

# La protection des données de santé

# Plan de la présentation

---

1. Présentation du droit applicable à la protection des données
2. Présentation de la CNIL
3. Les différentes notions
4. L'application du RGPD
5. Les règles d'or de la protection des données
6. Les grands principes en matière de protection des données de santé
7. La détermination de la formalité applicable
8. Comment mettre en œuvre le RGPD dans la pratique ?



# Présentation du droit applicable à la protection des données

# Le droit applicable à la protection des données

---

- ◊ **Règlement général sur la protection des données** (entré en vigueur le 25 mai 2018)
- ◊ **Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** dite « *informatique et libertés* » modifiée
- ◊ **Décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
- ◊ **Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé (SNDS...)**
- ◊ **Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé**
- ◊ **Autres dispositions légales (code pénal, code de la santé publique, code civil...)**



# Présentation de la CNIL

# Les missions de la CNIL (1)

## Informer et protéger

---

**189 877** APPELS

**16 877** REQUÊTES  
SUR LA PLATEFORME « BESOIN D'AIDE »

**8 millions**  
DE VISITES SUR CNIL.FR

**11 077**

PLAINTES

**+ 32,5%**

**4 264**

DEMANDES DE DROIT  
D'ACCÈS INDIRECT

**6 609**

VÉRIFICATIONS  
EFFECTUÉES

# Les missions de la CNIL (2)

## Accompagner et conseiller

---

 Délégué à la protection  
des données

**4 124**

DÉCISIONS  
ET DÉLIBÉRATIONS  
ADOPTÉES

**350** DÉLIBÉRATIONS  
DONT :

**177** AVIS SUR  
DES PROJETS  
DE TEXTE

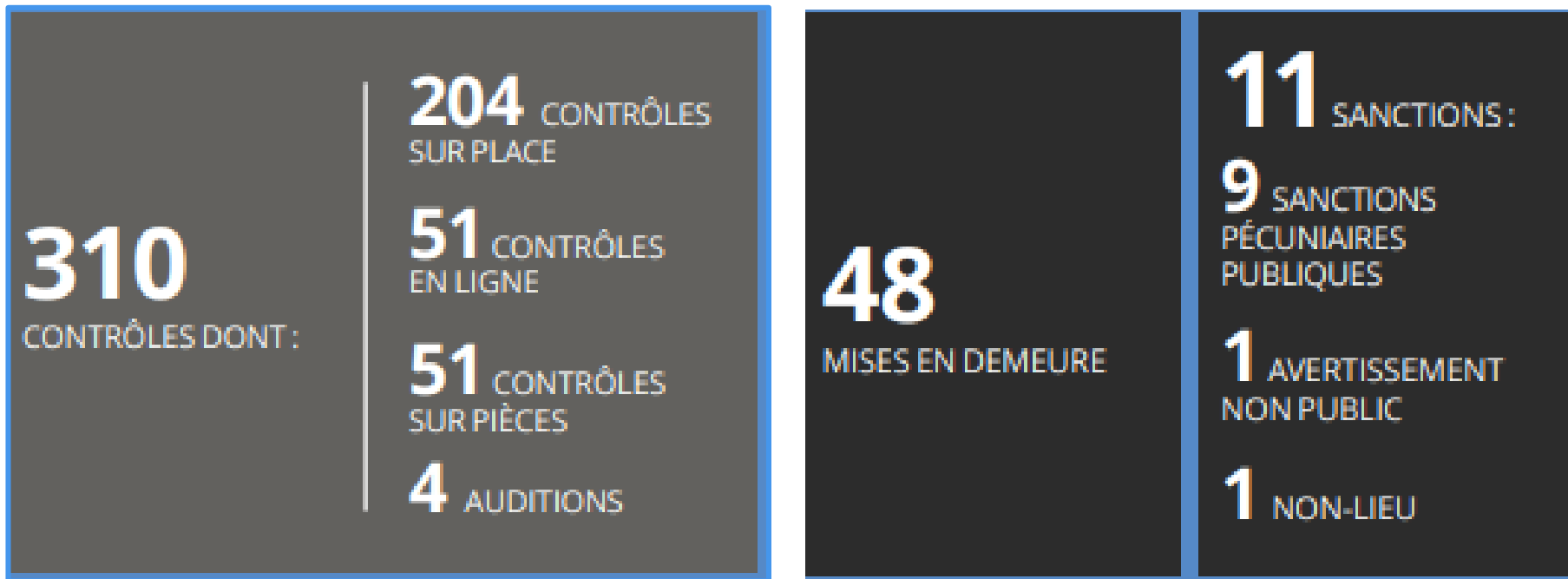
**101** AUTORISATIONS



## Les missions de la CNIL (3)

### Contrôler et sanctionner

---



# Les missions de la CNIL (4)

## Anticiper et innover

---





# Les différentes notions

# Qu'est ce qu'un traitement de données à caractère personnel ?

---

## Données à caractère personnel

Toute information se rapportant à une **personne physique identifiée** ou **identifiable** directement ou indirectement.

Directement identifiant

Indirectement identifiant

