02

3 Notions Clés

S

Donnée personnelle

- Personne physique
- Sauf donnée « domestique »

Traitement

- Manipulation
- De la collecte à la suppression

Responsable de Traitement

- Détermine l'usage de la donnée

03

Règles des textes relatifs à la protections des données personnelles : Les apports du RUE 2016/679 (RGDP)

Avant le règlement UE 2016/679 du 27 avril 2016

- Directive 95/46, concerne les traitements de données à caractère personnel
- Transposée en France en 2004 dans la loi Informatique et Libertés du 6 Janvier 1978

Le règlement UE 2016/679 du 27 avril 2016

- Un texte qui remplace la directive 95/46 et va impacter la loi Informatique et Libertés
- Un texte européen, commun à tous les EM et directement applicable en France (pas de transposition nécessaire)
- Un texte applicable dès le 25 mai 2018
- Un texte qui concerne toutes les entreprises ainsi que le secteur public
- pour tous les traitements de données à caractère personnel localisés en Europe ou concernant des citoyens européens

04

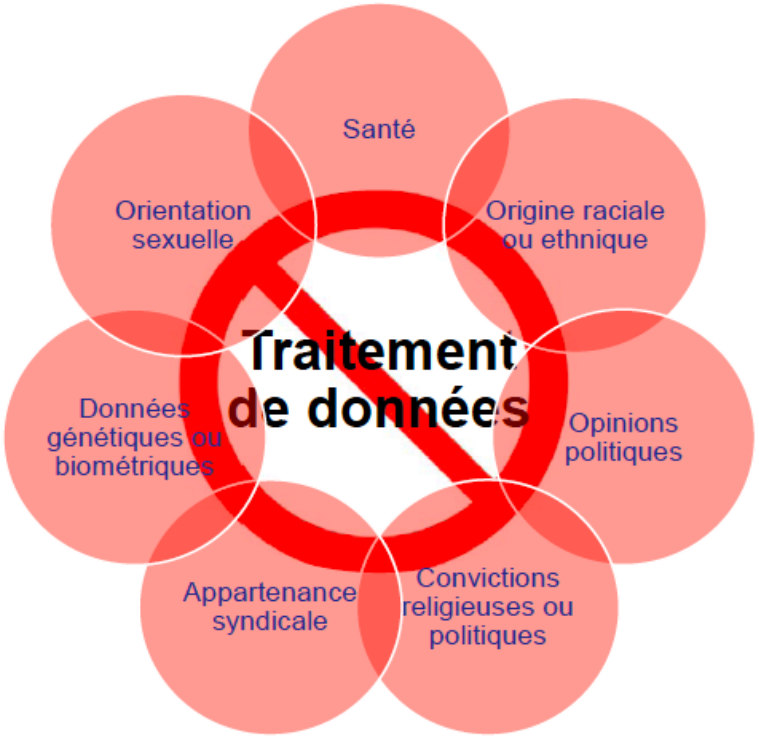
Données personnelles

Toute information de quelque nature qu'elle soit et indépendamment de son support concernant une personne DIRECTEMENT ou INDIRECTEMENT identifiée ou identifiable

- Nom, prénom, date de naissance
- Son, image
- Données électroniques
- Numéro d'identification
- Origine culturelle, sociale ou économique
- Données judicaires
- Données de santé
- Données biométries
- …..

05

Données sensibles



PRINCIPE
INTERDICTION DE TRAITEMENT
SAUF
EXCEPTIONS
VISÉES PAR LE RGPD (ARTICLE 9)

06

Les données personnelles : grands principes

07

Données de santé (article RGPD)

- Ensemble de données se rapportant à/révélant l'état de santé physique/ mental passé, présent ou futur
- Données génétiques = données santé particulière
- Données biométriques différents données de santé

- Données collectées lors de l'inscription en vue de soins de santé
- Numéro ou éléments spécifiques attribués pour l'identification unique à des fins de santé
- Informations obtenues lors de tests ou examens y compris à partir de données génétiques et d'échantillons biologiques
- Toute information sur maladie, handicap, risque de maladie, antécédents médicaux, traitements clinique ou état physiologique ou biomédical indépendamment de la source

