Guide du praticien par rapport à la RGPD

Cher client, nous sommes à vos côtés quotidiennement pour vous apporter des conseils et solutions à vos problématiques métiers. Vous le savez certainement, la CNIL (Commission Nationale Informatique & Libertés) demande à toutes les entreprises de se mettre aux normes concernant le Règlement Général sur la Protection des Données, ou RGPD, entré en application au 25 mai 2018.

Pour vous aider, nous vous proposons ce guide qui répondra à vos questions.

Quelles informations sur les patients pouvez-vous collecter ?

Les données que vous collectez sur les patients doivent être adéquates, pertinentes et limitées à ce qui est strictement nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostic et de soins.
A titre d'exemple, la collecte d'informations sur la vie familiale d'un patient n'est en principe pas appropriée.

Pouvez-vous transmettre les données de vos patients à tous les professionnels, organismes ou autorités qui vous les demandent ?

Vous devez limiter l'accès aux données de santé de vos patients : seules certaines personnes sont autorisées, au regard de leurs missions, à accéder à celles-ci (ex : équipe de soins d'un établissement de santé intervenant dans la prise en charge sanitaire du patient, secrétaire médicale, organismes d'assurance maladie pour le remboursement des actes et prestations et leur contrôle, etc.).
Ces personnes n'accèdent qu'aux données nécessaires à l'exercice de leur mission.

Par ailleurs, la loi peut autoriser certains tiers à avoir accès aux données de vos patients (ex : les organismes de sécurité sociale dans le cadre de la lutte contre la fraude, etc.).
Un "tiers autorisé" est un organisme qui peut accéder à certaines données contenues dans des fichiers publics ou privés parce qu'une loi l'y autorise expressément.
Ces "tiers autorisés" sont des autorités publiques ou des auxiliaires de justice.

Quelques exemples de "tiers autorisés" :

- L'administration fiscale.
- Les organismes de sécurité sociale, dans le cadre de la lutte contre la fraude, et les organismes en charge de l'instruction, du versement et du contrôle du RSA.
- Les administrations de la justice, de la police et de la gendarmerie.
- Les huissiers de justice.

Il faut cependant que le « tiers autorisé » remplisse certaines conditions pour obtenir des informations contenues dans un fichier :

- Sa demande doit être écrite et préciser le texte législatif justifiant la demande.
- Sa demande doit viser des personnes nommément identifiées ou identifiables (le tiers autorisé ne peut pas avoir accès à l'intégralité d'un fichier).
- Sa demande doit être ponctuelle.
- Sa demande doit préciser les catégories de données auxquelles il souhaite accéder.

Combien de temps pouvez-vous conserver les données que vous collectez sur vos patients ?

Les données que vous collectez sur vos patients doivent être conservées pour une durée déterminée. A 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.

Devez-vous informer les patients dont vous collectez et conservez les données de santé ?

Vous devez délivrer aux patients une information portant sur le traitement de données que vous effectuez pour leur prise en charge (soit dans votre logiciel de suivi, soit dans votre dossier papier). Cela peut être fait sous la forme d'une affiche, dans votre salle d'attente.

Devez-vous recueillir le consentement du patient pour collecter et conserver les données de santé que vous utilisez dans le cadre de votre activité ?

Vous n'avez pas besoin de recueillir le consentement des patients pour collecter et conserver les données de santé les concernant, dans la mesure où leur collecte et leur conservation sont nécessaires aux diagnostics médicaux et à la prise en charge sanitaire ou sociale des patients concernés.
Le consentement pour le traitement de données ne doit pas être confondu avec le consentement requis pour la réalisation de certains actes médicaux.

Etes-vous responsable de la mise en place de mesures de sécurité pour garantir le respect de la confidentialité des données de santé de vos patients ?

Vous devez respecter des règles de sécurité pour protéger les données des patients contre des accès non autorisés ou illicites et contre la perte, la destruction ou les dégâts d'origine accidentelle.
Pour ce faire vous devez mettre en place des mesures techniques et organisationnelles appropriées pour préserver la confidentialité et l'intégrité des données (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, une aide est disponible sur ce lien : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

Devez-vous toujours déclarer les traitements de données personnelles auprès de la CNIL ?

Avec l'entrée en application du RGPD, vous n'avez plus de formalité à accomplir auprès de la CNIL pour les traitements de données personnelles nécessaires à la gestion de votre activité (cabinet médical, d'infirmiers, d'orthophonistes, laboratoire de biologie médicale, officine pharmaceutique, opticien, etc.).
En revanche, vous devez être en mesure de démontrer à tout moment votre conformité aux exigences du RGPD en traçant toutes les démarches entreprises : mise en place d'un registre recensant vos fichiers, modalités de l'information délivrée au patient, actions menées pour garantir la sécurité des données de santé, etc.

Etes-vous obligé de désigner un délégué à la protection des données (DPO) ?

Dès lors que vous exercez à titre individuel, vous n'êtes pas soumis à l'obligation de désigner un DPO. Néanmoins, si en raison de votre activité, vous estimez que vous traitez des données de santé à grande échelle (ex : exercice au sein d'un réseau de professionnels, maisons de santé, centre de santé, dossiers partagés entre plusieurs professionnels de santé, etc.), vous devez soit désigner un DPO en interne, soit solliciter les services d'un DPO externe (consultants, cabinets d'avocats, etc.).

Devez-vous tenir un registre des activités de traitement des données ?

La constitution et le maintien d'un registre est une obligation prévue par le RGPD. Elle s'applique à toutes les structures qui traitent des données personnelles de façon régulière dans le cadre de leurs activités. Dans la mesure où vous mettez en œuvre des traitements des données pour l'exercice de votre activité professionnelle, vous devez tenir un registre des activités de traitement des données et le renseigner. La tenue de ce registre est l'occasion de se poser les bonnes questions et de limiter les risques au regard des principes du RGPD.

Pour vous aider dans l'élaboration de votre registre, vous pouvez consulter https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Pour faciliter la tenue de ce registre, la CNI propose un modèle que vous trouverez en suivant ce lien : https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf
Il est destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Une fois renseigné, devez-vous transmettre votre registre des activités de traitement des données à la CNIL ?

Votre registre doit être conservé en interne : il vous permet de documenter votre conformité au RGPD. Ainsi, la CNIL n'est pas destinataire des registres des activités de traitement des données des professionnels de santé. Néanmoins, si vous faites l'objet d'un contrôle de la CNIL, vous devez être en mesure de le mettre à disposition des agents de la CNIL effectuant le contrôle.

Devez-vous mener une analyse d'impact pour tous les traitements des données que vous mettez en place dans le cadre de votre activité (ex : gestion du suivi du patient, fournisseurs, salariés, etc.) ?

Dès lors que vous exercez à titre individuel, vous n'êtes pas soumis à l'obligation de mener une analyse d'impact pour les traitements que vous menez dans le cadre de votre activité.

Nous espérons que ce guide vous aura aidé dans vos démarches administratives.

La direction de Topaze Télévitale.