Le règlement européen sur la protection des données : Quels enjeux pour le médecin libéral ?

- ## Idée générale du RGPD

Le RGPD (Règlement général à la protection des données) est le règlement européen[1] venant harmoniser **le système de protection des données personnelles en Europe**. Il est applicable en France depuis le 25 mai 2018.

L'objectif est de rendre aux utilisateurs leurs droits sur les données personnelles qui les concernent.

Pour être incitatif, le RGPD instaure de lourdes sanctions en cas de violation des obligations.

- ## Le médecin libéral et le RGPD

Tous les acteurs économiques sont concernés, tous ceux qui, au cours de leur activité, enregistrent ou traitent des données personnelles.

Le médecin libéral est lui aussi concerné et ce, d'autant qu'il traite de **données** de santé qui sont considérées comme **sensibles**.

Il s'agit donc des informations collectées par le médecin aussi bien lors de l'inscription de la personne concernée dans le service de soin que lors de la réalisation des prestations de soins.

Ces données de santé qui ne peuvent être collectées par des médecins ou professionnels soumis au secret doivent faire l'objet d'une protection renforcée.

I. LE SYSTÈME DE PROTECTION DES DONNÉES TRAITÉES PAR LE MÉDECIN LIBÉRAL MIS EN PLACE PAR LE RGPD

A. Apports et renforcement des droits relatifs à la protection des données de santé

1. Le renforcement des droits des patients sur leurs données personnelles

Les droits dont bénéficient les patients dans le cadre du RGPD sont les mêmes que ceux qui étaient prévus par le code de la santé publique ou la Loi informatique et liberté :

- Le droit d'accès aux données collectées[2] : connaître les données collectées, et y avoir accès ;

- Le droit de rectification des données[3] ;

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[2] Article 15 du RGPD

[3] Article 16 du RGPD

- Le droit à la portabilité[4] : nouveauté introduite par le RGPD : le patient peut demander à un médecin de transférer ses données à l'un de ses confrères ;

- Le droit à la transparence sur le traitement des données : le médecin doit être en mesure de fournir au patient toutes les informations concernant le traitement des données le concernant.

2. Le principe de responsabilité renforcée du responsable du traitement que constitue le médecin libéral

Le respect du RGPD est assuré en France par la Commission nationale de l'informatique et des libertés (CNIL), qui est à même d'exercer des contrôles à tout moment afin de vérifier la conformité du professionnel au Règlement.

En cas de non-respect du Règlement, le professionnel de santé reçoit le plus souvent une demande d'information suite à un contrôle de la CNIL ou une plainte reçue ou une mise en demeure.

En cas de défaut de réponse, réponse non conforme, une amende peut être prononcée.

Cette amende administrative peut aller jusqu'à 2 % du chiffre d'affaires ou deux millions d'euros pour les infractions légères, et jusqu'à 4 % du chiffre d'affaires ou quatre millions d'euros pour les infractions les plus graves.

De telles sanctions ne sont toutefois que rarement mises en œuvre sans que la CNIL n'ait préalablement adressé au responsable de traitement un rappel à l'ordre ou une injonction de mise en conformité qui ne soit restée sans effet.

La difficulté pour le professionnel de santé est de respecter ses obligations de conserver les données tout en respectant les obligations du RGPD.

B. L'articulation entre les obligations légales du professionnel de santé et le RGPD

1. Le conflit entre l'obligation de conservation des données du médecin libéral et le droit à l'oubli du patient

Le RGPD prévoit un droit à l'effacement des données ou droit à l'oubli[5] profitant à la personne concernée par le traitement de données.

Toutefois, au regard des exigences de l'article L.1142-28 du Code de la santé publique relatif au délai de prescription des actions en responsabilité médicale, **les dossiers médicaux en possession du médecin doivent être conservés au moins 10 ans**.

En pratique, le médecin doit plutôt s'astreindre à une conservation des dossiers pendant une **durée de 30 ans,** car le point de départ du délai de prescription en cas de responsabilité civile peut considérablement varier.

Toutes les données en possession du médecin sont concernées, qu'elles figurent sur un support d'information matériel comme le papier ou qu'elles soient dématérialisées.