08

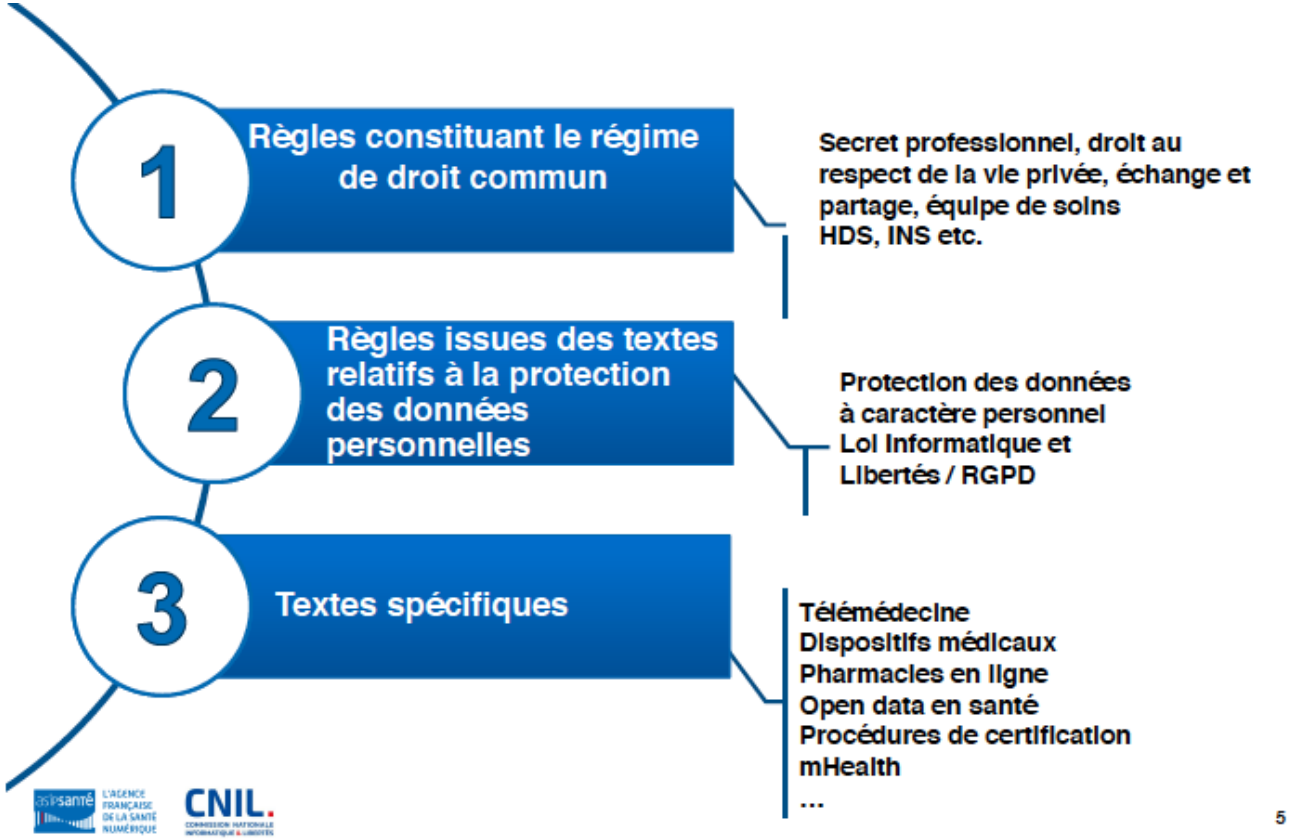
Focus sur les données de santé à caractère personnel

Les risques

- Confidentialité
- Discrimination
- Défaut de validation clinique
- Exploitation commerciale
- Failles de sécurité
- Manque de fiabilité de capteurs
- Impact sur le secret médical

09

Cadre juridique de la e-santé



Traitement des données

Toute opération ou ensemble d'opération effectuées ou non à l'aide de procédés automatisés et appliquées à des données

- Collecte
- Organisation
- Adaptation
- Extraction
- Utilisation
- Rapprochement
- Verrouillage
- Communication par transmission
- enregistrement
- conservation
- modification
- consultation
- Diffusion
- interconnexion
- effacement
- Destruction

2 grands principes du traitement des données

Anonymisation

- Empêche irréversiblement l'identification de la personne concernée
- Ré-identification impossible ou extrêmement compliquée

Pseudonymisation

- Empêche réversiblement l'identification de la personne concernée
- Ré-identification possible au moyen d'autres informations conservées séparément et soumises à des garanties fortes

Responsable du traitement RGPD

- Personne physique ou morale, autorité publique, service ou tout autre organisme qui seul ou conjointement avec d'autres détermine les finalités ou moyens de traitement
- Il est crucial de bien identifier le responsable
- Pluralité du responsable
- Parfois plusieurs scénarii possibles

