Version mai 2022

RGPD : Foire aux questions

Astuce : pour effectuer une recherche sur mot-clé : « CTRL + F »

Contenu :

I. Généralités

✎ Le RGPD s'applique-ils uniquement aux traitements informatisés (ex : logiciel utilisé pour la tenue du dossier patient) ou s'applique-t-il aussi à mes dossiers papiers ?

Le RGPD s'applique à **tous** les traitements de données à caractère personnel que ces traitements soient sous une forme électronique (ex. tenue du dossier médical informatisé) ou papier (ex. fiches patients).

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

Les dossiers médicaux doivent être conservés pendant minimum 30 ans et maximum 50 ans à compter du dernier contact avec votre patient.

✎ Puis-je transmettre les données de mes patients à tous les professionnels, organismes ou autorités qui me les demandent ?

Vous devez limiter l'accès aux données de santé de vos patients aux seuls besoins des personnes qui 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)*.

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

Oui. 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*).

Version mai 2022

Téléchargez votre affiche sur https://e-santewallonie.be/rgpd/

✎ Dois-je recueillir le consentement du patient pour collecter et conserver les données de santé que j'utilise pour la tenue de mes dossiers patients ?

Non. 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 éclairé 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 œuvre de mesures de sécurité pour garantir le respect de la confidentialité des données de santé de mes patients ?

Oui. En tant que responsable de traitement, 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-Healthbox, 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.

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

Si 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 médicale ou d'un centre de santé, vous devez évaluer si vous faites un traitement de données à large échelle (ex. plus de 10 000 patients/ seuil annuel). **Dans tous les cas, la désignation d'une personne référente pour la protection des données est encouragée** au sein du réseau de professionnels concernés. 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.

Version mai 2022

✎ 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.) ?

Si vous exercez votre activité à titre individuel, non.

Néanmoins, si en raison de votre activité, vous considérez que **vous traitez des données de santé à grande échelle (ex. 10 000 patients par an/seuil annuel)**, vous devez mener une analyse d'impact pour les traitements concernés.

✎ La désignation d'un délégué à la protection des données (DPO) est-il obligatoire pour une pratique solo ?

Non car la désignation d'un délégué à la protection des données est requise lorsqu'il y a un traitement de données de santé à large échelle. Le RGPD précise en son considérant 91 que *« le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients par un médecin ou un autre professionnel de la santé exerçant à titre individuel »*. Par conséquent, la désignation d'un délégué à la protection des données n'est pas obligatoire pour un prestataire de soins exerçant son activité à titre individuel.

✎ Si je travaille en cabinet collectif/de groupe mais que chacun des prestataires gère ses dossiers patients, prises de rendez vous, … comme indépendants et en version « location de plage horaire d'une pièce de soins », tombe-t-on sous la règle du critère de « large échelle » qui impose la désignation d'un DPO et d'une analyse d'impact ?

Non car chacun des prestataires agit ici comme responsables de traitement indépendamment des autres prestataires de soins. Par conséquent, vous êtes considérés comme travaillant à titre individuel, auquel cas la désignation d'un DPO et la réalisation d'une analyse d'impact ne s'appliquent pas.

✎ L'affiche RGPD doit-elle être mise dans la salle d'attente du cabinet ET sur le site internet ?

L'information doit être communiquée au patient, peu importe le moyen choisi. La salle d'attente et le site internet sont deux moyens complémentaires pour informer le patient.

✎ Quels sont les moyens de communication sécurisés recommandés pour échanger des données relatives à mes patients ?

- Le Réseau santé wallon
- La boite mail eHealthBox
- L'application MyRSW (prochainement disponible)

✎ Quel outil mettre en place entre un maitre de stage et son assistant pour respecter le RGPD ?

Version mai 2022

Il convient d'apposer une clause de confidentialité et de protection des données dans la convention de stage et de sensibiliser l'assistant aux obligations du RGPD.

✎ Quelles mesures de sécurité mettre pour une clé USB sur laquelle est réalisée une sauvegarde de données sensibles ?

Il est recommandé d'utiliser un chiffrement des données et de conserver la clé de chiffrement de manière sécurisée.

II. Dossier patient

✎ Mon fournisseur de logiciel métier est-il un sous-traitant RGPD ?

