

RGPD

Le RGPD ou le Règlement Général sur la Protection des Données, permet de **protéger les données personnelles sur le territoire de l'Union Européenne**. S'appliquant au secteur de la santé, vous êtes donc directement **concernés par les données sensibles que vous émettez et recevez en lien avec vos patients** (dossiers patient, plateforme de rendez-vous en ligne, ...) ou la **gestion de votre cabinet** (gestion du personnel, gestion des fournisseurs, ...).

Pour vous apporter toutes les informations sur le RGPD, l'URPS Médecin libéraux des Hauts-de-France et l'Assurance Maladie ont organisé [un webinaire](#) le jeudi 06 juillet 2023. En complément, nous vous proposons sur notre site internet, de reprendre les éléments clefs à connaître.



1 Outils numériques



Messagerie sécurisée



La messagerie sécurisée est un espace de confiance au sein duquel les professionnels habilités à échanger des données, en ville, à l'hôpital, ou dans les structures médico-sociales, peuvent **s'échanger par mail des données de santé de manière dématérialisée en toute sécurité.**

Pour les échanges avec d'autres professionnels, non professionnels de santé, intervenant dans la prise en soin du patient, **l'utilisation d'une messagerie standard implique de chiffrer les pièces sensibles à transmettre.**

Attention, votre corps de mail ne doit comporter aucunes informations sur les données de santé du patient.

Cependant, nous vous recommandons d'utiliser des messageries sécurisées hébergeurs de données de santé ou d'utiliser la messagerie sécurisée de santé de *Mon Espace Santé*.

Échanges sécurisés avec l'utilisateur



Les professionnels de santé équipés d'une messagerie sécurisée peuvent échanger avec leurs patients via la messagerie sécurisée de mon espace santé (MSS-C) de *Mon Espace Santé*, **à condition que l'utilisateur ait bien activé son compte.**

Pour les ordonnances, vous pouvez utiliser la messagerie sécurisée de *Mon Espace Santé*. L'initiation d'un échange avec l'utilisateur doit être faite par le professionnel de santé. Elle permet d'échanger des messages mais également des documents.

Certains outils ne sont pas adaptés pour recevoir ou communiquer des données de santé (ex: WhatsApp, gmail, etc...).

Sécurisation de vos outils numériques

- **Ordinateur** : Utilisation d'un mot de passe de **12 caractères (chiffres, lettres majuscules et minuscules, caractères spéciaux)**, à renouveler régulièrement et **verrouillage de votre session** informatique automatiquement après 30min d'inactivité.
- **Votre tablette ou votre téléphone portable** peuvent être utilisés, dans le cadre de votre activité professionnelle, à condition de respecter des règles de sécurité. Il est déconseillé de conserver des informations d'ordre médical dans la mémoire interne de votre tablette ou téléphone portable.

2 Identification du patient



Certains éléments permettent d'identifier le patient sans avoir besoin de collecter son nom ou prénom.

Une personne peut être identifiée :

- Directement (exemple son nom et prénom)
- Indirectement (exemple : un identifiant, un numéro de téléphone, une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique,)

L'identification d'une personne physique peut être réalisée :

- À partir d'une seule donnée (INS*, numéro de sécurité sociale, ...)
- À partir d'un ensemble de données (exemple : une femme vivant à telle adresse, date de naissance, ...)

*L'Identité Nationale de Santé (INS) permet de disposer d'une identité unique, pérenne et partagée par tous les acteurs de santé d'un même patient. Il comporte 5 traits obligatoires permettant de créer une identité : nom de naissance, premier prénom de naissance, date de naissance, sexe et code INSEE du lieu de naissance.

3 Archivage



Dossiers sous format papier

Vos locaux doivent être sécurisés, armoire contenant les dossiers **fermée à clé**.

Le RGPD s'applique peu importe le choix du support des dossiers patients (informatique ou dossier papier). Attention vous êtes responsable des données recueillies.



