

Vos obligations RGPD L'essentiel



Ramsay
Santé

Sommaire

03



Introduction

04
06

Qu'est-ce que le RGPD ?
Pourquoi ce guide ?

07



Définitions

08

Données personnelles
Données sensibles
Données de santé

09

Traitement de données
Responsable de traitement
Sous-traitant

10

Finalité
Base légale (ou base de licéité)
Proportionnalité / Minimisation
Personne concernée

11

Analyse d'impact sur la Protection des Données
Violation de données

12

Droit des personnes

13



Obligations

13

Documentation

15

Information des personnes

16

Deux principes gouvernent la mise en place
des traitements de données :

17

La sécurisation des traitements
Le respect et la gestion des droits des personnes

18

La gestion des violations de données

19

Encadrement de la sous-traitance

20



En pratique

21

Dossiers patients

22

La prise de rendez-vous

23

Messagerie électronique
Tablettes et téléphones portables

24

Recherches

25

Télémédecine

Introduction



Qu'est-ce que le RGPD ?

Règlement Général sur la Protection des Données

Texte européen d'applicabilité directe dans les Etats membres

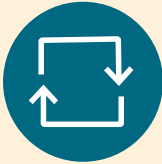
Contexte d'adoption :

- ➔ Un cadre juridique antérieur insuffisant (loi Informatique & Libertés de 1978)
- ➔ Une explosion de la quantité de données produites
- ➔ De nouveaux supports des données : dossiers informatisés, réseaux sociaux, etc., qui constituent de nouvelles pratiques à encadrer.





Entrée en application
25 mai 2018



Principaux changements

Renforcement des **droits des personnes**

Renforcement des **obligations des organismes**

Abandon des formalités déclaratives préalables auprès de la CNIL (sauf exceptions dont recherches médicales) au profit de la mise en place d'une **conformité en interne**

Changement de logique : il appartient à chaque responsable de traitement de **démontrer sa conformité à tout moment**



Autorité de contrôle

La Commission Nationale de l'Informatique et des Libertés (CNIL) : chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, publics comme privés. C'est une autorité administrative indépendante disposant d'un rôle d'alerte, de conseil et d'information, mais également d'un pouvoir de contrôle et de sanction.



Enjeux

- ➔ Renforcement des exigences des personnes sur leurs données
- ➔ Risque de sanction : Les sanctions potentielles en cas de non-conformité sont très importantes : 20 millions d'euros ou 4% du CA annuel mondial. Il faut aussi tenir compte de l'atteinte à l'image en cas de condamnation.



Pourquoi ce guide ?



Application à l'exercice libéral



Dans le cadre de votre exercice, vous **traitez des données à caractère personnel** (dossiers patients, secrétariat, gestion des rendez-vous, télémedecine, etc.).

Pour tous ces traitements de données, tous les praticiens libéraux et cabinets médicaux sont concernés par le RGPD : chaque structure a l'obligation d'entreprendre une démarche de mise en conformité. La sensibilité particulière des données médicales rend indispensable une bonne prise en compte de ce règlement.



Ce document a pour objectif de vous présenter les concepts du Règlement, de décrire les obligations qui vous sont faites et de vous orienter dans **la mise en œuvre de la démarche de conformité exigée** par la réglementation.



Pour tous ces traitements de données, tous les praticiens libéraux et cabinets médicaux sont concernés par le RGPD : chaque structure a l'obligation d'entreprendre une démarche de mise en conformité. La sensibilité particulière des données médicales rend indispensable une bonne prise en compte de ce règlement.

Définitions



Définitions



Données personnelles (données à caractère personnel)

Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, sous format papier ou numérique.

- **Identifiantes** (*M. François Martin – Monsieur le directeur de la clinique X/Y*)
- **Quasi-identifiantes** (*adresse mail, adresse IP, immatriculation véhicule, photo, IPP patient, NIR sécurité sociale*)
- **Données rattachées** (*caractéristiques : « glycémie = 1,2 », etc.*)