Recoupement d'informations anonymes

## Traitement

Toute **opération** portant sur des données personnelles, **quel que soit le procédé utilisé**.

### Par exemple:

- enregistrer,
- organiser,
- conserver,
- modifier,
- transmettre,
- etc.

# Données pseudonymisées # données anonymisées

---

## Article 4 du RGPD

**Pseudonymisation:** *«le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »*

Une donnée non directement identifiante peut être une donnée à caractère personnel : **donnée pseudonymisée / codée (la plupart du temps, en recherche)**

Une donnée « anonyme » n'est **PLUS/PAS** une donnée à caractère personnel **IMPORTANT**



# Données anonymisées

---

## Position du G29 (avis 05/2014 sur les techniques d'anonymisation)

« Une solution d'anonymisation doit être construite au cas par cas et adaptée aux usages prévus. Pour aider à évaluer une bonne solution d'anonymisation, le G29 propose trois critères :

**L'individualisation** : est-il toujours possible d'isoler un individu ?

**La corrélation** : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?

**L'inférence** : peut-on déduire de l'information sur un individu ?

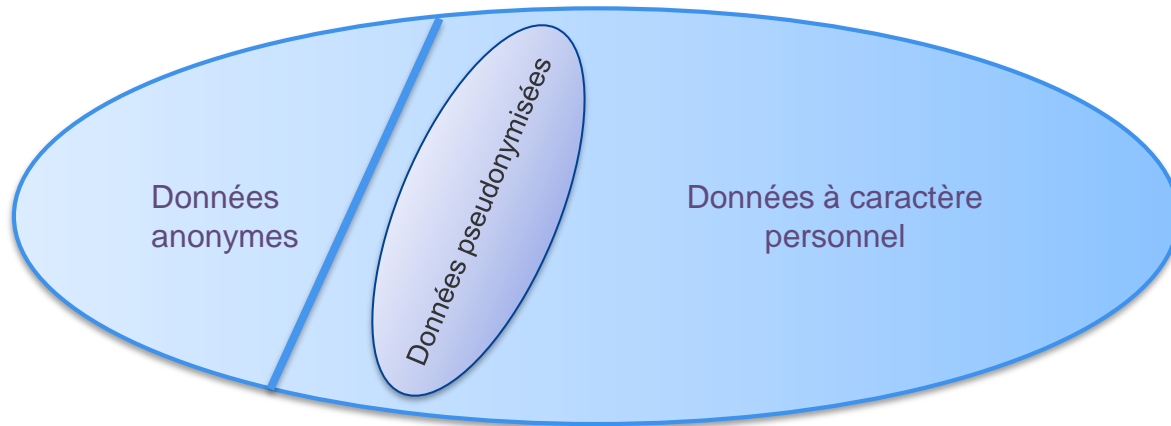
Ainsi :

**un ensemble de données pour lequel il n'est possible ni d'individualiser ni de corréler ni d'inférer est a priori anonyme ;**

**un ensemble de données pour lequel au moins un des trois critères n'est pas respecté ne pourra être considéré comme anonyme qu'à la suite d'une analyse détaillée des risques de ré-identification. »**

## En résumé

---



- Un **processus d'anonymisation est un traitement de données** à caractère personnel impliquant un **appauvrissement** des données brutes et une **restriction** du champ des exploitations possibles.
- Une donnée anonyme (selon les critères du G29) **n'est plus** une donnée à caractère personnel. Elle peut être diffusée et utilisée largement (Recherche, Open data).
- **Pseudonymiser** un jeu de données protège la vie privée (dé-identification) mais cela ne le rend **pas anonyme**. Il permet le **chaînage et l'appariement des données personnelles d'un individu**.