→ Délégué à la protection des données (DPO) obligatoire - Art 37 RGPD

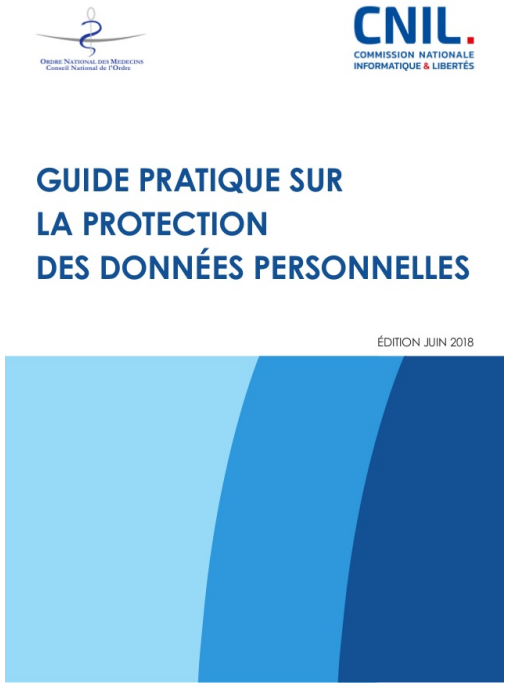
Sous - traitant

- Personne physique ou morale, autorité publique, service ou tout autre organisme qui traite les données pour le compte du responsable du traitement
- Ne pas confondre avec le responsable du traitement
- Obligation d'avoir un contrat de sous-traitance écrit contenant les clauses imposées par la loi

Nouvelles responsabilités reposant sur le responsable du traitement (RT)

RGPD
Accountability mesures de protection des données appropriés pour démontrer leur conformité à tout moment
Privacy by design/ Privacy by default garantir que les traitements de données ne portent pas atteinte à la vie privée dès la conception
Privacy Impact Assessment Obligation, pour les RT d'effectuer une **analyse d'Impact** relative à la protection des données préalablement aux traitements présentant des risques.
Data Protection Officer Rendu obligatoire dans certains cas

RGPD : en pratique pourquoi vous êtes concernés ?



- Quel cadre appliquer aux dossiers patients?
- Quel cadre appliquer à la prise de rendez –vous?
- Quel cadre appliquer à l'utilisation de la messagerie électronique?
- Quel cadre appliquer aux téléphones portables et aux tablettes?
- Quel cadre appliquer aux recherches?
- Quel cadre appliquer à la télémedecine?

16

Quel cadre appliquer aux dossiers patients ?

- Informations collectées pour activité de prévention, diagnostic, et de soins et qui servent à gérer votre cabinet

- Sont concernés
  - gestion des rendez-vous
  - La gestion des dossiers médicaux
  - Editions des ordonnances
  - Envoie des courriers aux confrères
  - Etablissement et la transmission des feuilles de soins

- Toute utilisation informations collectées à visée personnelle ou commerciales dans vos dossier est prohibée

Quel cadre appliquer aux dossier patient ?

Durée de conservation des données

- 20 ans à compter de la date de la dernière consultation du patient ;
- si le patient est mineur et que ce délai de 20 ans expire avant son 28ème anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date ;
- dans tous les cas, si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à compter de la date du décès ;
- en cas d'action tendant à mettre en cause la responsabilité du médecin, il convient de suspendre ces délais de conservation.

Les doubles des feuilles de soins doivent être conservés 3 mois.

Quel cadre appliquer aux dossier patient ?

Modèle feuille d'information salle d'attente

« Votre médecin, le Dr. XX, [adresse], est amené à recueillir et à conserver dans un dossier, [votre dossier patient], des informations sur votre état de santé.

Pourquoi votre médecin tient-il un dossier sur vous ?
La tenue du dossier « patient » est obligatoire. Ce dossier a pour finalité d'assurer votre suivi médical et de vous garantir la prise en charge la plus adaptée à votre état de santé. Il garantit la continuité de la prise en charge sanitaire et répond à l'exigence de délivrer des soins appropriés.

Quelle est sa durée de conservation ?
Il est conservé en principe pendant 20 ans à compter de la date de votre dernière consultation, par référence aux dispositions de l'article R. 1112-7 du code de la santé publique applicables aux établissements de santé.