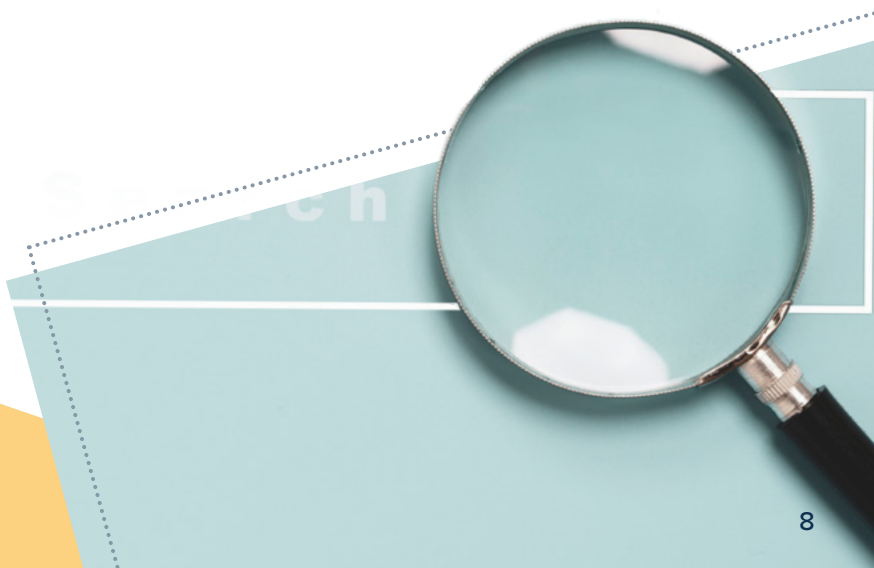
Données sensibles

Il s'agit des données de santé, religieuses, syndicales, politiques, sur l'orientation sexuelle, philosophiques : par défaut interdites de collecte sauf autorisation explicite par la loi.



Données de santé

Il s'agit des données 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.



Définitions



Traitement de données

Toute opération appliquée à des données à caractère personnel.
collecter, ordonner, structurer, organiser, traiter, exploiter, diffuser, partager, archiver, effacer, etc.



Responsable de traitement

Il s'agit de la personne morale ou physique qui définit la finalité et les moyens d'un traitement de données et porte la responsabilité juridique de la conformité pour son organisme (cabinet, clinique, GIE).



Sous-traitant

Il s'agit d'une personne morale ou physique qui réalise tout ou partie d'un traitement de données pour le compte du responsable de traitement via un contrat ou équivalent.



Ex : Hébergeur informatique, fournisseur, archiveur de dossiers papiers, ...



Finalité

Il s'agit du but du traitement de données. Elle doit être clairement identifiée et les données traitées pour sa réalisation ne peuvent pas être utilisées dans d'autres buts, sous peine de constituer un détournement de finalité, sanctionné par le RGPD.



Par exemple, les coordonnées des employés utilisées pour la gestion des absences ne peuvent pas être utilisées pour envoyer des offres commerciales.



Définitions



Base légale (ou base de licéité)

Il s'agit du fondement qui autorise légalement la mise en œuvre d'un traitement et qui donne le droit à un responsable de traiter des données à caractère personnel.

Six bases légales sont prévues par le RGPD :

- Le consentement de la personne: acte positif, explicite, clair ;
- Le contrat (travail, prestation) ;
- L'obligation légale du responsable de traitement (code de la santé, ...) ;
- La sauvegarde des intérêts vitaux de la personne ;
- L'intérêt public ;
- L'intérêt légitime du responsable de traitement.



Proportionnalité / Minimisation

Ce principe signifie que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.



Personne concernée

Toute personne dont les données sont traitées par un organisme.



Définitions



Analyse d'impact sur la Protection des Données

Il s'agit d'une étude devant être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.



Violation de données

Il s'agit de tout incident de sécurité, d'origine malveillante ou non / intentionnelle ou non, ayant comme conséquence de compromettre la confidentialité, l'intégrité ou la disponibilité des données personnelles.

C'est lorsque des données personnelles sont de manière accidentelle ou illicite : détruites, perdues, altérées, divulguées, indisponibles ou consultées par une personne non-autorisée.