# Les acteurs du traitement (1)

---

## Responsable de traitement

*« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »*  
(article 4 du RGPD)

### Exemples :

- ✓ Secteur privé : la société représentée par son président
- ✓ Secteur public : l'hôpital représenté par son directeur

## Les acteurs du traitement (2)

---

### Le sous-traitant

*« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »*  
(article 4 du RGPD)

En résumé: le sous-traitant agit sous l'autorité du responsable de traitement et sur ses instructions.



# L'application du RGPD

# Champ d'application du Règlement général sur la protection des données

---

1 Un traitement de données personnelles...

2 ...effectué par un responsable de traitement ou un sous-traitant...



établi sur le territoire de  
l'Union européenne :  
*critère de l'établissement*

ou

visant des personnes  
sur trouvant dans  
l'Union européenne :  
*critère du ciblage*



# Qui est concerné par le RGPD ?

---

Secteur public **et** secteur privé

---

Responsable de traitement **et** sous-traitant





# Les règles d'or de la protection des données

# Les principes clés



01



Licéité, loyauté & transparence du traitement

Finalité déterminée, explicite et légitime



02

03



Minimisation des données

Exactitude des données collectées



04

05



Durée de conservation limitée

**Intégrité  
Confidentialité  
Disponibilité**



**06**

**07**



**Respect des droits des  
personnes**



**Conformité**

# Les droits des personnes concernées

---



1. Droit à la transparence
2. Droit d'accès
3. Droit de rectification
4. Droit d'opposition
5. Droit à l'effacement
6. Droit à la limitation
7. Droit à la portabilité des données
8. Décision individuelle automatisée



# Les grands principes en matière de protection des données de santé

# Qu'est-ce qu'une donnée de santé ?

---

**Article 4 du RGPD** « données relatives à la **santé physique ou mentale**, passée, présente ou future, 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** »



Par nature



Par combinaison



Par destination

3 catégories de données de santé

# Exemples de traitements de données de santé

---

**Base de données PMSI de l'établissement de santé**

**Tenue d'un dossier patient (papier et informatisé)**

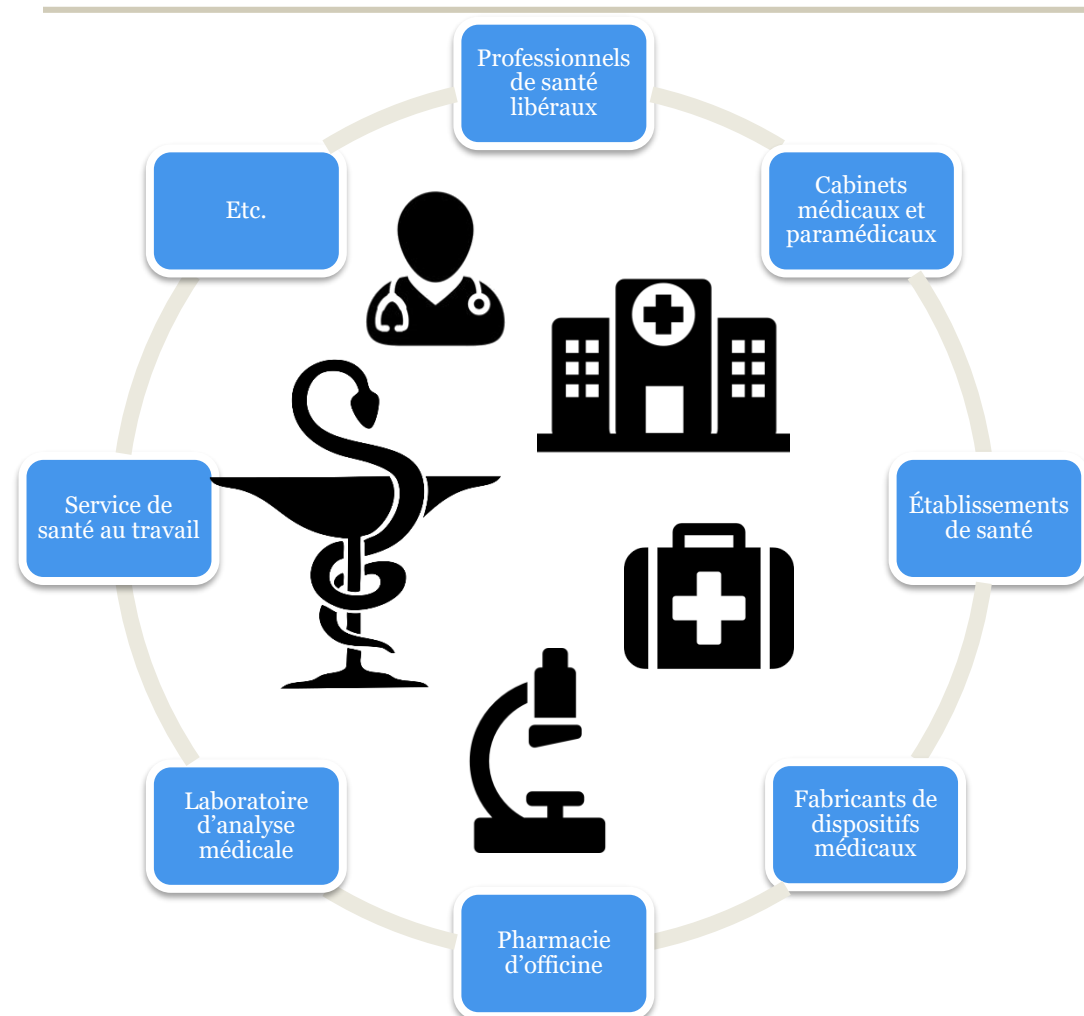
**Utilisation d'un dispositif de téléexpertise**

