Protéger les données de santé

Déontologie | Médecin | Numérique | RGPD

Publié le Vendredi 22 mars 2019 • Temps de lecture : 6 mn

Le règlement général sur la protection des données (RGPD) donne un cadre précis au recueil et à la protection de ces données.

Toute personne prise en charge par un professionnel, un établissement ou un réseau de santé a droit au respect de sa vie privée et au secret des informations la concernant. Ce secret couvre, sauf dérogations expressément prévues par la loi, l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé. Ce secret s'impose à tous les professionnels intervenant dans le système de santé.

Qu'est-ce qu'une donnée de santé ?

En tant que médecin, vous êtes amené à recevoir ou à émettre des informations sur vos patients, vous collectez des informations pour gérer votre cabinet (ex : gestion des fournisseurs, des personnels que vous employez, etc.). Ces informations que vous recevez et/ou émettez, à l'occasion de votre activité professionnelle, sont considérées comme des données personnelles.

En pratique, il peut s'agir :

- de données d'identification comme les nom, prénom, adresse, ou numéro de téléphone ;
- d'informations sur la vie personnelle du patient (ex : nombre d'enfants), sa couverture sociale (ex : assurance maladie obligatoire, assurance maladie complémentaire, etc.)
- et surtout d'informations relatives à sa santé (pathologie, diagnostic, prescriptions, soins, etc.), les éventuels professionnels qui interviennent dans sa prise en charge.

Vous détenez également, dans le cadre de votre exercice, le numéro de sécurité sociale des patients (Numéro d'Inscription au Répertoire des Personnes Physiques - NIR) pour facturer les actes réalisés.

Le cadre réglementaire

Le règlement général sur la protection des données (RGPD) est entré en application le 25 mai 2018. La loi française Informatique et Libertés a été adaptée en conséquence par la loi sur la protection des données personnelles en cours de promulgation. Ces deux textes constituent désormais le socle de la nouvelle réglementation sur la protection des données personnelles.

Le RGPD définit les données personnelles comme "toute information se rapportant à une personne physique identifiée ou identifiable" c'est-à-dire une personne physique qui peut être identifiée, directement ou indirectement.

Le guide pratique sur la protection des données personnelles, publié par le conseil national de l'Ordre des médecins, a pour ambition d'orienter les médecins libéraux dans la mise en œuvre des obligations prévues par la nouvelle réglementation sur la protection des données personnelles. En complément de ce guide, la CNIL a édité une fiche thématique : "RGPD et professionnels de santé libéraux : ce que vous devez savoir".

Informer vos patients

Vous devez délivrer aux patients une information portant sur le traitement de leurs données (soit dans votre logiciel de suivi, soit dans votre dossier papier). Cela peut être sous la forme d'une affiche, dans votre salle d'attente : voir la fiche thématique de la CNIL "Traitement de données de santé : comment informer les personnes concernées".

Pas de fichier à déclarer

Avec l'entrée en application du RGPD, il n'est plus nécessaire de déclarer votre fichier auprès de la CNIL.

Sécuriser vos données de santé

Vous devez protéger les données des patients contre des accès non autorisés ou illicites et contre la perte, la destruction ou les dégâts d'origine accidentelle. Vous devez donc mettre en place des mesures de sécurité adaptées (ex : utilisation de la carte professionnel de santé, mot de passe personnel, utilisation d'un système de chiffrement fort en cas d'utilisation d'internet, etc).

Pour vous aider à identifier les mesures de sécurité à mettre en place, vous pouvez consulter le Guide sur la sécurité des données personnelles publié par la CNIL.

Si vos données sont hébergées par un hébergeur de données de santé agréé ou certifié, celui-ci doit vous garantir un niveau de sécurité adapté au risque. Vous devez vérifier ce point et conclure un contrat avec votre prestataire, conformément à l'article L.1111-8 du code de la santé publique. Pour vous aider, le conseil national de l'Ordre des médecins a établi un contrat-type entre un médecin et un hébergeur de données de santé à caractère personnel.

Conseils pratiques pour les médecins libéraux

Les dossiers patients

- Je limite les informations collectées au nécessaire et j'utilise les dossiers patients conformément aux finalités définies (suivi des patients) ;
- Je tiens un registre à jour de mes "traitements" ;
- Je supprime les dossiers patients et de manière générale toute information ayant dépassé la durée de conservation préconisée. À titre d'exemple, les médecins libéraux conservent, conformément aux recommandations du Conseil national de l'Ordre des médecins, les dossiers médicaux des patients pendant 20 ans à compter de leur dernière consultation.
- Je mets en place les mesures appropriées de sécurité de mes dossiers "patients" ;
- J'informe mes patients et m'assure du respect de leurs droits.

La prise de rendez-vous

- Je limite les informations collectées par le prestataire et vérifie la conformité du prestataire avec la réglementation et notamment la présence des mentions obligatoires dans le contrat de sous-traitance que je passe avec lui ;
- Je tiens un registre à jour de mes "traitements" ;
- J'informe mes patients et m'assure du respect de leurs droits.

Les échanges via la messagerie électronique

- J'utilise un service de messagerie sécurisée de santé pour mes échanges avec d'autres professionnels de santé ;
- Si j'utilise une messagerie électronique standard ou des messageries instantanées, je m'assure que ces messageries sont bien sécurisées et adaptées à mon utilisation professionnelle ;
- Je chiffre les pièces jointes lorsque j'utilise des messageries standard sur internet qui ne garantissent pas la confidentialité des messages.

Les échanges via le téléphone portable ou la tablette

- Je sécurise l'accès à mon téléphone ou à ma tablette et à son contenu (mot de passe, chiffrement, etc.)
- Je ne stocke pas d'informations médicales relatives à mes patients sur mon téléphone portable ou ma tablette ;
- Je m'assure que l'accès à mon logiciel de dossiers "patients" sur mon téléphone portable ou ma tablette est sécurisé ;
- Je consulte mon logiciel de dossiers "patients" avec précaution.

Les données collectées dans le cadre de recherche médicales

- Je réalise une analyse d'impact avant la réalisation d'études internes sur les données de mes patients si le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ;
- Dans le cadre de recherches en partenariat avec un tiers, je m'assure que les recherches sont menées conformément à la réglementation ;
- Je tiens à jour le registre des activités de traitement ;
- J'informe mes patients et m'assure du respect de leurs droits.

Le guide pratique sur la protection des données personnelles, publié par le conseil national de l'Ordre des médecins, contient, en annexe, un exemple de notice d'information pour la gestion d'un cabinet médical et de registre des activités de traitement.

En établissement de santé, EHPAD, ou centre de santé

Vous pouvez vous rapprocher de la direction ou de toute personne susceptible de gérer la question des données personnelles. Si votre structure a désigné un délégué à la protection des données (DPO), ce dernier est l'interlocuteur privilégié pour vous renseigner sur l'état de conformité de votre structure au RGPD ou répondre à toutes vos questions.