---

[4] Article 20 du RGPD

[5] Article 17 RGPD

2. La dérogation à l'obligation de recherche du consentement du patient par le médecin libéral

De manière générale, le responsable du traitement doit rechercher le consentement de la personne concernée pour que le traitement soit licite.

Deux cas de figure se présentent alors au médecin dans le cadre de son exercice :

- En présence de données relatives à la santé du patient, le médecin peut passer outre le consentement de la personne pour traiter des données.

- En revanche, en présence de données qui ne sont pas relatives à la santé des patients, leur consentement doit être recueilli de manière explicite auprès de la personne, à moins que ces données ne soient elles-mêmes nécessaires sur le plan de la prise en charge médicale du patient.

Ainsi, pour l'ensemble des données de santé ou des données nécessaires pour l'exercice de l'art médical, le médecin peut se passer du consentement de la personne concernée et n'a pas vocation à soumettre un formulaire pour le traitement des données au patient.

II. LA MISE EN CONFORMITÉ DU SYSTÈME DE TRAITEMENT DES DONNÉES DU MÉDECIN LIBÉRAL AUX RGPD

Pour respecter ses obligations, le médecin libéral doit prendre des mesures concrètes au sein de son cabinet libéral.

A. Les démarches nécessaires

1. La création d'un registre des activités de traitement

Afin de procéder à sa mise en conformité au regard du RGPD, le médecin doit dans un premier temps faire l'inventaire de l'ensemble des données qu'il détient et leur circulation.

Il doit donc réaliser une cartographie des données et de leur traitement.

Concrètement, le professionnel de santé doit établir un **registre des données et de leur traitement** qui peut prendre la forme d'un tableau sur une feuille de calcul d'un tableur informatique, dont la CNIL fournit des modèles[6] disponibles en ligne.

En qualité de responsable de traitement, le médecin doit veiller à faire figurer dans le registre les informations relatives aux coordonnées du responsable du traitement (représentant légal : le médecin lui-même et le cas échéant le délégué à la protection des données s'il en a désigné un).

Le registre doit en outre mentionner :

- Les finalités du traitement (la prise en charge médicale des patients), la description des catégories de personnes concernées (patients, médecins, fournisseurs, salariés) ;

[6] https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

- Des catégories de données à caractère personnel (identité, données de localisation, éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, données de santé) ;

- Les flux de données, c'est-à-dire les catégories de destinataires auxquels les données ont été ou seront communiquées (patients, médecins) ;

- Les délais prévus avant l'effacement des différentes catégories de données (pour les données médicales, 30 ans en pratique) ;

- La description générale des mesures de sécurité techniques et organisationnelles mises en place pour assurer la conservation, l'intégrité et la confidentialité des données.

Sur ce dernier point, il s'agit concrètement d'identifier les acteurs internes (médecins, autres professionnels de santé ou paramédicaux, personnels administratifs, etc.) ou externes (prestataires extérieurs) susceptibles d'accéder aux données, et de décrire précisément le parcours des données et leur sécurisation, ainsi que le niveau d'accès des personnes concernées.

2. La mise en place d'un système de sécurité spécifique

Du fait de la sensibilité des données qu'il traite, le médecin est soumis à une **obligation de sécurité renforcée** s'agissant des données qu'il détient.

Il est donc tout particulièrement concerné par la mise en place d'un système de sécurité adéquat, afin de protéger les données récupérées auprès des patients.

Cette obligation découle de l'article 32 du RGPD, qui prévoit que le responsable du traitement doit mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

Ces mesures doivent permettre de garantie la confidentialité des données, leur conservation, leur intégrité et leur récupération.

Concrètement, la mise en œuvre des mesures de sécurité appropriée peut être assurée par la mise en œuvre des mesures suivantes :

- Application d'un dispositif d'anonymisation ou de chiffrement des données de santé récupérées ;

- Mise en place de mesure de contrôle de l'accès aux données (mots de passe, cartes d'accès pour certain locaux, verrouillage automatique des ordinateurs après un certain délai d'inactivité, etc.) ;

- Dispositifs de sauvegarde régulière des données informatiques afin de pouvoir récupérer les données en cas de piratage.

