Foire aux questions

Les dispositions du RGPD s'appliquent-ils uniquement aux traitements informatisés (ex : logiciel utilisé pour la tenue du dossier patient) ou s'appliquent-elles aussi à mes dossiers papiers ?

Les dispositions du RGPD s'appliquent à **tous** les traitements de données personnelles *(ex : nom, prénom, numéro de registre national, etc.)* que vous utilisez dans le cadre de l'exercice de votre mission de soin, que ces traitements soient sous une forme électronique *(ex : logiciel de gestion de votre cabinet médical, logiciel utilisé pour l'exploitation de votre pharmacie, de votre cabinet de kinésithérapeutes, etc.)* ou papier *(ex : dossier patient papier)*.

Quelles informations sur les patients puis-je collecter ?

Les données que vous collectez sur vos patients et que vous inscrivez dans les dossiers de vos patient 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. Toutes les données que votre patient a pu vous révéler, dans le cadre de vos échanges, ne doivent pas nécessairement être intégrées dans son dossier médical. Seules les données qui sont pertinentes et utiles au suivi thérapeutique de votre patient peuvent être enregistrées et conservées. *A titre d'exemple, la collecte d'informations sur la vie familiale d'un patient n'est en principe pas pertinente.*

Combien de temps puis-je conserver les données que je collecte sur mes patients ?

Les données que vous collectez sur vos patients doivent être **conservées pour une durée déterminée**. *A titre d'exemple, les médecins généralistes sont, conformément à l'article 24 du Code de déontologie médicale, tenus de conserver les dossiers médicaux pendant 30 ans à compter de leur dernière consultation avec le patient.*

Puis-je 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 légitimement autorisées, au regard de leurs missions, à accéder à celles-ci *(ex : une équipe de soins d'un établissement de santé intervenant dans la prise en charge sanitaire du patient, une secrétaire médicale, les 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 *(ex : le secrétaire médical accède aux*

données administratives permettant de gérer les prises de rendez-vous mais n'accède pas à la totalité du dossier médical).

A l'heure actuelle, les données de santé deviennent des ressources prisées du monde extérieur, ce pourquoi vous pourriez être sollicités par des acteurs économiques. Assurez-vous de ne pas transmettre les données personnelles de vos patients à ces acteurs qui ne sont pas légitimement autorisés à accéder à celles-ci (*ex : compagnies d'assurance, start-up commerciales…*)

✎ Dois-je informer mes patients que je collecte et conserve leurs données de santé ?

Vous devez **informer explicitement vos patients que leurs données personnelles sont recueillies et traitées en vue d'assurer une prise en charge optimale de leur santé en conformité avec le RGPD**. Cette information peut se faire par voie d'affichage, dans la salle d'attente, ou par la remise d'un document spécifique (*ex: dépliant remis au patient ou mis à disposition dans la salle d'attente*).

✎ Dois-je recueillir le consentement du patient pour collecter et conserver les données de santé que j'utilise pour la mise en œuvre de mon activité professionnelle ?

Vous n'avez pas besoin de recueillir le consentement de vos 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** du patient a toutefois vocation à s'appliquer dans le cadre **d'un échange électronique et sécurisé des données de santé**. Aucun partage de données médicales ne pourra s'effectuer au travers du Réseau Santé Wallon sans avoir préalablement recueilli le consentement du patient.

Un consentement libre, spécifique et éclairé est également requis pour la participation à des recherches scientifiques et études cliniques.

✎ Suis-je responsable de la mise en oeuvre de mesures de sécurité pour garantir le respect de la confidentialité des données de santé de mes patients ?

En tant que responsable du traitement des données que vous effectué dans le cadre de votre mission de soins, vous êtes tenus de respecter des règles de sécurité pour protéger les données de vos 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 d'un mot de passe personnel, utilisation d'un antivirus et d'une protection « firewall » en cas de connexion à Internet, une*

bonne gestion des backups, l'utilisation d'une messagerie sécurisées et cryptées telle qu'e-Hbox, etc.).

