Foire aux questions

Listes des questions

1. Le RGPD s'applique-t-il aussi aux fiches papiers que je tiens sur mes patients ?
2. Dois-je obtenir le consentement de mes patients pour traiter et conserver leurs données à caractère personnel ?
3. Quelles informations personnelles puis-je collecter sur mes patients ?
4. Combien de temps puis-je conserver les données de mes patients ?
5. Comment puis-je informer mes patients sur la protection de leurs données personnelles ?
6. Dois-je encore déclarer les traitements de données personnelles auprès la Commission de la vie privée ?
7. Suis-je soumis à l'obligation de tenir un registre des traitements ?
8. Une fois mon registre des activités de traitement constitué, dois-je le transmettre à toute personne qui en ferait la demande ?
9. Suis-je obligé de désigner un délégué à la protection des données (DPO pour *Data Protection Officer*)?
10. Les confrères à qui j'adresse mes patients sont-ils considérés comme mes sous-traitants ?
11. Que faire lorsqu'un sous-traitant, à qui j'ai envoyé un contrat relatif à la protection des données, ne répond pas ou ne refuse de signer ledit contrat ?
12. Quelles sont les mesures de sécurité que je dois prendre pour assurer la confidentialité et la sécurité des données de mes patients ?
13. Suis-je responsable des manquements RGPD des membres de mon personnel ?
14. Si j'ai obtenu le consentement de mon patient, puis-je lui transmettre par email ses résultats médicaux, un rapport de laboratoire ou encore une prescription électronique ?
15. Lors d'un cambriolage dans mon cabinet, certains dossiers de mes patients ont disparus, que dois-je faire ?
16. Puis-je transmettre les données de mes patients à tous les professionnels, organismes ou autorités qui en feraient la demande ?
17. Dois-je réaliser une analyse d'impact pour tous les traitements de données que je réalise dans le cadre de mon activité professionnelle (ex : gestion du suivi du patient, fournisseurs, salariés, etc.) ?
18. Dans le cadre de leur mission de santé publique, les autorités organisent des études prospectives. A cette fin, elles m'adressent un questionnaire à soumettre à mes patients. Quelles sont les démarches à réaliser pour être en conformité avec le RGPD ?
19. L'Autorité de Protection des Données (APD) peut-elle me sanctionner ?

Q1. Le RGPD s'applique-t-il aussi aux fiches papiers que je tiens sur mes patients ?

Le RGPD s'applique à tout traitement de données à caractère personnel, que ce traitement de données se présente sous une forme papier ou sous une forme électronique.

Par conséquent, si vous tenez un dossier patient, sous forme papier (fiches patients) ou sous une forme informatique (vous disposez d'un logiciel métier), vous êtes soumis aux exigences du RGPD.

Q2. Dois-je obtenir le consentement de mes patients pour traiter et conserver leurs données à caractère personnel ?

Vous n'avez pas besoin de recueillir le consentement de vos patients pour collecter et conserver leurs données personnelles (données de santé ou données administratives)**,** dans la mesure où leur collecte et leur conservation sont nécessaires aux diagnostics médicaux et à la prise en charge sanitaire ou sociale de vos patients.

Le **consentement** du patient a toutefois vocation à s'appliquer dans le cadre **d'un échange électronique et sécurisé des données de santé entre prestataires de soins**. Aucun partage de données médicales ne pourra s'effectuer au travers du Réseau Santé Wallon sans avoir préalablement recueilli le consentement du patient.

Q3. Quelles informations personnelles puis-je collecter sur les patients?

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.

Q4. 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 sont tenus, conformément à l'article 46 du Code de déontologie médicale, de conserver les dossiers médicaux pendant 30 ans à compter de leur dernière consultation avec le patient.*

Q5. Comment puis-je informer mes patients sur la protection de leurs données ?

Vous avez une obligation de transparence vis-à-vis de vos patients. Informez-les que **leurs données personnelles sont recueillies et traitées en vue d'assurer une prise en charge optimale de leur santé et que le traitement de leurs données se fait de façon responsable en conformité avec les exigences du RGPD**. Cette information peut se faire par voie d'un 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*).

Q6. 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 vos patients, etc.

Q7. Suis-je soumis à l'obligation de tenir un registre des activités de traitement de données ?

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.

Un modèle de registre des activités de traitement est disponible sur notre site internet.

Q8. Une fois mon registre des activités de traitement constitué, dois-je le transmettre à toute personne qui en ferait 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 « grand public », en ce compris le patient et ses proches.**

Toutefois, le registre doit **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.