**PACS d'imagerie médicale**

**Collecte d'échantillons pour réaliser des recherches**

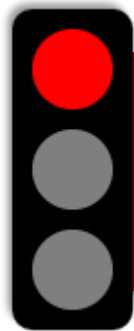
**Etc.**

# Qui est concerné dans le secteur de la santé ?



# Le principe en matière de données de santé

---



**Interdiction de traiter des données relatives à la santé**  
(*article 9-I du RGPD et article 6 LIL*)



Pour traiter des données de santé, il faut justifier de l'une des **exceptions** de **l'article 9.2 du RGPD**

**Attention** : à ne pas confondre avec la base légale (art. 6 du RGPD)

# Les exceptions à ce principe d'interdiction

(article 9.2 RGPD + articles 6 et 44 de la loi « informatique et libertés »)

---

- Le **consentement** explicite
- **Obligations** liées au droit du travail, protection sociale, sécurité sociale
- Sauvegarde des **intérêts vitaux** de la personne
- Les traitements mis en œuvre par une association ou autre **organisme à but non lucratif** si :
  - le traitement se rapporte exclusivement aux membres de l'organisme ou personnes entretenant des contacts réguliers et
  - la personne concernée a donné son consentement pour les données transmises hors de l'organisme
- **Données rendues publiques** par la personne concernée
- Constatation, exercice ou défense d'un **droit en justice**
- **Motifs d'intérêt public important**
- **Médecine préventive, diagnostics médicaux**, prise en charge sanitaire ou sociale ou **gestion des systèmes et services de soins en santé**
- **Motifs d'intérêt public** dans le domaine de la **santé publique**
- **Recherche scientifique**, fins archivistiques ou statistiques

# Les dispositions spécifiques en santé de la loi « informatique et libertés »

---

## Section 3

Traitements de données à caractère personnel dans le domaine de la santé (art. 64 et s. LIL)

Sous - section 1 : dispositions générales

Sous - section 2 : traitements à des fins de recherche, étude ou évaluation en santé

# Exceptions à l'application de la section 3

## Article 65 de la loi Informatique et Libertés

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.