Conservation des dossiers

20 ans à compter de la date de la dernière consultation du patient :

- **Patient mineur** : si le délai de 20 ans expire avant son 28^{ème} anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date.
- **Décès d'un patient** : 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 en justice** : mise en cause de la responsabilité du médecin, il convient de suspendre ces délais de conservation.

4 Formalités auprès de la CNIL



Depuis le 25 mai 2018, vous n'avez plus de formalités à réaliser auprès de la CNIL. Seul un registre des activités de traitement recensant tous les traitements de données est à établir.

Le registre des activités

Document de recensement et d'analyse, présentant la réalité de vos traitements de données.

Les éléments devant figurer sur ce registre :

- Les parties prenantes (représentant, sous-traitants, ...) qui interviennent dans le traitement des données
- Les catégories de données traitées
- A quoi servent ces données (ce que vous en faites), qui accède aux données et à qui elles sont communiquées
- Combien de temps vous les conservez
- Comment elles sont sécurisées

 Afin de vous accompagner, nous mettons à votre disposition un exemple de registre des activités, n'hésitez pas à nous contacter.

Registre en cours de construction

Les sanctions



Sanction administrative de la CNIL : La CNIL peut prononcer, en fonction de la gravité du non-respect de la réglementation, des amendes administratives allant jusqu'à **20 millions d'euros** ou **4% du chiffre d'affaires annuel**.

Sanction pénale :

Pour une personne physique, de 5 ans d'emprisonnement et 300 000 d'euros d'amende

Pour une personne morale, 1,5 millions d'euros d'amende

À noter : si la CNIL constate un défaut de conformité et vous met en demeure de vous conformer, vous avez encore la possibilité d'adopter les mesures nécessaires pour éviter une sanction.

 **À savoir :** en décembre 2020 deux médecins libéraux ont été condamnés par la CNIL à une amende de 3 000 euros et pour le second médecin à 6 000 euros pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL conformément au RGPD¹.

¹CNIL, délibérations n° SAN-2019-014 et n° SAN-2019-015, 7 décembre 2020

Secrétariat et gestion du dossier patient



La prise de rendez-vous

Lors de la prise de RDV, sont collectées, enregistrées et utilisées des données personnelles concernant vos patients (identité, coordonnées personnelles, motif de consultation) par votre cabinet, par un prestataire tiers de permanence téléphonique, par une plateforme en ligne.

- Responsabilité : Vous restez « responsable de traitement » des données d'identification des patients et des données de santé collectées lors de la prise de rendez-vous
- Sécurisation : sécurisation du planning et de son contenu, enregistrement des données strictement nécessaires
- Suppression des données : Les données relatives à la prise de rendez-vous peuvent être supprimées lorsqu'elles ne sont plus nécessaires.

Accès au dossier patient

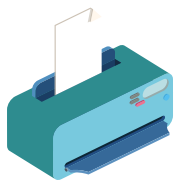


Le personnel administratif n'a pas un accès global aux dossiers patients mais uniquement à certaines informations (nom, prénom, code acte, NIR, date de consultation), informations pouvant être adressées aux organismes d'assurance maladie via la télétransmission ou les feuilles de soins.

Les ordonnances

Les secrétaires peuvent-elles intégrer les ordonnances au dossier patient ?

Les secrétaires peuvent s'occuper de scanner les ordonnances (à condition qu'il n'y ait aucune modification du document par les secrétaires) ou comptes rendus afin de les intégrer au logiciel du médecin.



Les secrétaires peuvent-elles réimprimer les ordonnances perdues ?

Les secrétaires médicales ne sont pas autorisées à réimprimer des ordonnances perdues. En cas de demande d'un patient, elle doit donc transmettre au médecin la demande de réédition de l'ordonnance, le médecin décidera, s'il réédite l'ordonnance sans revoir le patient. Si il décide de rééditer une ordonnance sans revoir le patient, il rédigera alors la nouvelle prescription ou la réédite ainsi la secrétaire pourra l'adresser au patient.