Il s'agit également de mettre en place des procédures permettant d'analyser l'efficacité des mesures de sécurité des données.

En cas de violation du système de sécurité, et conformément aux articles 33 et 34 du RGPD, le médecin doit en faire état à l'autorité de contrôle (CNIL) et aux patients concernés.

B. Les contrats de service pour l'accompagnement du médecin libéral dans sa mise en conformité

1. La mise en place d'un Délégué à la Protection des Données (DPD) ou *Data Protection Officer* (DPO) en principe facultative pour le médecin libéral

Le Délégué à la Protection des Données (DPD) est le successeur du Correspondant Informatique et Libertés (CIL) depuis l'entrée en vigueur du RGPD.

Le DPD est chargé de veiller de manière indépendante à la conformité en matière de protection des données chez le professionnel concerné (qui peut être un cabinet médical).

Sa désignation est rendue obligatoire dans certains cas, notamment si un professionnel assure le traitement à grande échelle de données sensibles, telles que des données de santé.

En l'occurrence, si le traitement des données des patients au sein d'un hôpital est considéré comme un traitement à grande échelle de données sensibles obligeant la désignation d'une DPD, tel n'est pas le cas du traitement des données des patients par un médecin libéral, qui n'est donc pas astreint à la nomination d'un DPD.

L'intervention d'un DPD peut toutefois s'avérer utile pour le médecin, afin de bénéficier de son expertise juridique et technique pour lui permettre de cartographier ses traitements de données personnelles et d'assurer la conformité en continu.

Le DPD n'est toutefois pas responsable des infractions au RGPD et ne peut faire l'objet de sanctions par l'autorité de régulation. Il peut en revanche engager sa responsabilité en cas de sanction vis-à-vis de son client, le médecin qui lui aurait confié la mission.

Le DPD peut être un avocat spécialiste de la question. Il faut que le médecin soit vigilant lors de la signature d'une mission de DPD afin que celui-ci soit couvert en cas de sanction par la CNIL.

2. La mise en place éventuelle d'un contrat de sous-traitance par le médecin libéral

Dans le cadre de son activité, le médecin libéral peut faire appel à des fournisseurs divers (sous-traitants). Le sous-traitant peut alors lui-même être amené à traiter les données sensibles des patients conservées par le médecin (exemple : logiciel de gestion de rendez-vous par internet, logiciel de gestion de cabinet, société d'archivage pour stocker les données qu'il collecte).

Attention, le sous-traitant doit signer des contrats précis et très strictement encadrés par le RGPD. L'article 28 du règlement y fait référence.

Dans ce cadre, le médecin doit s'assurer que le sous-traitant auquel il a recours dispose de « garanties suffisantes » pour répondre à la nécessaire sécurité des données traitées.

Il est conseillé à chaque médecin libéral d'interroger ses fournisseurs pour vérifier les contrats existants et notamment qu'ils sont conformes au RGPD particulièrement vérifier ce qui est prévu pour la sécurisation et le traitement des informations des données de santé.

***

Conclusions : La CNIL a déjà prononcé les premières amendes dont certains sont des professionnels de santé médicaux.

Par conséquent, les médecins libéraux même isolés, doivent absolument s'intéresser à la question de la conformité de leur pratique au RGPD et procéder aux démarches nécessaires, en premier lieu la réalisation du registre des données puis la sécurisation de leurs outils informatiques, mise en place de mot de passe, d'accès restreint et de chiffrement des données ainsi qu'une stratégie de sauvegarde et restauration des données rassemblées.

Bien que la CNIL soit dans une démarche d'accompagnement et de tolérance, il est probable que cette tolérance ne soit que provisoire dans la mesure où le RGPD est en vigueur depuis le 25 mai 2018 et que le médecin libéral ne peut prétendre aujourd'hui ignorer les règles. Pour l'aider dans sa démarche de mise en conformité, il ne faut pas hésiter à faire appel à un délégué à la protection des données qui aura la fonction de chef d'orchestre de la mise en conformité. Ce délégué doit être indépendant et le plus souvent, il s'agit d'un avocat spécialiste de ces questions.

Thibaud VIDAL
Associé fondateur
AARPI CHOLEY & VIDAL Avocats