Le **consentement** explicite

Sauvegarde des **intérêts vitaux** de la personne

Les traitements mis en œuvre par une association ou autre **organisme à but non lucratif** si :

- le traitement se rapporte exclusivement aux membres de l'organisme ou personnes entretenant des contacts réguliers et
- la personne concernée a donné son consentement pour les données transmises hors de l'organisme

**Données manifestement rendues publiques** par la personne concernée

Constatation, exercice ou défense d'un **droit en justice**

Etudes conduites à partir des données recueillies lors du suivi médical ou individuel par les personnels assurant ce suivi et pour leur usage exclusif (« **étude interne** »)

Traitements mis en œuvre pour l'exercice de leurs missions par les **organismes chargés de la gestion d'un régime de base d'assurance maladie** ainsi que la **prise en charge des prestations par les organismes d'assurance maladie complémentaire**

**Médecins responsables de l'information médicale** (DIM) dans les établissements de santé pour leurs missions

Traitements effectués par les **ARS et par l'Etat sur l'activité des établissements de santé**

Traitements mis en œuvre par **l'Etat** aux fins de **conception, de suivi ou d'évaluation des politiques publiques** dans le domaine de la santé ainsi que ceux réalisés aux fins de collecte, d'exploitation et de diffusion des statistiques dans ce domaine.

# Check-list des questions à se poser (pour tout traitement de données de santé)

## Sur la collecte des données

- 1) Quel est l'**objectif** (finalité) de mon traitement ?
- 2) Cette finalité est-elle **déterminée, explicite et légitime** ?
- 3) Quelle est la **base légale du traitement** ?
- 4) A quel titre puis-je **déroger au principe d'interdiction de la collecte des données de santé** ?
- 5) Les données collectées sont-elles **adéquates, pertinentes et nécessaires** au regard de la finalité du traitement ?
- 6) Les données collectées sont-elles **exactes et mises à jour** ?
- 7) Le patient est-il **informé** au moment de la collecte et peut-il exercer ses droits ?
- 8) La **durée de conservation** des données est-elle adaptée à la finalité du traitement ?
- 9) Des **mesures de sécurité** sont-elles mises en place pour garantir l'intégrité et la confidentialité des données ?
- 10) Le traitement est-il dans le **périmètre de la section 3 de la LIL** ?
- 11) Si je souhaite mener un projet de recherche, quelle est la qualification de mon étude? S'il s'agit d'une recherche n'impliquant pas la personne humaine, je vérifie qu'il ne s'agit pas d'une étude interne.
- 12) Mon traitement est-il conforme à un référentiel homologué par la CNIL?

## Sur l'échange/partage des données

- 1) Le patient est-il bien **informé** en amont du partage/de l'échange de ses données ?
- 2) Ce partage intervient-il dans le cadre de **l'équipe de soins** ou **en dehors de celle-ci** ?
- 3) Le partage / l'échange des données est-il **licite** ?
- 4) Les personnes sont-elles bien **autorisées à accéder** aux données de santé du patient ?
- 5) Une procédure de **gestion des habilitations et des accès** est-elle mise en place ?
- 6) Les professionnels de santé utilisent-ils la **messagerie sécurisée** pour échanger entre eux ?

Toutes les questions résultant de l'application des dispositions du code de la santé publique (identifiant national de santé, référentiels de sécurité, HDS, ...).

Véronique CABANES et Manon de FALLOIS



# La détermination de la formalité applicable

# Les formalités pour les traitements de données de santé

## Demande d'autorisation

- Pour les traitements présentant une **finalité d'intérêt public** (ex: entrepôt, etc.)
- Pour les traitements à des fins de **recherche, d'étude ou d'évaluation** dans le domaine de la santé

**Décision unique** : même demandeur, même finalité , catégories de données identiques, catégories de destinataires identiques

## Demande d'avis sur un **projet d'acte réglementaire** autorisant un traitement de données de santé

# Quelle démarche effectuer?

|                           | <u>Hors</u> section 3  | Section 3  |
|---------------------------|--|--|
| <b>Formalité</b>          | <b>Aucune formalité</b>  | <b>Conformité à un référentiel</b><br>(engagement de conformité auprès de la CNIL)<br><u>OU</u><br><b>Demande d'autorisation</b> auprès de la CNIL |
| <b>Responsabilisation</b> | Inscription du traitement dans le <b>registre</b> du RT  | Inscription du traitement dans le <b>registre</b> du RT  |
|                           | Documentation de la conformité du traitement (AIPD, etc.).   | Documentation de la conformité du traitement (AIPD, etc.).   |
|                           | S'appuyer sur les <b>référentiels sectoriels</b> pour la mise en conformité (grille de bonnes pratiques) | Respect du référentiel le cas échéant  |

Pour en savoir plus : fiche pratique « *Quelles formalités pour les traitements de données de santé à caractère personnel ?* » sur [cnil.fr](http://cnil.fr)