[Dans le cas d'un logiciel hébergé par un prestataire] *Votre dossier est hébergé sur les serveurs de XXX, qui dispose d'un agrément / d'une certification délivrée en application des dispositions de l'article L.1111-8 du code de la santé publique. Le Dr. XX, [adresse], présent chez l'hébergeur est garant de la confidentialité des données de santé. Vous pouvez vous opposer à l'externalisation de vos données soit en contactant directement votre médecin soit en contactant directement l'hébergeur de données de santé par courrier postal ou à l'adresse électronique / xxxx@xxx.com.*

Quels sont les destinataires des informations figurant dans votre dossier ?
Seuls ont accès aux informations figurant dans votre dossier votre médecin et, dans une certaine mesure, au regard de la nature des missions qu'il exerce, son personnel. Votre médecin, avec votre consentement, pourra également transmettre à d'autres professionnels de santé des informations concernant votre état de santé. Enfin, afin de permettre la facturation des actes qu'il réalise, votre médecin est amené à télétransmettre des feuilles de soins à votre caisse de sécurité sociale.

Quels sont vos droits et comment les exercer ?
Vous pouvez accéder aux informations figurant dans votre dossier. Vous disposez, par ailleurs, sous certaines conditions, d'un droit de rectification, d'effacement de ces informations, ou du droit de vous opposer ou de limiter leur utilisation.

Pour toute question relative à la protection de vos données ou pour exercer vos droits, vous pouvez vous adresser directement à votre médecin. En cas de difficultés, vous pouvez également saisir la Commission nationale de l'informatique et des libertés (CNIL) d'une réclamation. »

Ordre National des Médecins
Conseil National de l'Ordre

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Quel cadre appliquer aux dossier patient ?

Modèle feuille d'information salle d'attente

A PROPOS DE LA PROTECTION DE VOS DONNEES PERSONNELLES,

VOTRE MEDECIN VOUS INFORME

La loi reconnait la protection de vos données personnelles.

Votre médecin est tenu par la loi au secret professionnel, sauf cas d'exception légale (maltraitance…)

Lorsque vous consultez un médecin, il recueille, pour l'accomplissement de sa mission, vos données personnelles, consigne ses observations et prescriptions dans votre dossier médical couvert par le secret professionnel.

La loi vous reconnait le droit personnel :

- d'accéder à ce dossier et d'en obtenir une copie,
- de compléter les informations y figurant,
- de demander la rectification des informations inexactes,
- de demander leur effacement dès lors que celles-ci ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été données et à l'expiration du délai de conservation de votre dossier médical auquel est légalement tenu votre médecin
- le droit à la portabilité

Votre médecin a mis en place les mesures nécessaires notamment au plan de la sécurité informatique pour satisfaire à la réglementation applicable à la protection de vos données personnelles.

Votre médecin reste bien évidemment à votre disposition pour toute précision complémentaire.

CSMF
Confédération des Syndicats Médicaux Français

Quel cadre appliquer aux dossier patient ?

Sécurisation du système informatique

- Utilisation mot de passe conforme recommandations CNIL : 12 caractères (chiffre, lettres majuscules, minuscules, caractères spéciaux) renouvelé régulièrement
- Verrouillage de votre session informatique automatiquement après 30 mn max d'inactivité
- Antivirus à jour, pare-feu, application systématiques de correctifs de sécurité du systèmes informatique et des logiciels
- Sauvegarde régulière des données (au minimum hebdomadaire , avec conservation sauvegarde mensuelles sur 12 mois glissants) et leur conservations dans un lieu différents de votre cabinet.
- Chiffrement des données avec logiciel adapté
- Absence ou minimisation des connections d'appareils non professionnels sur le réseau
- Authentification via votre CPS ou tout moyen alternatif d'authentification forte

Quel cadre appliquer aux dossier patient ?

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Société (si DPO externe) :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliquez ici.

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects
Activité 3	Cliquez ici. ex. Gestion des fournisseurs
Activité 4	Cliquez ici. ex. Vente en ligne
Activité 5	Cliquez ici. ex. Sécurisation des locaux
Activité 6	Cliquez ici.
Activité 7	Cliquez ici.
Activité 8	Cliquez ici.

Vous devrez créer et tenir à jour une fiche de registre par activité.
Le modèle de fiche de registre est disponible sur la page suivante, copier / coller autant de fois la sélection qu'il y a d'activité listée.

16

Quel cadre appliquer aux dossier patient ?

Check-list des bonnes pratiques à respecter :

→ Je limite les informations collectées au nécessaire et j'utilise les dossiers patients conformément aux finalités définies (suivi des patients) ;

→ Je tiens un registre à jour de mes « traitements » (voir annexe n° 2 « Registre des activités de traitement) ;

→ Je supprime les dossiers patients et de manière générale toute information ayant dépassé la durée de conservation préconisée ;

→ Je mets en place les mesures appropriées de sécurité de mes dossiers « patients » ;

→ J'informe mes patients et m'assure du respect de leurs droits (voir l'annexe n° 1 « Exemple de notice d'information »).

