LA PROTECTION DES DONNÉES PERSONNELLES
AU SEIN D'UN CABINET DE KINÉSITHÉRAPIE

Par **Nesrine Benyahia**, Docteur en droit de la santé
Présidente & Fondatrice de DR DATA

INTRODUCTION

Le 25 mai 2018, le règlement général relatif à la protection des données personnelles est entré en application.

Ce règlement, aussi appelé **RGPD**, pose un cadre européen uniformisé du traitement de données personnelles, avec de grands principes tels que le **principe de transparence, de licéité et de respect des droits et des libertés des personnes.**

Les trois principaux axes en protection des données personnelles sont l'obligation de garantir :

1. La **confidentialité** des données
2. L'**intégrité** des données
3. La **disponibilité** des données

Le RGPD ne concerne pas que les données sous format électronique, mais bien toute donnée personnelle traitée, même sur un support papier.

La donnée personnelle ici renvoie à toute information qui permet d'identifier une personne physique : un prénom, un nom, un numéro d'identification, une adresse email, une adresse IP...

En France, l'autorité en charge de faire respecter ce cadre juridique et réglementaire est la **Commission nationale de l'informatique et des libertés (CNIL)**. Aujourd'hui, la CNIL communique pour sensibiliser sur les enjeux relatifs à la protection des données, notamment dans le domaine de la santé.

LES DONNÉES PERSONNELLES DE SANTÉ : DES DONNÉES SENSIBLES À PROTÉGER ET À SÉCURISER

Les données personnelles de santé font partie des catégories particulières de données personnelles dites **"données sensibles"**, figurant ainsi aux côtés notamment des données biométriques (empreinte digitale, scan rétinien etc.), des données génétiques et des données révélant l'appartenance religieuse ou bien l'orientation sexuelle par exemple.

Les données personnelles concernant la santé sont celles qui révèlent toute information sur l'état de santé physique ou mentale d'une personne. Cela peut être une information sur ses pathologies, ses prescriptions (produits de santé ou actes de soins), ses antécédents, son handicap physique ou mental... En bref, **principalement toutes les données présentes dans le dossier patient.**

A l'ère du tout numérique, **la prise de rendez-vous en ligne** n'échappe pas à la règle puisque la prise de rendez-vous par un patient est considérée comme une donnée personnelle de santé, dès lors que la nature du rendez-vous peut indiquer indirectement une information sur l'état de santé du patient.

Ces données sont sensibles car elles touchent à la dignité humaine de la personne.

LE RÔLE DU KINÉSITHÉRAPEUTE DANS LA PROTECTION DES DONNÉES DE SES PATIENTS

Le kinésithérapeute, de par la nature de son activité, traite des données personnelles de santé.

Il est le responsable de traitement ; ses fournisseurs de logiciels ou d'outils numérique (télémédecine, IA…) **sont ses sous-traitants au regard du RGPD**. Le kinésithérapeute est responsable des données qu'il traite.

Dans sa pratique quotidienne, le kinésithérapeute organise ses journées grâce à son agenda contenant les rendez-vous fixés très souvent avec le prénom et le nom du patient. Qu'il s'agisse d'un agenda en ligne ou d'un agenda papier, la loi s'applique de la même façon.

Aussi, lorsque le patient arrive en consultation, le kinésithérapeute accède au dossier du patient et prend connaissance de l'état de santé de ce dernier, il peut également par le biais de son logiciel prescrire des produits de santé ou des actes de soins. Le professionnel de santé inscrit aussi les actes réalisés lors de la consultation dans le dossier du patient.

Dans ce cas dit "classique", il n'y a pas besoin du consentement du patient puisque le traitement de ses données est impératif pour sa prise en charge.

• Dans certains cas, il est possible que le kinésithérapeute demande **l'avis d'un confrère** ou d'un autre professionnel de santé sur la prise en charge du patient. Cette demande d'avis peut se matérialiser par un échange téléphonique avec son confrère, par fax ou bien par des échanges électroniques. Dans ce cas, il faut être vigilant à ce que ce partage de données entre dans le cadre de l'équipe de soins, autrement il faudra obtenir le **consentement tracé du patient**, c'est le cas notamment pour la télé-expertise.

• La **téléconsultation**, qui constitue un des actes de télémédecine majoritairement effectués en France, nécessite également le consentement tracé du patient au traitement de ses données dans le cadre d'un acte de télémédecine. En général, l'outil ou la plateforme utilisé fournit la possibilité d'obtenir ce consentement, mais le professionnel de santé est bien responsable de la vérification de ceci.

Ainsi, **tout au long de sa journée d'activité, le kinésithérapeute accède, collecte, manipule, partage...les données de santé de ses patients.** Toutes ces actions sont des traitements de données personnelles, elles doivent donc être réalisées en toute sécurité et en respectant les droits et libertés des patients.
Il est fortement recommandé de tenir un registre de tous les traitements de données réalisés.

Les patients doivent alors être informés de tous les traitements de données qui sont réalisées sur leurs données personnelles. Cette information doit être claire et compréhensible. Elle peut par exemple se matérialiser par l'affichage d'un document d'information décrivant les traitements de données effectués par le kinésithérapeute, **quel type de logiciel est utilisé et pour quoi faire, comment les données sont conservées, comment les patients peuvent accéder à leurs données**, etc.

