RGPD : comment se mettre en conformité ?

Depuis le 25 mai 2018, le Règlement Général européen sur la Protection des Données (RGPD) **est applicable en France**. De nombreuses formalités auprès de la CNIL ont disparu, il n'est aujourd'hui plus obligatoire de déclarer votre fichier patient auprès de la CNIL.
En revanche, **vous devez être en mesure de démontrer à tout moment votre conformité aux exigences du RGPD.** Pour cela, vous pouvez mettre en place un registre recensant vos fichiers, décrire les modalités de l'information que vous délivrez au patient et les actions menées pour garantir la sécurité des données de santé que vous conservez, etc.

Pour rappel, en tant que professionnel libéral de santé, vous stockez des données dites « sensibles » (coordonnées des patients, numéro de sécurité sociale, état de santé etc.).
Attention, les données que vous collectez sur vos patients doivent être adéquates, pertinentes et limitées à ce qui est strictement nécessaire à la prise en charge du patient.

Objectifs : Le RGPD a deux objectifs principaux : renforcer le droit des personnes dans la gestion de leurs données personnelles et responsabiliser les acteurs traitant des données, c'est-à-dire vous !

Données concernées : Le règlement s'applique aux *« données à caractère personnel »* qui se définissent comme *« toute information se rapportant à une personne physique identifiée ou identifiable »* (article 4 RGPD). **Le fichier informatisé n'est donc plus le seul concerné mais également les fichiers papiers** dans lesquels sont stockées des données personnelles des patients ou clients qui doivent être protégées dans les mêmes conditions.

Acteurs concernés : Toute entreprise ou organisme qui détient des données dites sensibles, par lesquelles une personne physique est identifiée ou identifiable. En clair, les employeurs, les administrations, et aussi vous !
Vous êtes « responsable de traitement », c'est-à-dire responsable des données que vous conservez. Si vous sous-traitez des tâches, les sous-traitants sont eux aussi responsables de traitement. Par exemple, si vous stockez les données sur un serveur à distance (cloud), si vous télétransmettez, ou encore si vous travaillez sur un logiciel de gestion de cabinet qui transmet des données sur un serveur à distance.
Tous les professionnels libéraux devront assurer une protection optimale de leurs données à chaque instant et être en mesure de la démontrer.

Et le secret professionnel ? Vous devez bien évidemment le respecter mais il ne dispense pas de se conformer au RGPD.

Obligations : À tout moment, vous devez être en mesure de démontrer que vos fichiers patients sont protégés. De plus, vous avez l'obligation de notifier à la CNIL toute violation de données à caractère personnel (par exemple vol d'ordinateur ou fuites de données) dans les 72 heures.

Parution dans le LME n°39 de septembre 2018

Actions à mener au cabinet : Il n'est pas nécessaire d'obtenir le consentement des patients pour collecter et conserver les données de santé les concernant car leur collecte et leur conservation sont indispensables pour réaliser un diagnostic et la prise en charge du patient.
Le site de la CNIL met à disposition un modèle de registre, des fiches et guides pratiques qui vous aideront à identifier les données que vous collectez et les mesures à mettre en place pour les sécuriser *(voir les liens en fin d'article)*. Le registre doit être conservé en interne, il permet de documenter votre conformité ; vous ne devez pas le transmettre à la CNIL.
La constitution du registre est l'occasion de faire le point sur la façon dont vos patients sont informés de l'utilisation faite de leurs données. **Vous devez indiquer à vos patients les modalités de conservation de leurs données ainsi que leur droit d'accès et de modification. L'information doit être claire, compréhensible et accessible pour l'ensemble de vos patients (personnes majeures, mineures, personnes âgées etc).**
Pour cela, vous pouvez les informer sous forme d'affichage dans votre salle d'attente *(voir modèle CNIL en fin d'article)*. Vous pouvez également, dans vos correspondances (courriers, mails), préciser les données collectées, l'identité de la personne qui est responsable de la conservation de ces données (vous ou un sous-traitant) et préciser les modalités d'exercice du droit d'accès (possibilité pour les patients d'accéder à leurs données ou de les modifier).

Actions à mener avec les tiers : L'accès aux données de santé de vos patients doit être bien évidemment limité. Seules certaines personnes sont autorisées, au regard de leurs missions, à accéder aux données nécessaires (ex : secrétaire du cabinet, équipe de soins avec laquelle vous travaillez, les organismes d'assurance maladie etc).
De plus, vous devez être attentif à la rédaction des contrats si vous sous-traitez une tâche, si vous avez conclu un contrat de maintenance, si vous stockez vos données à distance (cloud). Les données sous-traitées doivent bénéficier de garanties suffisantes et vous devez exiger du sous-traitant la communication de sa politique de sécurité. En résumé, vous devez obtenir toutes informations utiles afin de pouvoir démontrer que vous avez pris les précautions nécessaires pour sécuriser les données que vous stockez et auxquelles une entreprise tiers a accès.

Les salariés du cabinet : La CNIL propose un modèle d'engagement de confidentialité à faire signer aux salariés qui sont amenés à travailler avec des données personnelles dites sensibles. Vous pouvez aussi insérer une clause de confidentialité dans le contrat de travail visant les données à caractère personnel.
Exemple d'engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel : *https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs*.

Faire appel à un expert : Vous pouvez faire appel à une entreprise spécialisée mais attention aux arnaques, leur technique bien rodée consiste à insister sur les sanctions financières encourues et à promettre une mise en conformité à distance de manière rapide avec une prétendue certification ou recommandation de la CNIL.
Attention, la CNIL ne recommande, ni ne certifie aucune entreprise. De plus, soyez prudent, ne communiquez pas vos coordonnées bancaires par téléphone !

Sanctions : Le non respect du règlement est passible d'amende très lourde, 4% du chiffre d'affaires annuel pouvant atteindre 20 millions d'euros.

Où vous renseigner ?

- Guide pratique de sensibilisation au RGPD : *https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf*
- Modèle de registre : *https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique*
- RGPD et professionnels de santé libéraux: *https://www.cnil.fr/fr/rgpd-et-professionnels-de-sante-liberaux-ce-que-vous-devez-savoir*

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Ce lieu de soins dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients et à assurer la facturation des actes et, le cas échéant, la télétransmission des feuilles de soins aux caisses de sécurité sociale.

Les informations qui vous sont demandées feront l'objet, sauf opposition justifiée de votre part*, d'un enregistrement informatique.

Vous pouvez accéder aux informations vous concernant auprès de votre professionnel de santé**.

*Article L.1111-8 du Code de la Santé Publique

**Loi n°78-17 du 6 janvier 1978 modifié en 2004 relative à l'informatique, aux fichiers et aux libertés.

Céline DELRIEU
Attachée juridique de l'ANGAK

Parution dans le LME n°39 de septembre 2018