Oui car il traite des données relatives à votre patient pour votre compte et selon vos instructions.

✎ Le Réseau Santé Wallon/Bruxellois est-il un sous-traitant RGPD ?

Oui. La FRATEM agit en qualité de sous-traitant. Pour plus d'informations : https://www.reseausantewallon.be/SiteCollectionDocuments/Documents-officiels-EN/RVP-EN.pdf

✎ Comment s'assurer que notre sous-traitant est conforme avec le RGPD?

Avant de faire appel à un sous-traitant, il est de votre responsabilité de vérifier qu'il présente suffisamment de garanties quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement des données qui lui est confié réponde aux exigences du RGPD et garantisse la protection des droits et libertés de vos patients. En ce sens, vous pouvez lui adresser un **questionnaire de sécurité** pour connaître quelles sont les mesures qui permettent d'assurer la confidentialité, l'intégrité et la disponibilité des données. Une fois votre sous-traitant sélectionné, vous devez conclure un **contrat de sous-traitance** avec lui (article 28 du RGPD).

✎ Existe-t-il un logo ou un sigle indiquant que le logiciel avec lequel un prestataire de soins travaille est conforme avec le RGPD ?

A ce jour, non.

✎ Si mon comptable a accès aux extraits de compte sur lesquels sont repris les noms et traitements de mes patients, mon comptable est-il un sous-traitant RGPD ?

Oui car il va traiter des données personnelles pour votre compte et selon vos instructions. Un contrat de sous-traitance est alors nécessaire (article 28 du RGPD).

Je tiens un dossier patient sous format papier, suis-je soumis au RGPD ?

Oui. Le RGPD s'applique à **tous** les traitements de données à caractère personnel que ces traitements soient sous une forme électronique ou papier (ex. fiches patients).

Le secrétariat social est-il aussi un sous traitant ?

Oui. Pour un grand nombre d'activités, votre secrétariat social agit en qualité de sous-traitant (par ex. : l'activité d'administration des salaires dans les différentes entités secrétariat social) car il traite des données personnelles d'employés sur base de vos instructions.

Est-ce que le RGPD s'applique aussi aux médecins-conseils des mutuelles ?

Oui.

Comment envoyer un document à nos patients de manière sécurisée ?

- Via le réseau santé wallon si le patient a consenti au partage électronique de ses données de santé.
- Via l'application MyRSW (prochainement disponible)
- Via un courrier confidentiel
- Via un autre moyen qui atteste de la sécurité des données (ex. chiffrement des données de bout en bout et au repos).

Comment puis-je renforcer la sécurité de mes données ?

1. Chiffrez vos données sensibles et conservez en toute sécurité vos clés privées.

Voir question « Comment chiffrer mes données ». Une fois vos données chiffrées, n'oubliez pas de faire une copie de vos clés privées soit sur une clé usb placée dans un coffre, soit une copie dans un répertoire de votre ordinateur qui soit protégé et chiffré lui aussi. Ne stockez pas vos clés dans la même pièce que vos ordinateurs et, ne transmettez pas vos clés privées et mot de passe via mail et/ou web mail, ces canaux ne sont pas sécurisés et peuvent être piratés.

2. Choisissiez un mot de passe sûr et utilisez une authentification à plusieurs facteurs

Changez régulièrement votre mot de passe et utilisez un **mot de passe complexe** contenant des majuscules, minuscules, chiffres et caractères spéciaux. Gardez à l'esprit que la menace ne vient pas de vous mais de l'extérieur. Les mots de passe de type "test", prénoms de vos enfants et autres ne vous offrent aucune sécurité.

Version mai 2022

Vous pouvez également recourir à un **gestionnaire de mot de passe** (ex. KeePass, Lastpass, Dashlane, 1Password, Botwardn, NordPass, Kaspersky…).

Pour vous authentifier, c'est-à-dire pour priver votre identifié lorsque vous vous connectez à votre ordinateur ou logiciel, pensez à recourir à au moins deux moyens différents. L'authentification à plusieurs facteurs est un procédé de sécurité. Par exemple, connectez-vous avec un mot de passe + un code envoyé par sms ou bien un mot de passe + lecture de votre carte d'identité ou un mot de passe + votre empreinte digitale.