Quelques conseils pratiques :

- *Ne pas échanger d'informations identifiantes sur des patients avec vos confrères ou d'autres professionnels de santé sans utiliser une messagerie sécurisée de santé dédiée.*

- *Si votre patient vous demande l'accès à son dossier médical, ne l'envoyez pas par une messagerie non sécurisée et non hébergée chez un hébergeur certifié. Privilégiez une messagerie sécurisée de santé professionnel-patient, ou bien la remise en main propre contre signature d'une décharge de remise des documents demandés.*

- *En cas de demande d'exercice des droits, demande d'accès ou d'effacement du dossier du patient par exemple, vous disposez d'un mois pour répondre à la demande, après avoir bien entendu analysé son bien fondé et sa recevabilité. Pensez à vérifier l'identité de la personne qui demande ces droits.*

- *En cas de violation de données personnelles, c'est-à-dire si vous perdez votre ordinateur contenant les dossiers des patients sans savoir si une personne extérieure peut y accéder, ou si vous faites l'objet d'une confiscation des données par un hacker et d'une rançon, si votre ordinateur et vos documents patients sont détruits et que vous perdez complètement les données sans avoir fait préalablement une sauvegarde….Vous devez **alerter la CNIL dans les 72 heures** suivant la connaissance de la violation. Vous devrez remplir un formulaire vous demandant de décrire ce qu'il s'est passé et de fournir des éléments de réponse quant à la gestion de la violation, les mesures que vous mettez ou que vous allez mettre en place pour y remédier ou éviter que cela ne se reproduise...*

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES : LE BRAS DROIT DU PROFESSIONNEL DE SANTÉ POUR ASSURER SA MISE EN CONFORMITÉ ET MAINTENIR LA RELATION DE CONFIANCE AVEC SES PATIENTS

Le Délégué à la protection des données, aussi appelé **DPO pour Data Protection Officer**, est une nouvelle fonction créée par le RGPD pour garantir la mise en oeuvre des exigences en protection des données.
Ce DPO est à la fois le pilote et le chef d'orchestre de la conformité.

Auprès d'un kinésithérapeute, le DPO :

1. Informe et conseille dès que s'en ressent le besoin ;
2. Accompagne dans toute sa mise en conformité avec la tenue d'un registre, la rédaction des documents nécessaires, ...
3. Audite l'activité du praticien pour vérifier les mesures de sécurité, et le cas échéant, lui trouve des solutions
4. Gère les demandes de droits des patients sur leurs données ;
5. Est le point de contact privilégié avec la CNIL, notamment en cas de contrôle ou de notification de violation de données personnelles.

Si l'on veut comparer le DPO à une fonction habituelle, nous le comparerons à l'expert comptable. Le DPO, lui, est expert des données et apporte le soutien et le conseil nécessaire au professionnel de santé afin de protéger les données de ses patients et de respecter la loi.

Quelques conseils dans le choix du DPO :

- *Le DPO peut être interne ou externe. Un DPO externe peut être une société de conseil, un cabinet d'avocat par exemple.*
- *Le DPO doit être indépendant et ne pas être en conflit d'intérêts, ainsi un associé d'un cabinet ne peut être DPO car il est à la fois juge et partie.*
- *Le DPO doit disposer des compétences juridiques et techniques nécessaires.*
- *Le DPO doit maîtriser votre secteur d'activité, la santé est un domaine particulier dans lequel s'amoncellent différentes réglementations locales allant au-delà du RGPD.*
- *Le DPO doit être bon communicant pour assurer un contact sérieux et serein avec les patients et l'autorité de contrôle.*
- *Enfin, le DPO est là pour faciliter votre activité et ne pas vous freiner dans vos projets en exploitation de données, il doit tout mettre en oeuvre pour trouver les solutions adaptées.*

CONCLUSION

Avec le RGPD, nous sommes passés d'un régime déclaratif dans lequel nous étions habitués à effectuer des déclarations à la CNIL pour tout traitement de donnée personnelle, à un **régime de responsabilité** dans lequel la majorité des obligations de déclaration a disparu pour laisser place à "***l'accountability***", c'est-à-dire la responsabilisation des acteurs : **Il faut être conforme et pouvoir prouver sa conformité en amont.**

Cette nouvelle réglementation européenne s'étend aujourd'hui à de nombreux pays en dehors de l'Union Européenne, qui s'adossent au RGPD afin d'offrir un cadre respectueux de l'usage des données de santé vis-à-vis du patient.

Les professionnels de santé, principaux "producteurs" de données avec les patients, sont les premiers acteurs concernés.
Les kinésithérapeutes traitant des données sensibles sont *de facto* concernés et se doivent de maintenir la relation de confiance avec leurs patients.

Union Régionale des Professionnels de Santé
Masseurs-Kinésithérapeutes d'Île-de-France

www.urps-kine-idf.com

Tél. 09 52 00 34 59 - contact@urps-mk-idf.org - Suivez-nous