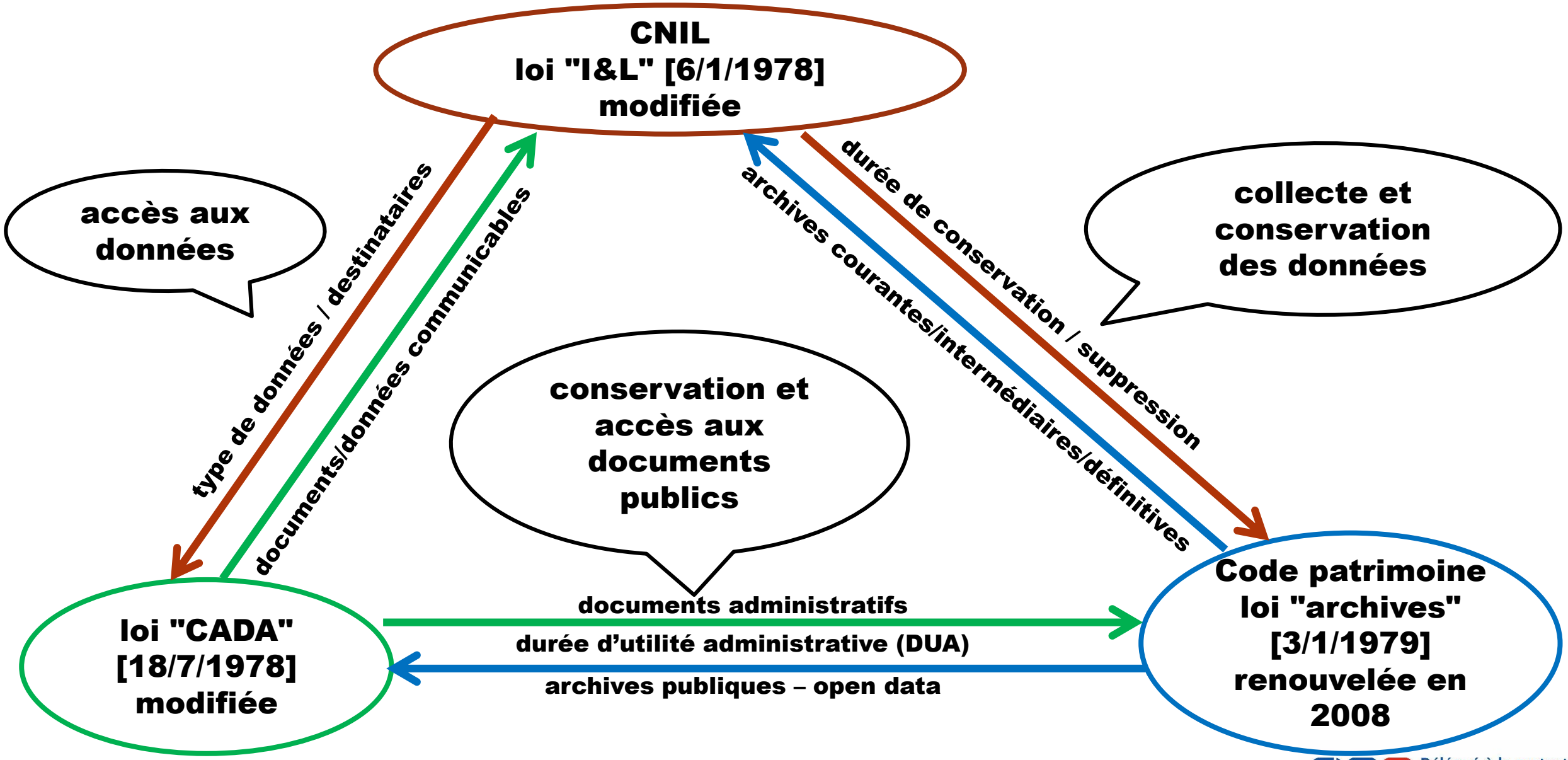
Mots clés : éthique, confidentialité, sécurité, légalité

Délégué à la protection des données

vue "CNIL" de la vie d'une donnée



3 lois concomitantes liées par des critères communs



Délégué à la protection des données

Enjeux de protection des données personnelles selon les différentes phases d'un traitement de recherche