Définitions

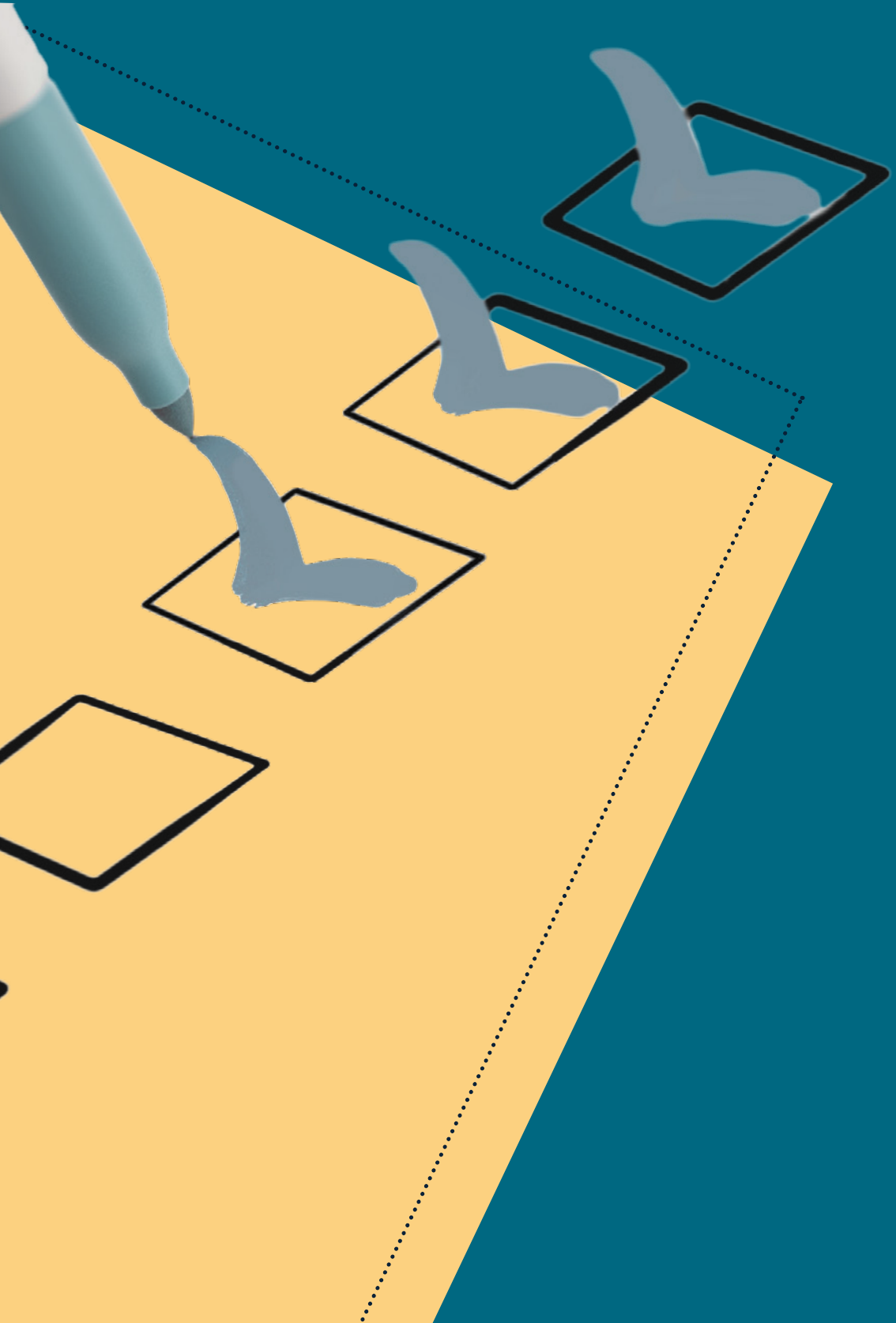


Droit des personnes

Les personnes concernées par des traitements disposent de droits sur leurs données :

- **Droit à l'information** : Les personnes concernées doivent être informées des caractéristiques du traitement, de manière claire et précise, au moment de la collecte de leurs données.
- **Droit d'accès** : Toute personne peut accéder à l'ensemble des informations la concernant, à leur origine, et en demander la copie.
- **Droit de rectification** : Toute personne peut exiger que ses données soient, selon les cas, rectifiées, complétées ou mises à jour.
- **Droit à l'effacement** : Toute personne peut demander la suppression des données la concernant détenues par un responsable de traitement.
- **Droit d'opposition** :
 1. Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf si celui-ci répond à une obligation légale.
 2. Les personnes doivent pouvoir s'opposer à la réutilisation par le responsable du fichier de leurs coordonnées à des fins de sollicitations (notamment commerciales) lors d'une commande ou de la signature d'un contrat.
- **Droit à la limitation** : Il s'agit pour une personne de demander à un organisme l'arrêt du traitement d'une donnée la concernant (le temps d'obtenir sa rectification ou d'exercer un droit par exemple).
- **Droit à la portabilité** : Toute personne a le droit de recevoir les données qui la concerne et qu'elle a fournies à un responsable de traitement, de les réutiliser, et de les transmettre à un autre responsable de traitement.

Obligations



Obligations



Documentation

Afin de prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire, notamment un registre de vos activités de traitement, inventaire et descriptif détaillé de vos activités.