17

Quel cadre appliquer à la prise de rendez-vous ?

6 RÈGLES D'OR DU TRAITEMENT DE DONNÉES RGPD ART. 5

Check-list des bonnes pratiques à respecter :

→ Je limite les informations collectées par le prestataire et vérifie la conformité du prestataire avec la réglementation et notamment la présence des mentions obligatoires dans le contrat de sous-traitance que je passe avec lui ;

→ Je tiens un registre à jour de mes « traitements » (voir annexe n° 2 « Registre des activités de traitement ») ;

→ J'informe mes patients et m'assure du respect de leurs droits (voir l'annexe n° 1 « Exemple de notice d'information »).

Quel cadre appliquer à la prise de rendez-vous ?

- Contrat de sous traitance / Bien vérifier avant signature
  - Ne traite les données à caractère personnel que sur votre instruction
  - Veille à la signature d'engagement de confidentialité par le personnel
  - Prend toute les mesures de sécurité requises
  - Ne recrute pas de sous traitant sans votre autorisation écrite préalable
  - Coopère avec vous pour le respect de vos obligations en tant que responsable du traitement, notamment lorsque les patients ont des demandes concernant leurs données
  - Supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations
  - Collabore dans le cadre d'audits

Si le prestataire héberge les données → hébergeur de données de santé agréé

Quel cadre appliquer à l'utilisation des messageries électroniques ?

6 RÈGLES D'OR DU TRAITEMENT DE DONNÉES RGPD ART. 5

Check-list des bonnes pratiques à respecter :

→ J'utilise un service de messagerie sécurisée de santé pour mes échanges avec d'autres professionnels de santé ;

→ Si j'utilise une messagerie électronique standard ou des messageries instantanées, je m'assure que ces messageries sont bien sécurisées et adaptées à mon utilisation professionnelle ;

→ Je chiffre les pièces jointes lorsque j'utilise des messageries standard sur internet qui ne garantissent pas la confidentialité des messages.

Quel cadre appliquer aux téléphones portables et tablettes ?

6 RÈGLES D'OR DU TRAITEMENT DE DONNÉES RGPD ART. 5

Check-list des bonnes pratiques à respecter :

→ Je sécurise l'accès à mon téléphone ou à ma tablette et à son contenu (mot de passe, chiffrement, etc.)

→ Je ne stocke pas d'informations médicales relatives à mes patients sur mon téléphone portable ou ma tablette ;

→ Je m'assure que l'accès à mon logiciel de dossiers « patients » sur mon téléphone portable ou ma tablette est sécurisé ;

→ Je consulte mon logiciel de dossiers « patients » avec précaution.

Quel cadre appliquer aux recherches ?

6 RÈGLES D'OR DU TRAITEMENT DE DONNÉES RGPD ART

Check-list des bonnes pratiques à respecter :

→ Je réalise une analyse d'impact avant la réalisation d'études internes sur les données de mes patients si le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ;

→ Dans le cadre de recherches en partenariat avec un tiers, je m'assure que les recherches sont menées conformément à la réglementation ;

→ Je tiens à jour le registre des activités de traitement (voir annexe n° 2 « Registre des activités de traitement ») ;

→ J'informe mes patients et m'assure du respect de leurs droits (voir annexe n° 1 « Notice d'information »).

Quel cadre appliquer à la télémédecine ?

- Définition
- Cadre légal / règles déontologiques
- Règles de droit commun de facturation / paiement en ligne

Check-list des bonnes pratiques à respecter :

→ Je m'assure que le prestataire de télémédecine choisi est bien conforme avec la réglementation ;

→ Je vérifie la présence des mentions obligatoires dans son contrat.

→ Je contrôle que le patient a bien été informé ;

- Contrat de sous traitance
- Hébergeur de données de santé agréé

Conclusion RGPD

- Définition européenne de la données de santé
- Allègement des procédures administratives préalables au traitement des données à caractères personnelles de santé
- Renforce les obligations en terme de droit des personnes, de sécurité et de confidentialité
- Responsabilisation accrue des acteurs

Les Assises
de la Pneumologie
Libérale

Merci pour votre attention

https://www.facebook.com/APLiberale/ https://twitter.com/apliberale https://www.linkedin.com/company/aplib

#APLib

www.ap-lib.com


JOURNEES PRATIQUES
JPRS
RESPIRATION SOMMEIL
Save the date !
11ème édition
12 au 14 Mars 2020
Au Pharo à MARSEILLE
FFP
Fédération Française de Pneumologie
facebook.com/JPRSommeil
twitter.com/JPRSommeil
www.jprs.fr