3. Protégez votre système d'information

Vérifiez l'installation et la configuration des différentes parties de votre infrastructure et installez des couches de sécurité sur votre réseau. Veillez à avoir un Firewall, anti-virus mis à jour, protection des connexions Internet, ...

Comment chiffrer mes données ?

Le chiffrement des données est une méthode qui consiste à protéger ses documents en les rendant illisibles par toute personne n'ayant pas accès à une clé dite de déchiffrement.

Il existe divers outils gratuits qui permettent de chiffrer de cette façon des fichiers. Par exemple :

- Une bonne solution gratuite est **GnuPGP**, également connu sous le nom de GPG. Disponible sur : https://gnupg.org
- **7-Zip** (prononcer « seven zip ») est un logiciel qui permet de compresser un ou plusieurs documents, et de les chiffrer. Il est gratuit, téléchargeable sur 7-Zip.org, disponible en français et librement redistribuable.
- **Peazip** est un logiciel libre semblable à 7-Zip. Il est gratuit, téléchargeable sur www.peazip.org, disponible en français et librement redistribuable.
- **VeraCrypt** est un logiciel libre qui permet de chiffrer un répertoire sous Windows, Mac et GNU/Linux.
- **Zed!** est un outil de chiffrement plus avancé, développé par la société Prim'X, dont une version de découverte gratuite permet de chiffrer des fichiers jusqu'à 200 Mo.

Vous trouverez sur internet différents tutoriels pour vous expliquer comment utiliser ces outils.

Les conditions générales d'utilisation du logiciel patient mentionnent des clauses relatives au RGPD et renvoi vers un contrat RGPD. Est-ce valable pour avoir un contrat de sous-traitance RGPD en bonne et due forme ?

Oui, si les conditions générales et le contrat associé mentionnent bien les éléments et clauses obligatoires de l'article 28 du RGPD.

✎ Si un médecin conseil demande nos notes personnelles pour une expertise médicale suite à un accident peut-on ou doit-on lui fournir?

Les annotations personnelles d'un praticien professionnel et les données concernant des tiers n'entrent pas dans le cadre du droit de consultation du dossier du patient (article 9 loi sur les droits du patient).

✎ Doit-on conserver les dossiers patients en version papier si ceux-ci ont été numérisés ?

Non. Une sauvegarde numérisée suffit.

✎ Si un patient souhaite que ses données soient supprimées, quel délai avons-nous pour lui répondre? Comment informer le patient?

Le droit de suppression ne s'applique pas car en tant que prestataire de soins vous avez l'obligation de conserver les données pendant minimum 30 ans et maximum 50 ans à compter du dernier contact avec votre patient. Toutefois, vous avez 30 jours maximum pour lui répondre. Vous pouvez informer votre patient au sujet de l'exercice de leurs droits via l'apposition d'une affiche dans votre salle d'attente (affiche prête à télécharger https://e-santewallonie.be/rgpd/).

✎ Un contrôleur du fisc qui accède à mes extraits de compte et des noms qui y figurent est-il un sous-traitant ?

Non. Il agit en qualité de responsable de traitement indépendemment de vous.

✎ Arrivés à la pension à 67 ans, dois-je encore conserver les dossiers patients ?

Lorsque votre pratique cesse, vous devez en informer de manière proactive vos patients en les invitant à leur faire savoir à quel prestataire vous devez transmettre les renseignements utiles pour garantir la continuité des soins ou si le patient préfère recevoir ceux-ci directement. Pour la conservation des dossiers et leur transmission, vous pouvez recourir à un prestataire de service en charge du stockage de vos données confidentielles.

Si vous êtes médecin, et que vous n'êtes pas en mesure de trouver un confrère, vous vous adressez au cercle des médecins généralistes ou au conseil provincial de l'Ordre pour l'aider à trouver un médecin prêt à assumer cette tâche. Le cercle de médecins généralistes peut lui-même se charger de la conservation de ces dossiers, sous la responsabilité de son président. En dernier recours, il incombe au conseil provincial de trouver une solution pour la conservation adéquate des dossiers des patients, afin de garantir la continuité des soins et la préservation du secret professionnel.

✎ Quelle est la responsabilité RGPD de la banque et des moyens de payement électronique ?

Ils agissent en qualité de responsable de traitement indépendamment de vous. Ils ne sont donc pas vos sous-traitants. Un contrat de sous-traitance RGPD n'est donc pas nécessaire avec eux.