Q9. Suis-je obligé de désigner un délégué à la protection des données (DPO pour *Data Protection Officer*) ?

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.

Q10. Les confrères à qui j'adresse mes patients sont-ils considérés comme mes sous-traitants ?

Vos confrères ne rentrent pas dans la définition de « sous-traitant » au sens du RGPD. Ils sont considérés comme des responsables de traitement, au même titre que vous. En effet, ils ne traitent pas de données personnelles pour votre compte et selon vos instructions, ils traitent votre demande

de manière autonome, en déterminant les finalités et les moyens de traitement nécessaires pour l'exercice de leur activité professionnelle.

Les sous-traitants dans le milieu de la santé sont tout particulièrement **votre logiciel métier, le Réseau Santé Wallon, les sociétés qui offrent un service d'agenda en ligne, les secrétariats sociaux, les services *cloud*...**

En toute hypothèse, dès que vous sollicitez les services d'un sous-traitant, vous devez **formaliser la relation que vous entretenez avec eux par un contrat de sous-traitance** conforme avec l'article 28 du RGPD**.** Il s'agit là d'une nouvelle obligation du RGPD.

Q11. Que faire lorsqu'un sous-traitant, à qui j'ai envoyé un contrat relatif à la protection des données, ne répond pas ou ne refuse de signer ledit contrat ?

Si le RGPD n'instaure pas de délai dans lequel le sous-traitant est tenu de répondre, il est évident que tant votre responsabilité que celle de votre sous-traitant seraient engagées si vous ne parveniez pas à conclure un contrat de sous-traitance conforme à l'article 28 du RGPD. Comme il est de votre responsabilité de faire appel uniquement à des sous-traitants présentant des garanties suffisantes en termes de protection des données, **deux possibilités** se présentent à vous :

- soit vous entrez dans des négociations contractuelles avec votre sous-traitant ;
- soit vous décidez de ne plus recourir aux services de ce prestataire.

Veillez à acter et à conserver les échanges avec votre sous-traitant pour prouver votre bonne foi vis-à-vis de l'autorité de protection des données.

Q12. Quelles sont les mesures de sécurité que je dois prendre pour assurer la confidentialité et la sécurité des données de mes patients ?

La gestion des accès est un élément essentiel à la confidentialité et à la sécurité des données de vos patients. Veillez donc à sécuriser suffisamment les accès aux données de vos patients.

En particulier :

- prévoyez une authentification forte pour l'accès à votre logiciel métier. Un mot de passe est individuel et ne peut pas être partagé ;
- fermez vos portes à clé après vos consultations ;
- verrouillez systématiquement votre poste de travail lorsque vous vous absentez ;
- utilisez un antivirus et une protection « firewall » en cas de connexion à Internet ;
- limitez les accès aux informations aux seules personnes autorisées et aux seules informations dont elles ont besoin pour leur fonction ;
- sensibilisez les membres votre personnel au caractère confidentiel des données patients ;
- formalisez vos relations avec vos sous-traitants (contrats) ;
- ayez une bonne gestion de vos backups ;
- utilisez des moyens de communication avec votre patient sécurisés (ex : utilisation de la messagerie sécurisées et cryptées) ;
- …

Besoin d'aide ? Consultez et impliquez votre informaticien !

Q13. Suis-je responsable des manquements RGPD des membres de mon personnel ?

Oui, les membres de votre personnel **agissent sous votre autorité directe**. Il est donc de votre responsabilité de les sensibiliser aux exigences du RGPD en veillant notamment à ce qu'ils

- soient informés de la nature confidentielle des données à caractère personnel de vos patients ;
- aient suivi une formation appropriée sur la protection de vie privée, du secret professionnel et de la législation relative à la protection des données ;
- suivent une procédure d'identification lorsqu'ils accèdent à des données confidentielles ;
- soient soumis à des dispositions contractuelles (dans leur contrat de travail) ou à une obligation légale ou professionnelle de confidentialité.

Conscientisez vos collaborateurs aux mesures de sécurité qui protègent les données de vos patients et **déterminez qui a accès et à quelles données**.

Q14. Si j'ai obtenu le consentement de mon patient, puis-je lui transmettre par e-mail ses résultats médicaux, un rapport de laboratoire ou encore une prescription électronique ?

