



## Qu'est-ce que le RGPD ?

Le Règlement Général sur la Protection des Données est un texte de loi européen qui est entré en vigueur au 25 mai 2018. Son but est de mieux protéger les données des individus et de leur permettre un meilleur contrôle sur ces dernières.

Il concerne :

- Le traitement des données, c'est à dire tout ce qui touche à leur manipulation, stockage, utilisation ou communication
- Une meilleure distinction entre les données personnelles et les données dites sensibles qui doivent être mieux protégées
- La responsabilité des individus vis-à-vis des données qu'ils manipulent.

## Quel impact pour vos données patients ?

En tant que professionnel de santé, vous êtes amené à traiter et recueillir les données de santé de vos patients dans le cadre de leur prise en charge. Vous récupérez et scannez leurs ordonnances qui contiennent leur traitement, et faites parfois une [démarche de soins infirmiers](#) dans laquelle vous notez des observations et établissez un diagnostic infirmier. Vous prenez également des constantes vitales que vous reportez dans un [dossier de soins](#) ou bien vous chargez une autre personne de [faire tout ceci pour vous](#). Toutes ces informations que vous traitez et stockez sont des données personnelles mais également à caractère sensible.

Elles entrent donc pleinement dans le cadre du RGPD et doivent faire l'objet d'une attention toute particulière. Ainsi, vous devez garantir leur sécurité, leur accessibilité par le patient, qui peut vous demander de les supprimer lorsque vous n'en avez plus l'utilité, ou de les modifier. Vous êtes responsable de toutes les données que vous récoltez auprès de vos patients et devez donc garder en tête ce principe quand vous choisissez vos outils de travail.

## Les bonnes pratiques à mettre en place

**Ne conserver aucune donnée en « local » ou sur un serveur autre que celui de votre logiciel :**

- Une clé USB peut être facilement perdue ou volée.
- Votre propre ordinateur peut tomber en panne ou être piraté.
- Un serveur doit répondre à un niveau d'exigence élevé en matière de sécurité afin de pouvoir héberger des données sensibles telles que des données de santé.

Concernant votre logiciel, sachez que chez Albus vos données sont stockées sur des serveurs sécurisés ayant reçus le label « [Hébergement de Données Santé](#) », label certifiant que l'hébergeur de vos données est agréé par le Ministère de la Santé.

De la même manière, quand vous partez en tournée il est important de garder ce principe à l'esprit car un smartphone n'est pas plus sécurisé qu'un ordinateur. Pour échanger avec vos collègues, il est donc recommandé de passer par [une application sécurisée](#).

**La sécurité avant tout :**

- Ne jamais partager son identifiant et son mot de passe.
- [Avoir un bon mot de passe](#) : choisir un mot de passe sécurisé en respectant [les minima recommandés](#) à savoir 12 caractères de long ; des chiffres, des lettres et des caractères spéciaux ; un mot de passe anonyme et unique.

**Ne collecter que l'essentiel :** c'est le principe de minimisation. On ne collecte que les données dont on a besoin pour la prise en charge et on laisse de côté le superflu.

**Limiter la durée de la conservation des données :** l'idée ici est de prendre en compte les obligations de conservation des données de santé mais sans faire de zèle ! Une fois le délai de conservation passé, on n'hésite pas à faire le tri. En plus, cela permet d'y voir plus clair. A titre indicatif, le délai de conservation recommandé est de 20 ans pour les médecins.

**Informez les personnes du traitement de leurs données :** il est important d'informer les patients que vous êtes amené à collecter leurs données et les stocker. Vous n'êtes pas obligé de recueillir leur consentement puisque la collecte de données est nécessaire dans le cadre de la prise en charge. Vous pouvez aussi informer les patients par voie d'affichage dans votre cabinet.

**Limitez l'accès à ces données :** Vous devez faire en sorte de ne donner l'accès aux données des patients qu'aux personnes autorisées, et une fois de plus, seulement les données dont elles ont besoin. Il est tout à fait possible par exemple de donner un accès à la secrétaire de votre cabinet.

**Tenir un registre des activités de traitement** : il permet de recenser toutes vos activités de traitement des données dans le cadre de votre exercice. Vous pouvez vous inspirer des modèles disponibles en ligne comme [celui de la CNIL](#).

## Quelques questions fréquemment posées

- Dois-je toujours me déclarer auprès de la CNIL ?
  - Non, cette démarche n'est plus d'actualité depuis l'entrée en vigueur du RGPD. Par contre, vous devez être en mesure de prouver que vous êtes en conformité avec cette loi.
- Dois-je désigner un Délégué à la Protection des Données (DPO) ?
  - Dans une activité exercée à titre individuel, vous n'êtes pas obligé de désigner un DPO. La désignation du DPO peut être envisagée dans le cas où vous traiteriez de nombreuses données (par exemple en établissements comme les maisons santé).
- Le RGPD concerne-t-il uniquement les données numérisées ?
  - Non, cette loi concerne aussi bien le traitement numérique que papier de vos données.

Pour de plus amples informations sur le sujet, n'hésitez pas à consulter [la plaquette de la CNIL](#).