- **NB : la collecte des 1ères données marque le début du traitement**
- **La sélection des personnes sujets potentiels de la recherche**
  - **critères de sélection**, contact (mail…), …
  - constitution de fichier de volontaires ? : identité, adresse, contact, sexe, âge…
- **L'inclusion des personnes (données personnelles contextuelles brutes)**
  - consentement, table de correspondance → **conservation sécurisée indépendante** des données recherche
  - **critères d'inclusion** : plus **intrusifs** (données « sociodémographiques », comportement, état de santé…

Font partie du traitement

- **La collecte des « données de recherche » (données brutes)**
  - données à caractère personnel **liées à la finalité** (métier) de la recherche
  - par **questionnaires**, **entretiens**, **mesures** (EEG…), **extractions** depuis un autre traitement (données patients CHU, BigData données médico-administratives : SNDS, CNAM, MSA…), etc.
- **L'exploitation des données brutes et la production des résultats**
  - plus de nouvelles données collectées
  - **attention : sécuriser les transferts de données du lieu de collecte au lieu d'exploitation (pas de mail ou chiffrer les données…)**
  - résultats **« anonymes »** (agrégés, pseudonymisés) produits à partir des données
- **La mise à disposition des données (science ouverte ←→ loi pour une république numérique, RGPD)**
  - public : résultats statistiques, agrégés → ne permettent pas d'identifier les personnes
  - chercheurs : données de recherche pseudonymisées pour réutilisation ultérieure éventuelle

Collecte et conservation de données

- **La conservation débute dès la collecte**
- **Les questions à se poser <u>avant la collecte</u> sur la conservation (« stockage »)**
  - Où sont (stockées) les données ?
  - Quelle sécurité ? → serveur local sécurisé ? **portable chercheur chiffré ?**
  - Quelle protection de confidentialité ? : gestion des accès, chiffrement des données…
  - Combien de temps ? : quelle est la durée maximum pertinente « d'utilité » des données ?
- **Les réponses à apporter sont fonctions**
  - de la nature des données collectées et conservées
    - légales (consentement)
    - confidentielles (table de correspondance
    - données personnelles), sensibles (données de santé…)
  - des supports et moyens de collecte et de conservation

Collecte et conservation de données

Collecte directe auprès de la personne

- questionnaire
  - papier
  - en ligne → **pas de plate-forme « cloud » → utiliser les plates-formes locales de l'université (Lime Survey, Sphinx)**
- entretien (semi) dirigé
  - retranscrits à l'entretien (notes, grilles…)
  - enregistrés et retranscrits « plus tard » → **sécuriser les enregistrements et les effacer dès retranscription**
- vidéo → **attention : droit à l'image éventuel → réduire la zone filmée tant que possible**
- mesures (capteurs) : EEG, ECG, oralité, déplacements… → **attention si géolocalisation**

Collecte indirecte (extraction…) : conditions préalables (rappel)

- les personnes doivent
  - être informées préalablement du possible traitement de leurs données (ex. données patients CHU pour la recherche universitaire)
  - être en mesure de s'y opposer (faisabilité raisonnable)
- formalités « CNIL » pour les traitements de données de santé à des fins de recherche externe (hors lieu de soins, universitaire…)

Durées de conservation

La conservation après la collecte (exploitation et production de résultats)

- veiller à la sécurisation des transferts de données et à la suppression des données sur les supports de collecte

Données de santé traitées en recherche

- la conservation de données de santé à des fins de recherche n'est pas soumise à agrément du Ministère de la santé
- **pour autant la sécurité des données de santé conservées ne doit pas être négligée**
- durées de conservation standard (MR-001, MR-003, MR-004)
  - **données des personnes concernées par la recherche : jusqu'à deux ans après la dernière publication des résultats** de la recherche ou du rapport final de la recherche puis archivage sur support papier ou informatique pour une durée de vingt ans maximum ou conforme à la règlementation en vigueur
  - données des **professionnels intervenant dans la recherche** ne peuvent être conservées **au-delà d'un délai de quinze ans après la fin de la dernière recherche** à laquelle ils ont participé. Elles font ensuite l'objet d'un archivage sur support papier ou informatique pour une durée conforme à la réglementation en vigueur.