Il doit contenir, pour chaque traitement :

- ➔ Une description de sa finalité ;
- ➔ Les responsabilités associées au traitement ;
- ➔ La base de licéité du traitement ;
- ➔ Les supports des données et détail des applications utilisées ;
- ➔ Les catégories et le détail des données traitées ;
- ➔ Les destinataires des données ;
- ➔ Les personnes concernées par le traitement ;
- ➔ Les durées de conservation prévues pour les données ;
- ➔ Les mesures de sécurité techniques et organisationnelles mises en place.

Obligations



Information des personnes

Toute personne concernée doit recevoir une **information concise, compréhensible et aisément accessible** sur le traitement de données. L'information doit comprendre notamment :

- ➔ L'identité et les coordonnées du Responsable de traitement ;
- ➔ La finalité du traitement ;
- ➔ Les données traitées, et le caractère obligatoire ou facultatif de leur collecte
- ➔ Les destinataires des données ;
- ➔ La base légale du traitement ;
- ➔ La durée de conservation des données ;
- ➔ Les droits dont les personnes disposent ;
- ➔ Le droit d'introduire une réclamation auprès de la CNIL.

Obligations

Deux principes gouvernent la mise en place des traitements de données :



La protection des données personnelles par défaut
Pour tout traitement et par principe, il faut minimiser :

- L'étendue de leur collecte (strict nécessaire pour la réalisation de la finalité)
- Leur durée de conservation
- Leur accessibilité



La protection des données personnelles dès leur conception

Il faut démontrer (dans la conception d'un outil, la mise en place d'un traitement) :

- L'existence de mesures de sécurité techniques et organisationnelles
- La minimisation des données
- Une documentation transparente

Obligations



La sécurisation des traitements

Le responsable de traitement est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour assurer aux données qu'il a collectées les moyens de sécurité technique et organisationnelle adaptés.



Le respect et la gestion des droits des personnes

Pour chaque demande formulée par une personne, il convient :

- ➔ D'analyser la demande (analyse du/des cadres juridiques applicables, vérification de l'identité du demandeur si nécessaire) ;
- ➔ Obligation de répondre dans un délai d'un mois maximum ;
- ➔ Tracer la demande dans un registre dédié.



Obligations



La gestion des violations de données

Si une violation de données survient au sein d'une entité, il appartient au responsable de traitement de :

Notifier la violation :

- ➔ À la CNIL : dès lors qu'il existe un risque pour les droits et libertés des personnes concernées, dans un délai de 72h ;
- ➔ Aux personnes concernées : obligatoire dès lors que le risque apparaît comme élevé, le plus rapidement possible.

Tracer la violation dans un registre dédié. Il doit notamment comprendre les éléments suivants :

- ➔ La nature de la violation ;
- ➔ Les catégories et le nombre approximatif des personnes concernées ;
- ➔ Les catégories et le nombre approximatif de fichiers concernés ;
- ➔ Les conséquences probables de la violation ;
- ➔ Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- ➔ Le cas échéant, la justification de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées.



Obligations



Encadrement de la sous-traitance

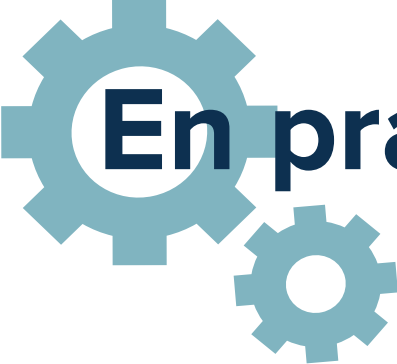
Le sous-traitant a des obligations propres prévues par le RGPD : Il est responsable à part entière de la partie de traitement qu'il réalise. Il sera responsable en cas de manquement à ses obligations légales ou contractuelles.

Chaque prestation comprenant un traitement de données à caractère personnel (secrétariat, hébergement, archivage physique) doit être encadrée dans un contrat par une clause ou un avenant portant sur le traitement de données personnelles, indiquant notamment :

- ➔ Les statuts et responsabilités des acteurs impliqués ;
- ➔ La description de l'activité de sous-traitance et des données et personnes concernées ;
- ➔ Des garanties quant à la confidentialités des données collectées ;
- ➔ Les mesures de sécurité prévues ;
- ➔ Les modalités de gestion des demandes d'exercice de droit des personnes ;
- ➔ Les modalités de gestion des violations de données ;
- ➔ Les modalités d'audit prévues.