Si vous passez par un prestataire de service qui traite des données en votre nom et pour votre compte, celui-ci doit, en tant que sous-traitant, vous garantir un niveau de sécurité adapté au risque. Vous devez vérifier ce point et conclure un contrat de sous-traitance avec votre prestataire précisant les mentions obligatoires de l'article 28 du RGPD.

✎ Dois-je encore déclarer les traitements de données personnelles auprès la Commission de la vie privée ?

Depuis l'entrée en application du RGPD, **vous n'avez plus de formalité à accomplir auprès de l'ex-Commission vie privée, aujourd'hui appelée « autorité de protection des données » (ADP),** pour les traitements de données personnelles nécessaires à la gestion de votre activité professionnelle.

En revanche, **vous devez être en mesure de démontrer à tout moment votre conformité avec les exigences du RGPD en documentant toutes les démarches que vous entreprenez** : mise en place d'un registre recensant les activités de traitement des données personnelles, notice d'information délivrée au patient, actions menées pour garantir la sécurité des données de santé, etc.

✎ Dois-je tenir un registre des activités de traitement ?

La tenue d'un registre des activités de traitement est une nouvelle obligation prévue par l'article 30 du 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 pour l'exercice de votre activité professionnelle *(ex : pour la gestion de votre cabinet, pour l'exploitation de votre pharmacie, pour votre cabinet de kinésithérapeutes, etc.)*, vous devez tenir un registre des activités de traitement 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. Avez-vous vraiment besoin de cette donnée dans le cadre de votre activité ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.

✎ Une fois mon registre des activités de traitement constitué, dois-je le transmettre aux personnes qui en feraient la demande ?

Par nature, le registre est un **document interne et évolutif** qui doit avant tout vous aider à piloter votre conformité avec les exigences du RGPD. Ainsi, **il n'a pas vocation à être mis à la disposition du public, en ce compris le patient et ses proches.**

Le registre doit toutefois pouvoir être communiqué à l'autorité de protection des données lorsqu'elle en fait la demande. Elle pourra notamment l'utiliser dans le cadre de sa mission de contrôle des traitements de données.

✎ Suis-je obligé de désigner un délégué à la protection des données (DPO) ?

Dès lors que vous exercez votre activité professionnelle à titre individuel, vous n'êtes pas soumis à l'obligation de désigner un DPO.

En revanche, si vous exercez votre activité au sein d'un réseau de professionnels, au sein d'une maison de santé ou d'un centre de santé, **la désignation d'une personne référente pour la protection des données est encouragée**. Cette personne serait en charge d'assurer la mise en conformité réglementaire du RGPD et aurait notamment pour mission de veiller à sensibiliser l'équipe de soins et les autres membres du cabinet à la protection des données, à tenir et à mettre à jour le registre des activités de traitement, à être la personne de référence pour toutes questions relatives à la protection des données et à être la personne de référence pour centraliser les fuites de données et en faire rapport à l'autorité de protection des données.

✎ Dois-je réaliser une analyse d'impact pour tous les traitements que je réalise dans le cadre de mon activité professionnelle (ex : gestion du suivi du patient, fournisseurs, salariés, etc.) ?

Dès lors que vous exercez votre activité 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. Néanmoins, si en raison de votre activité, vous estimez que **vous traitez des données de santé à grande échelle**, vous devez mener une analyse d'impact pour les traitements concernés.

En cas de doute quant à la nécessité d'effectuer une analyse d'impact et dans la mesure où l'analyse d'impact est un outil important pour les responsables du traitement aux fins du respect de la législation sur la protection des données, **il est recommandé d'en effectuer une malgré tout.** La réalisation d'une analyse d'impact est indépende de l'obligation d'assurer la confidentialité et la sécurité des données de vos patients.

Par Emeraude Camberlin, juriste