Partage et/ou mise à disposition de données de recherche
besoins et risques

Contexte lié aux besoins

- beaucoup de projets interdisciplinaires faisant intervenir plusieurs équipes ou laboratoires
- diversité des lieux et des modes de collecte des données
- multiplication des lieux de conservation (stockage) de données identiques

Les risques

- pertinence des données partagées ou mises à disposition → risques : **données excessives → atteinte à la vie privée**
- sécurité et confidentialité des données conservées → risques : **pertes, accès illégitimes**
- sécurité des transferts entre les chercheurs, les équipes… → risques : **accès illégitimes**

Partage et/ou mise à disposition de données de recherche
Compromis entre besoins de recherche et risques sur les données

- **Mesures organisationnelles (processus) et techniques à mettre en œuvre par les personnes en charge de la mise en œuvre : chercheurs, techniciens…**
- **Au niveau du projet**
  - établir un plan (même minimal) de management des données
  - définir les données pertinentes à partager : niveau d'anonymat ?
  - définir un lieu unique et sécurisé d'hébergement des données à partager (ex. UMS GRICAD)
  - définir les personnes habilitées à accéder aux données et gérer les habilitations (ex. connexion authentifiée, journalisation des accès…)
- **Au niveau individuel**
  - protéger les données sur son ordinateur : ex. chiffrement complet (recommandation CNRS)…
  - a minima protéger les données transférées : ex. chiffrer les fichiers, utiliser un serveur sécurisé de dépôt/téléchargement (FileSender de RENATER), connexion directe et sécurisée au serveur…

Recherche et HDS (Hébergement de Données de Santé)

- **Hébergement de Données de Santé**
  - Article R1111-8-8 du Code de la santé publique (Créé par Décret du 26 février 2018)
  - ***I. - L'activité d'hébergement de données de santé à caractère personnel mentionnée au I de l'article L.1111-8 consiste à héberger les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social***
- **On entend beaucoup de la nécessité d'avoir un hébergeur de données qui soit certifié HDS**
- **Cette obligation ne s'applique pas aux données de recherche**
- **Pour autant, les obligations du RGPD (sécurité et confidentialité des données) s'appliquent pendant toute la durée de conservation des données, que les données soient ou non hébergées par un tiers**

Stockage, mise à disposition, réutilisation
le cas du dossier patient

- **Appel à la vigilance et à la rigueur : une donnée stockée et mise à disposition pour un usage ne doit pas être accédée pour une autre finalité! (1 traitement = 1 finalité, principe n°2)**
- **Le dossier patient contient des données confiées par un patient à l'équipe de soins pour sa prise en charge et l'amélioration de sa prise en charge**
  - activités et suivi de soins
  - recherches internes : par l'équipe de soins à destination exclusive de l'équipe de soins.
- **La mission d'intérêt public de recherche permet de poser une licéité pour concevoir un traitement de ces données mais en aucun cas d'accéder au dossier patient sans autre formalité**
  - recherches externes : multicentriques ou données accédées hors équipe de soins
- **Attention : la mise à disposition de données du dossier patient sans formalité et/ou accord du patient constitue une violation de données sanctionnable par la CNIL au titre de la loi I&L**

Open Data en santé

- **Un domaine complexe, sans réponses claires dans les textes**
- **En 1er niveau, la mise en disposition publique est incompatible avec la notion de données personnelles (a fortiori de santé)**
- **Il convient donc de se placer dans un cadre de données « anonymes » : ne permettant pas d'identifier directement ou indirectement une (ou plusieurs) personne(s) physique(s)**
- **Une évaluation de la possibilité de ré-identification doit être faite au cas par cas avec les responsables de la recherche, le DPO et d'autres personnes en mesure d'apporter une expertise : RSSI, DSI…**
  - ex. validation de l'anonymat pour un ensemble restreint de photographies de chirurgie bariatrique uniquement grâce à la faible dimension par rapport au nombre d'instances existantes
- **Cette évaluation doit être menée dans une AIPD (minimisation des risques d'impact du traitement de données sur la vie privée)**

Traitements de recherche universitaire opérés dans les structures de recherche

Principales thématiques de recherche

- santé et SHS, mais de plus en plus économie/gestion, agronomie, nouvelles technologies…

Responsabilités

- responsable le de traitement structure propre : l'établissement tutelle (chef d'établissement)
- responsable le de traitement structure multi-tutelles (UMR, UMS, U, US…) : Directeur.trice de l'unité
- responsable de mise en œuvre : le.la responsable scientifique
- **nb : le.la doctorant.e ne porte pas de responsabilité mais est tenu .e de respecter les obligations légales**

Quel Délégué à la protection des données (DPO) ?