En pratique





En pratique

Dossiers patients



Je limite les informations collectées au nécessaire et j'utilise les dossiers patients conformément aux finalités définies (suivi des patients) : la gestion des rendez-vous / l'envoi de courriers aux confrères / la gestion des dossiers médicaux / l'édition des ordonnances / l'établissement et la télétransmission des feuilles de soins.



Toute autre utilisation des informations que vous collectez à l'occasion de la prise en charge ne peut être réalisée sans critères de conformité (proportionnalité, détournement de finalité). En particulier, toute utilisation personnelle ou commerciale des dossiers de vos patients est naturellement prohibée.



Je tiens un registre à jour de mes traitements ;



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



Je mets en place les mesures appropriées permettant d'assurer à mes dossiers patients un niveau de sécurité adapté ;



J'informe mes patients et m'engage à assurer le bon exercice de leurs droits.

En pratique

La prise de rendez-vous



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



Les informations collectées lors de la prise de rendez-vous (motif de consultation, médecin spécialiste,...) peuvent renseigner sur l'état de santé des patients et constituent ainsi des données de santé.



Les autres obligations sont identiques à celles relatives aux dossiers médicaux :



Je tiens mon registre des traitements à jour;



Je respecte une durée de conservation appropriée;

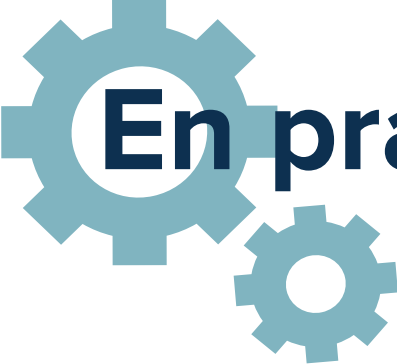


J'informe mes patients et m'assure du respect de leurs droits.



→ Le prestataire tiers gérant la prise de rendez-vous agit pour votre compte et est considéré comme sous-traitant.





En pratique

Messagerie électronique

- J'utilise un service de messagerie sécurisée de santé pour mes échanges avec d'autres professionnels de santé (confrères, laboratoires, ...) ;
- Si j'utilise une messagerie électronique standard ou des messageries instantanées, je m'assure qu'elles sont bien sécurisées et adaptées à mon usage professionnel ;
- Lorsque j'utilise des messageries standard sur Internet qui ne garantissent pas la confidentialité des messages, je protège les pièces jointes au moyen d'un dispositif cryptographique (chiffrement), archive avec mot de passe.

Tablettes et téléphones portables

- 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 permettant l'identification de mes patients sur mon téléphone portable ou ma tablette ;
- Je m'assure que l'accès au logiciel de gestion de dossiers patients sur mon téléphone portable ou ma tablette est sécurisé ;
- Je consulte mon logiciel de dossiers patients avec précaution (espaces publics).

En pratique

Recherches

- **Avant la réalisation d'études internes sur les données de mes patients, je réalise une analyse d'impact si le traitement de données est susceptible d'engendrer un risque élevé pour leurs droits et libertés ;**
- **Dans le cadre de recherches en partenariat avec un tiers, je m'assure que celles-ci sont menées conformément à la réglementation (notamment en établissant une convention ou un contrat) ;**
- **J'intègre à mon registre des traitements les activités découlant de la recherche ;**
- **J'informe mes patients des modalités de l'étude et de leurs droits inhérents que je m'assure de respecter en toutes circonstances.**



- Dans la mesure où ces études sont réalisées par vous et sont destinées à votre usage exclusif, aucune autorisation de la CNIL n'est nécessaire. Seul un avis favorable du Comité de Protection des Personnes doit être recueilli préalablement à la mise en œuvre de la recherche si celle-ci implique la personne humaine.



En pratique

Télémédecine

- Je m'assure que le prestataire de télémédecine choisi est bien conforme avec la réglementation ;
- Je vérifie la présence des mentions obligatoires dans le contrat qui me lie à lui ;
- J'informe mes patients sur les modalités du traitement de télémédecine ;
- Je tiens à jour mon registre des activités de traitement.



➔ Si vous avez recours à de la télémédecine, l'ensemble de vos obligations déontologiques habituelles s'appliquent, ainsi que vos obligations relatives aux informations que vous êtes amené à connaître sur vos patients ou sur d'autres professionnels de santé intervenant dans leur prise en charge.

Les règles relatives à l'échange et au partage de données entre professionnels sont également applicables.



Ramsay
Santé

Lien utiles

<https://www.cnil.fr>

<https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnile.pdf>

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

<https://www.cnil.fr/fr/guides-aipd>