À savoir également que si le patient a déjà déposé une première fois son ordonnance en pharmacie et que celle-ci n'est pas périmée, le patient peut pour un traitement en renouvellement, se rendre dans sa pharmacie et demander d'utiliser l'ordonnance scannée lors de votre premier passage.

Pour éviter, ces situations, nous vous recommandons d'inciter les patients à activer leur espace DMP afin que les ordonnances puissent être dématérialisées.

Dossier patient



Quelles sont les informations que je peux collecter et garder sur mon patient ?

- Informations cohérentes avec la prise en soin du patient
- Limitées à ce qui est nécessaire
- Pas d'informations relatives à la vie privée sauf si elles sont en lien et nécessaire pour la prise en charge

Mon patient me demande son dossier patient, que dois-je faire ?

- Délai pour répondre : un délai maximum de 8 jours. Si les informations médicales remontent à plus de 5 ans, le délai maximal de réponse est de 2 mois.
- Support pour communiquer le dossier patient : à décider avec l'utilisateur (ex : messagerie sécurisée de *Mon Espace Santé*, ...)

7 Information aux patients sur le traitement des données



Information des patients portant sur le traitement des données

En tant que médecin vous devez délivrer une information aux patients portant sur le traitement de données dans le cadre de leur prise en charge (logiciel de suivi, dossier papier). Elle peut être délivrée à l'oral, à l'écrit ou par tout autre moyen (affichage dans les lieux de soins, dans les secrétariats, ...).

A savoir que pour la collecte et la conservation des données de santé, vous n'avez pas besoin de recueillir le consentement des patients.

L'information doit comporter les éléments suivants :

- Votre nom et vos coordonnées
- Les finalités et la base juridique du traitement, y compris les finalités ultérieures
- Les destinataires des données
- La durée de conservation
- Les droits de la personne : accès, rectification, à certaines conditions effacement, limitation, opposition, ...
- Caractère obligatoire des données fournies et des conséquences éventuelles d'un défaut de réponse
- Le cas échéant, utilisation ultérieure des données pour une finalité autre que celle pour laquelle les données ont été collectées (ex : utilisation ultérieure des données à des fins de recherche).

L'affiche est divisée en deux sections principales : 'Dossier patient' et 'Patient'. La section 'Dossier patient' explique comment les informations sont recueillies, quelles sont les informations recueillies, combien de temps est conservé le dossier, et qui peut accéder aux informations. La section 'Patient' détaille les droits du patient : droit d'accès, droit de modification ou rectification, droit à l'effacement ou à l'oubli, et droit à l'opposition. Elle mentionne également comment exercer ces droits. L'affiche est présentée sur un fond bleu clair avec des éléments graphiques comme des icônes de dossier et de patient.

Droit des patients sur les données

Les patients peuvent :

- Accéder aux données les concernant
- Rectifier ces données en cas d'erreur
- S'opposer au traitement pour des raisons tenant à leur situation particulière
- Effacer les données, dans certaines situations particulières (dossier patient conservé trop longtemps, données non adéquates, ...)

 Afin de vous accompagner, nous mettons à votre disposition un exemple d'affiche à personnaliser en [cliquant ici](#).

8 DPO ou « Data Protection Officer »



Qu'est-ce qu'un DPO ?

Délégué à la protection des données. Le DPO est chargé de piloter la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Est-ce que je dois nommer un DPO ?

- Exercice individuel : pas d'obligation de désigner un DPO
- Exercice en groupe : Si vous estimez que vous traitez des données de santé à grande échelle (ex : exercice au sein d'un réseau de professionnels, MSP, dossiers partagés entre plusieurs professionnels de santé, etc.), **2 possibilités** :
 - Désigner un DPO en interne
 - Solliciter les services d'un DPO externe (consultants, cabinets d'avocats, etc.)