- structure propre (tutelle unique) : DPO de l'établissement tutelle
- structure mixte (multi-tutelles) : UMR, UMS, U, US… : DPO de l'établissement tutelle employeur Directeur.trice

Difficultés et risques

- faible pourcentage des projets analysés sur le RGPD → **risque juridique = non-conformité RGPD**
- la qualification des traitements au regard des finalités poursuivies et des données traitées
  - RIPH ou non ? ex. étude en psychologie mise en œuvre par questionnaire ; étude psychomotrice (tests de marche…)
  - les recherches traitant « à la marge » des données de santé entrent-elles dans le cadre des recherches en santé ? ex. études de l'apprentissage de la lecture chez les enfants dyslexiques

Traitements de recherche universitaire opérés dans les structures de formation

Principales thématiques

- SHS (mémoires de Master)
- **thèses en médecine générale (DMG)** : études de pratiques en cabinet de MG, recherches externes portant sur des données de santé

Responsabilités

- le responsable de traitement est l'établissement de formation (université…)
- la responsabilité de mise en œuvre est portée par la direction de la formation ou le directeur de thèse
- **nb : l'étudiant.e ne porte pas de responsabilité mais est tenu.e de respecter les obligations légales**

Quel Délégué à la protection des données (DPO) ?

- DPO de l'établissement

Difficultés et risques

- (non) conscience des responsables sur leurs responsabilités
- pas de sensibilisation des étudiants sur la protection des données
- seules une partie (15%) des thèses DMG sont déposées pour instruction RGPD
- → **risque juridique = non-conformité au RGPD**

Données de santé – définition d'après cnil.fr : « Qu'est-ce ce qu'une donnée de santé ? »

Le RGPD donne une définition large des données de santé (article 4.15)

- «données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne; »
- On peut dire que sont des données de santé des données à caractère personnel permettant de manière directe, indirecte, par croisement ou par déduction de révéler des informations sur l'état de santé d la personne à laquelle se rapportent ces données.

Les données de santé peuvent être regroupées en 3 catégories

- les données de santé **par nature** : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
- les données qui, prises isolément ne portent pas d'information sur la santé mais **dont l'association (recoupement, croisement) avec d'autres données** permet de révéler une(des) information(s) sur l'état de santé ou un risque pour la santé de la personne
  - ex. poids + taille [+ sexe] [+ âge] → IMC = information sur une obésité, anorexie… éventuelle
  - ex. mesure de tension + mesure d'effort → information sur un risque éventuel : infarctus, AVC…
- les données **qui deviennent des données de santé** en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Données de santé – formalités pour les traitements de recherche universitaires

- **L'allègement des formalités des traitements par le RGPD n'impacte pas les demandes d'autorisations en matière de recherche et d'évaluation soumises au chapitre IX de la loi « informatique et libertés ».**

- **La CNIL propose des référentiels : méthodologies de référence (MR-xxx) qui allègent les formalités de certains traitements dès lors qu'ils satisfont à ces référentiels et ont fait l'objet d'un engagement de conformité de la part du responsable de traitement (université ou laboratoire)**

- **Outre les dispositions spécifiques de la loi informatique et libertés, les dispositions générales du RGPD s'appliquent en tout état de cause**

Délégué à la protection des données

Les outils pour accompagner les chercheurs

Le Comité d'éthique pour la recherche, Grenoble Alpes (CERGA)

- analyse et avis éthique des projets soumis
- attribution d'un numéro IRB (institutional review board) : validation éthique pour les publications internationales

Les délégués à la protection des données (DPO)

- **rappel** : DPO obligatoire pour les établissements et les structures mixtes de recherche
- le DPO mutualisé du site Grenoble Alpes (DPO des 5 établissements universitaires du site)
- Le DPO de la structure mixte (DPO de l'établissement employeur du DU)
- Le DPO du CHU Grenoble Alpes

Les RSSI des établissements et les CSSI des structures de recherche

MERCI DE VOTRE ATTENTION

Des questions ?.....

Contact : DPO@grenet.fr

Délégué à la protection des données