## Comment mettre en œuvre le RGPD dans la pratique ?

### ILLUSTRATIONS

# La tenue des dossiers médicaux

---



Les dossiers **papiers** ou du **logiciel** médico-administratif doivent répondre à des **finalités déterminées, explicites et légitimes**



Les données collectées doivent être adéquates, pertinentes et limitées à **ce qui est nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostic et de soins**



Les données collectées sur les patients doivent être conservées pour une durée **qui n'excède pas la durée nécessaire à leur utilisation.**



**Informez les patients** de l'existence des dossiers et de leurs droits



Prendre toutes les précautions utiles pour **empêcher que des tiers non autorisés** aient accès aux données de santé

# Les entrepôts de données de santé

---



Entrepôts de données créés principalement pour collecter et disposer de **données massives**



Les données sont ensuite **réutilisées**, principalement à des fins **d'études, de recherches et d'évaluations** dans le domaine de la santé



Information **individuelle** complète, claire et lisible



Consentement **explicite** des personnes concernées pour la **constitution de l'entrepôt** de données ?

*Oui* : aucune formalité; *Non*: demande d'autorisation auprès de la CNIL.



Réalisation d'une **AIPD**

Pour en savoir plus : fiche pratique « **Comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?** » sur [cnil.fr](https://www.cnil.fr)

# Recherche en santé : les thèses et les mémoires

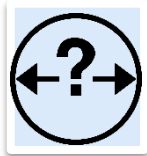
**Attention:** recherche en santé = régime spécifique

Pour aller plus loin



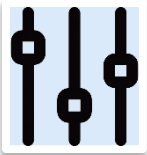
## 1. Identifier la nature de la recherche

- Recherche impliquant la personne humaine
- Recherche n'impliquant pas la personne humaine



## 2. Identifier le périmètre de la recherche

- Recherche interne
- Recherche multicentrique



## 3. Procéder aux ajustements nécessaires

Avant la mise en œuvre de l'étude, il est nécessaire de corriger les points de non-conformité. Une attention particulière doit être apportée à l'information et à la sécurité des données.



## 4. Réaliser les démarches

Les démarches (autorisation CNIL, saisine comité éthique, etc.) varient en fonction de la nature (étape 1) et du périmètre (étape 2) de la recherche.

2 fiches pratiques dans la rubrique santé (cnil.fr)  
- « [Recherche en santé : quel est le cadre légal ?](#) »  
- « [Comment procéder pour une thèse ou un mémoire ?](#) »



**Bonne pratique :** prévoir en interne des procédures pour faciliter l'instruction des dossiers « recherche »



Comment mettre en œuvre le RGPD dans la pratique ?

## **LES OUTILS POUR VOUS AIDER**

# Pour se former

## Formation en ligne « L'atelier RGPD »

The screenshot shows a digital learning environment. At the top, a header reads 'MODULE 3 : LES RESPONSABILITES DES ACTEURS'. Below this, a question is posed: 'Le responsable de traitement d'une société doit-il obligatoirement communiquer le registre de sa société si une personne le lui demande?'. Two buttons, 'Oui' and 'Non', are provided for selection. A 'Valider' button is at the bottom. The interface also displays 'Module 4 : le DPO et les outils de la conformité' with a sub-unit 'Unité 1 : Le délégué à la protection des données'.

## Guides et fiches thématiques

A collage of three documents. The first is titled 'Télémedecine : comment protéger les données de santé?' and discusses the specific challenges of remote medical services. The second is 'Groupement hospitalier de territoire et protection des données de santé', focusing on data protection in hospital networks. The third is 'Qu'est-ce qu'une donnée de santé?', providing a clear definition and context for health data under the GDPR.

## Ateliers

The screenshot shows an 'Agenda' page with social media icons for Facebook and Twitter. A navigation bar includes 'Tous', 'Sessions plénières', 'Formation restreinte', 'Evénements', and 'Conférences'. A section titled '1 évènement à venir' features a card for an event on '09 DÉCEMBRE 2019' at 'Palais d'Ile de France, Paris - r1hp'. The event is organized by CNIL and focuses on reflection around the theme 'Les clubs tech bouillonnent-ils vraiment la démocratie?'.