9 Accès et échange des données de santé des patients



L'accès aux données médicales est limité aux informations strictement nécessaires à l'exercice de leur profession et donc à la prise en soin de l'utilisateur.

De manière générale aucun document médical n'est communicable à un tiers (personne de confiance, avocat, assurance, banque, etc..)

Échange au travers du dossier patient entre professionnels de santé

Vous pouvez être amené à échanger et partager des informations entre professionnels de santé ou avec les autres professionnels des champs sociaux et médico-social.

Dans le cadre d'une équipe de soins :

Les professionnels participant à la prise en charge d'une même personne peuvent échanger ou partager les seules informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention, ou au suivi médico-social et social du patient concerné. Les informations échangées et partagées sont limitées au périmètre des missions de chacun des professionnels. Le professionnel de santé devra informer le patient de l'échange et du partage sécurisé de ses informations.

En dehors de l'équipe de soins, le consentement préalable du patient est nécessaire

10

Obligation de sécurisation des données



Hébergement des données de santé

Le choix de l'hébergement des données de santé de vos patients est crucial. Afin d'assurer la protection des données sensibles des patients, les serveurs doivent respecter des normes strictes en matière de sécurité et de confidentialité.

En France, une certification « HDS » permet d'attester que l'hébergeur respecte les exigences réglementaires en matière de protection des données de santé.

Sauvegarde 1-2-3

En tant que responsable des données de santé de vos patients, nous vous conseillons d'appliquer la méthode de sauvegarde 1-2-3. Elle permet d'assurer une protection robuste et fiable des données en cas de perte, de panne matérielle ou de cyberattaque. Voici un aperçu de la méthode de sauvegarde 1-2-3

11

Télémédecine



Les vigilances à avoir en cas de mise d'une activité de télémédecine :

- Avant de faire votre choix sur le logiciel ou la plateforme que vous allez utiliser, vous devez vous assurer qu'il respecte la réglementation liée au RGPD.
- Vous devez être vigilant sur l'utilisation, la collecte et les mesures de sécurité par l'éditeur des données personnelles et de santé des patients.
- Vous devez également vous assurer que le logiciel ou la plateforme soit hébergé par un hébergeur de données de santé agréé ou certifié.

12

Pharmacie



Avec l'accord du patient, puis-je transmettre son ordonnance à une pharmacie via une messagerie non sécurisée ?

Malgré l'accord du patient, il n'est pas recommandé de transmettre une ordonnance via une messagerie non sécurisée. Pour les ordonnances, vous pouvez utiliser la messagerie sécurisée de Mon Espace Santé. Vous pouvez également mettre directement l'ordonnance via Mon Espace Santé afin que le patient puisse directement transmettre l'ordonnance à la pharmacie de son choix depuis leur messagerie sécurisée.

13

Établissement de santé



En cas d'hospitalisation d'urgence, peut-on transmettre des informations entre professionnels de santé ?

Lorsqu'un patient est admis en urgence, les professionnels de santé peuvent échanger des informations médicales pertinentes afin d'assurer la prise en charge du patient, y compris des antécédents médicaux ou médicaments en cours seulement aux professionnels de santé directement impliqués dans la prise en charge du patient.

Cependant, si les professionnels de santé ne font pas partie de l'équipe de soins, vous devez informer préalablement le patient de la nature des informations devant faire l'objet de l'échange ainsi que l'informer de l'identité du destinataire des informations (nom, profession ou qualité au sein d'une structure).

Dans le cadre d'une équipe de soins, les professionnels partagent les informations relatives à une personne prise en charge dans les strictes limites et en informent préalablement la personne concernée.

Lorsque la personne est hors d'état d'exprimer sa volonté, seule l'urgence ou l'impossibilité d'informer cette personne peut dispenser le professionnel ou la personne participant à sa prise en charge de l'obligation d'information préalable. La personne concernée est toutefois informée, dès que son état de santé le permet, de l'échange ou du partage des informations auquel il a été procédé. Il en est fait mention dans le dossier médical.