Comme le précise l'ordre des médecins dans son avis du 27 avril 2019 sur le RGPD, « *le transfert de données de santé doit se faire d'une façon particulièrement sécurisée. Les données de santé ne peuvent être envoyées numériquement que par des systèmes avec authentification à plusieurs facteurs. Par conséquent,* ***le médecin ne peut pas envoyer de données médicales par e-mail non sécurisé, même pas dans le cas où le patient a marqué son accord****. Le médecin doit utiliser les applications de réseaux d'informations sécurisées, avec un niveau de sécurisation conforme aux règles en vigueur* ».

L'e-mail « standard », même s'il représente une voie de communication très importante pour de nombreux secteurs, **n'est pas reconnu aujourd'hui comme un moyen de communication sûr pour transmettre des données de santé**. Vous êtes dès lors invités à utiliser une messagerie électronique sécurisée au moyen de garanties forte (chiffrement du message et des pièces jointes) telle que la EHbox.

Si vous ne disposez pas d'une messagerie électronique sécurisée **telle qu'une messagerie encryptée,** il semble plus opportun de recourir à un autre moyen de communication considéré comme davantage sécurisé :

- L'envoi de courriers sensibles par **la poste (sous le cachet « confidentiel »)** reste une voie de communication considérée par le RGPD comme suffisamment respectueuse de la protection de la vie privée des patients ;
- A côté de cette voie de communication "classique", vous pouvez également utiliser la voie du réseau de santé coordonné, le **Réseau Santé Wallon,** via lequel il est possible de publier des rapports d'examens médicaux.

Q15. Lors d'un cambriolage dans mon cabinet, certains dossiers de mes patients ont disparus, que dois-je faire ?

La première chose à faire est certainement de porter plainte auprès des services de police.

Vous noterez qu'un vol de dossiers médicaux est considéré comme une fuite de données au sens du RGPD et doit, à ce titre, être notifiée à l'Autorité de Protection des Données (APD) dans les 72 heures à partir de la constatation des faits.

Pour pouvoir remplir au mieux le formulaire de notification d'une fuite de données à l'APD, **évaluez ce qui vous a été dérobé en termes de « données à caractère personnel »** : nombre de dossiers patients concerné par le vol, nombre de patients concernés, quelles informations ont-été dérobées,

s'agit-il de données sensibles, des mesures de sécurité ont-elles été prises (back-ups, mesures de cryptage, accès limités aux données…)? Etc.

Réfléchissez également sur **les conséquences possibles pour les droits et libertés des patients concernés** par le vol de leurs données (atteinte à son intégrité physique ou morale, discrimination,…).

Vous devez enfin **mettre toutes les précautions nécessaires pour limiter les risques** d'atteinte à la vie privée de vos patients et veiller à **mettre toutes les protections nécessaires autour des données** de vos patients pour que cela ne se reproduise plus.

Q 16. Puis-je transmettre les données de mes patients à tous les professionnels, organismes ou autorités qui en feraient la demande ?

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 de sécurité sociale pour le remboursement des actes et prestations et leur contrôle, le SPF Santé, 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 devez être vigilants ! 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…*)

Q17. Dois-je réaliser une analyse d'impact pour tous les traitements de données 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.

Q18. Dans le cadre de leur mission de santé publique, les autorités organisent des études prospectives. A cette fin, elles m'adressent un questionnaire à soumettre à mes patients. Quelles sont les démarches à réaliser pour être en conformité avec le RGPD ?

Dans ce cadre, vous devez :

- informer vos patients sur les modalités et les finalités de la collecte de leurs données ;
- veillez à ce que les formulaires soient anonymisés, à tout le moins pseudonymisés ;
- communiquer les questionnaires remplis via un outil sécurisé.

Q19. L'Autorité de Protection des Données (APD) peut-elle me sanctionner ?

Si vous ne respectez pas les grands principes et les obligations du RGPD, vous pouvez faire l'objet d'une **amende administrative** de l'APD, voire d'une **sanction pénale.** Nonobstant, l'Autorité de Protection des Données (APD) peut préférer vous imposer d'adopter des **mesures correctrices** (par exemple, mise en conformité dans un délai déterminé, limitation de traitement, rectification ou effacement de données). Le juge vous comparera toujours à un autre prestataire de soins normalement prudent et diligent placé dans les mêmes circonstances.

L'essentiel est donc de pouvoir démontrer dès à présent à l'APD que vous vous êtes engagé dans une démarche sérieuse de mise en conformité.

Mise à jour le 09/12/2019