Est-ce autorisé d'envoyer des résultats par mail, comme beaucoup trop souvent demandé (exemple ordonnance ou résultat de labo)?

Uniquement si l'email est sécurisé (ex. chiffrement des données de bout en bout et au repos).

Dois-je tenir un registre des activités de traitement si j'exerce mon activité en « solo »?

Oui. La tenue d'un registre des activités de traitement est une obligation qui s'impose à tous les prestataires de soins, qu'ils exercent leur activité en « solo » ou en groupe.

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

Le registre est un **document interne**. 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.

Les données des cabinets et des patients sont stockées sur le cloud et gérées par le fournisseur du logiciel. Quelle est la part de responsabilité de ce fournisseur par rapport au prestataire de soins?

Votre fournisseur de logiciel, en qualité de sous-traitant, a aussi des obligations RGPD. Il s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles autour de la tenue des dossiers patients. Ce sous-traitant s'engage aussi à une obligation de collaboration et d'assistance à votre égard. L'ensemble de ses obligations et responsabilités se trouvent dans le contrat de sous-traitant conclu avec vous.

Si je travaille en solo mais que je suis remplacé à l'occasion. Suis-je toujours considéré comme un prestataire de soins qui travaille en solo ?

Oui. Dans cette dernière hypothèse, votre remplaçant interviendrait comme tiers responsable.

En travaillant en solo, dois-je tenir un registre des traitements de données ?

Oui. La tenue d'un registre des traitements s'impose à tous prestataires de soins qui exerçent une activité libérale, en solo ou en pratique de groupe.

Si on décède, est ce que l'obligation de la conservation des dossiers médicaux s'arrête ? Ou nos descendants/proches/collègues sont-ils tenus de conserver les dossiers patients ?

L'obligation de conserver les dossiers médicaux ne s'arrête pas à votre décès mais après minimum 30 ans et maximum 50 ans après le dernier contact avec votre patient. La conservation des dossiers médicaux est un éléments de prevueve das le cadre d'une responsabilité déonotologique ou civile. Afin de conserver cette preuve et la protection des données de santé convertes par le secret médical, les dossiers patients doivent être conservés par un autre professionnels de la santé. Par conséquent, veillez à anticiper, de votre vivant, la cessation de vos activités. Lorsque la fin de vos activités approchent, il convient d'en informer de manière proactive vos patients en les invitant à leur faire savoir à quel prestataire vous devez transmettre les renseignements utiles pour garantir la continuité des soins ou si le patient préfère recevoir ceux-ci directement. En pratique, lors du décès d'un prestataires, si certains patients demandent que leur dossier soit confié à leur nouveau médecin, d'autres ne se manifestent pas et la famille se retrouve dans l'embarras, ne sachant comment gérer de tels volumes d'archives si aucun confrère n'accepte de s'en occuper. Il est dès lors primordial que vous anticipiez cette situation de votre vivant.

Voyez pour plus d'informations : https://ombbw.be/images/documents/conservation_DM.pdf

✎ Suis-je censé imprimer toutes les pièces du dossier demandées par le patient lorsqu'il souhaite exercer son droit d'accès ? Et si oui, à quel tarif?

Conformément à la loi sur les droits du patient, le patient peut exercé son droit à une copie de son dossier médical. II doit être donné suite au patient dans les meilleurs délais et au plus tard dans les 15 jours de la demande du patient visant à consulter le dossier le concernant. Notez que les annotations personnelles d'un praticien professionnel et les données concernant des tiers n'entrent pas dans le cadre de ce droit de consultation. Depuis l'entrée en vigueur du RGPD, la première copie est gratuite. Néanmoins, le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire peut être demandé (article 15 §3 du RGPD).

III. Registre

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

Oui. La tenue d'un registre des activités de traitement est une 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.

✎ 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.

IV. Fuite de données

Comment notifier une fuite de données à l'autorité de protection des données (APD) ?

La notification d'une fuite de données à l'APD se fait au moyen d'un formulaire *ad hoc* en ligne que vous pouvez retrouver sur le site internet de l'APD.

Un mode d'emploi vous est proposé sur notre site (http://www.e-santewallonie.be/rgpd) en vue de vous aider à réaliser en bonne et due forme cette notification à l'APD.