# Pour se renseigner

**Besoin d'aide**

**Posez votre question, la CNIL vous répond**

Vous recherchez une information ? Les questions les plus fréquemment posées sont recensées ici question dans l'encadré ci-dessous, notre système vous transmettra les questions-réponses en lien avec votre problématique.


Rechercher dans notre base de réponses

nos questions fréquentes

**QUESTIONS FRÉQUENTES**

- RGPD règlement européen : faut-il encore effectuer des déclarations à la CNIL ?
- RGPD règlement européen sur la protection des données : que faut-il savoir ?
- RGPD régime de sécurité sociale des enfants en école primaire : une mairie peut-elle le demander ?
- RGPD droit d'accès, c'est quoi ?
- RGPD FICBA (Fichier national des comptes bancaires et assimilés) : les héritiers peuvent-ils identifier les

**Rubrique « Besoin d'aide » : + 500 Q/R**

 **CNIL**  
COMMISSION NATIONALE  
INFORMATIQUE & LIBERTÉ

**GUIDE PRATIQUE SUR  
LA PROTECTION  
DES DONNÉES PERSONNELLES**

ÉDITION JUIN 2018

**Fiches pratiques et guides (rubrique « Santé » + Guide sécurité)**



**Votre réseau sectoriel (homologues, fédérations, etc.)**

# Les sources d'informations disponibles

---

- **Site web de la CNIL - Fiches pratiques :**
  - Thématique santé : données de santé, télémédecine, recherche, formalités ...
  - Rubrique ma conformité au RGPD : RGPD par ou commencer, etc.
  - Rubrique besoin d'aide
- **Site web de la CNIL - Outils à disposition des acteurs :**
  - Logiciel « Analyse d'impact », modèle de « registre d'activités de traitements », infographie, MOOC, etc.
- **Services de la CNIL : Possibilité d'adresser une demande de conseil par courrier**
- **Charte d'accompagnement des professionnels**

# Les lignes directrices de la CNIL et du CEPD

---

- **Les lignes directrices de la CNIL :**
  - [Lignes directrices sur les analyses d'impact relatives à la protection des données \(AIPD\) prévues par le règlement général sur la protection des données \(RGPD\)](#)
  - [Lignes directrices sur les AIPD obligatoires ou non obligatoires](#)
- **Les lignes directrices endossées par le Comité Européen de la Protection des Données (CEPD)**
  - [Lignes directrices concernant l'analyse d'impact relative à la protection des données \(AIPD\) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement \(UE\)2016/679](#)
  - [Lignes directrices sur la transparence au sens du règlement \(UE\) 2016/679](#)
  - [Lignes directrices concernant les délégués à la protection des données \(DPD\)](#)
  - A venir : Lignes directrices sur la recherche scientifique

# Les guides spécifiques

---

- **Les guides :**
  - [Référentiel des durées de conservation dans le domaine de la santé hors recherche](#)
  - [Référentiel des durées de conservation dans le domaine de la recherche en santé](#)
  - [Référentiel pour la gestion des traitements courants des cabinets médicaux et paramédicaux](#)
  
  - A venir : Référentiel pharmacies d'officine, référentiel opticien lunetier / audioprothésiste
  
  - [Guide sur les modalités de circulation du NIR pour la recherche en santé aux fins d'appariement de données avec le SNDS](#)
  - [Guide pratique sur les durées de conservation](#)
  - [Guide du sous-traitant](#)
  - [Guide pratique sur les mesures de sécurité élémentaires à mettre en œuvre](#)

# Les référentiels spécifiques

---

- **Les référentiels relatifs à des traitements soumis à autorisation (déclaration de conformité) :**
  - [Référentiel pour la gestion des vigilances sanitaires](#)
  - [Méthodologies de référence \(recherche médicale - MR 001 à MR 006\)](#)
  - A venir : Référentiel entrepôt de données de santé
  - Mise à jour du référentiel (AU 41) relatif aux ATU et RTU
  - Mise à jour des méthodologies de référence (MR 002; MR 005; MR 006)

# Pour poser une question

Par téléphone au 01 53 73 22 22

---

## Permanence juridique

- Du lundi au vendredi (sauf le mercredi)
- De 10h à 12h et de 14h à 16h

## Permanence santé

- Tous les jeudis de 14h30 à 16h30

## Permanence DPO

- Du lundi au vendredi (sauf le mercredi)
- De 10h à 12h

Merci de votre attention !