

Obligations des médecins issues de la loi de protection des données

par le Dr Constance AUDET*

* Assistante en médecine générale
1180 Uccle
audet.constance@gmail.com

L'auteure déclare ne pas présenter de liens d'intérêts avec l'industrie pharmaceutique ou de dispositifs médicaux en ce qui concerne cet article.

Les médecins généralistes, en tant que responsables du traitement des données à caractère personnel de leurs patient-es, doivent se conformer à la loi belge du 30 juillet 2018 sur la protection des données, qui intègre les principes du RGPD^a.

Il est important de souligner que le RGPD s'inscrit dans le cadre global du droit fondamental à la vie privée, qui s'applique également dans le domaine des soins de santé, conformément à la loi du 22 août 2002 relative aux droits du/de la patient-e. Les règles de confidentialité liées à la protection de la vie privée complètent les règles sur le secret médical, et aucune ne compromet l'autre.

Le RGPD s'applique à tous les traitements de données à caractère personnel, et ce, **quel qu'en soit le support**, électronique ou papier.

Il est entendu par « **données à caractère personnel** », toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement par un nom, prénom, adresse IP, adresse électronique, numéro de téléphone, certificat médical, imagerie, etc. Le « **traitement des données** » englobe toute action réalisée sur ces données : collecte, enregistrement, organisation, consultation, extraction, diffusion, destruction...

L'Ordre des médecins se tient à disposition des professionnel·les pour répondre aux questions pratiques et recommande de consulter régulièrement les sites des autorités publiques telles que l'Autorité de protection des données^b, l'INAMI^c, et la plate-forme e-santewallonie^d.

Plusieurs questions se posent lorsqu'en tant que médecin nous traitons des données à caractère personnel : suis-je autorisé-e à traiter les données personnelles de ce patient ou patiente ? Suis-je autorisé-e à les transmettre ? Ma patientèle est-elle au courant de ce que je fais de ses données ? Est-ce que je conserve les données de manière sécurisée ?

Se conformer au RGPD implique dès lors le respect de différents principes que nous tenterons ici de résumer.

ABSTRACT

Doctors are responsible by law for their patients' personal data protection. They need to abide by the law of data protection, ruled by the principles of GDPR. The present article aims to help doctors understand and respect the law to better protect their patients' data.

Keywords : personal data, GDPR, data-processing.

RÉSUMÉ

Les médecins, en tant que responsables du traitement des données à caractère personnel de ses patient-es doivent se soumettre à la loi de protection des données intégrant les principes RGPD. Cet article vise à rappeler ces différents principes afin d'aider au mieux les médecins à comprendre et respecter la protection des données des patient-es.

Mots-clés : données à caractère personnel, RPD, traitement des données.

- Le texte complet du RGPD est accessible via le lien suivant : <https://eur-lex.europa.eu/FR/legal-content/summary/general-data-protection-regulation-gdpr.html>
- <https://www.autoriteprotectiondonnees.be/citoyen>
- <https://www.inami.fgov.be/fr/professionnels/information-tous/Pages/reglement-general-protection-donnees.aspx>
- <https://e-santewallonie.be/rgpd/>

Principe de licéité, de loyauté et de transparence

Les médecins généralistes peuvent traiter des données à caractère personnel d'un ou d'une patient·e uniquement dans le cadre d'une relation thérapeutique, en cabinet ou en cas de prise en charge urgente. Sans relation thérapeutique, les médecins doivent pouvoir justifier l'accès aux données de patient·es par une base juridique (article 6 du RGPD) et un motif d'exception (article 9.2 du RGPD).

En effet, le traitement des données à caractère personnel doit reposer sur une des six bases juridiques reprises dans l'article 6 du RGPD :

- le consentement ;
- le contrat ;
- le respect d'une obligation légale ;
- la sauvegarde d'un intérêt vital ;
- l'exécution d'une mission d'intérêt public ;
- l'intérêt légitime poursuivi par le responsable ou par un tiers qui prévaut sur les intérêts et droits des patient·es.

Les données relatives à la santé sont dites « sensibles » et doivent de fait satisfaire également à un des motifs d'exception prévu à l'article 9.2 RGPD, à savoir :

- le consentement de la personne concernée ;
- la réalisation de diagnostics médicaux ;
- la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique en cas d'incapacité physique ou juridique de la personne à donner son consentement ;
- l'exercice de la médecine préventive ;
- l'exercice de la médecine du travail ;
- l'appréciation de la capacité de travail ;
- la prise en charge sanitaire ou sociale et la gestion des systèmes et des services de soins de santé ou de protection sociale ;
- l'exercice ou la défense d'un droit en justice.

Chaque traitement de données doit être conforme à la loi et doit donc respecter le secret médical, la loi relative aux droits du/de la patient·e, la loi qualité, l'interdiction d'accéder à un système informatique sans y être autorisé·e, etc.

Il est utile de rappeler que, même dans le cadre d'une relation thérapeutique, le ou la patient·e doit avoir préalablement consenti à l'accès à ses données avant tout traitement par le ou la médecin et doit en être informé·e. Les médecins doivent rendre l'information relative à ce traitement accessible et facile à comprendre.

Principe de finalité

Les données collectées doivent l'être à des fins explicites et légitimes et ne peuvent être traitées ultérieurement à d'autres fins ne respectant pas ces principes. À noter que le traitement ultérieur à des fins de recherches scientifiques est soumis à un régime spécifique qui n'est pas abordé dans le texte proposé.

Principe de pertinence et de minimisation

Les médecins ne recueillent et ne traitent que les données nécessaires, adéquates et pertinentes à la finalité pour laquelle elles sont recueillies, par exemple pour la bonne tenue du dossier médical (énoncées par la loi qualité) ou pour dispensation de soins de santé.

La consultation des données d'un·e patient·e doit se faire pour raisons pertinentes : avoir une relation thérapeutique avec un·e patient·e ne peut justifier l'accès continu à ses données, la curiosité ne constitue pas une raison légitime. Le secret médical impose de se taire mais ne donne en aucun cas le droit de savoir.

Les médecins doivent limiter l'accès aux données de ses patient·es aux seules personnes légitimement autorisées à y accéder et uniquement pour les données nécessaires à l'exercice de leur mission.

Les patient·es ont le droit d'accéder à leurs données de santé en vertu de la loi RGPD et de la loi relative aux droits des patient·es.

Principe d'exactitude

Les données à caractère personnel doivent être tenues à jour.

Principe de sécurisation, d'intégrité et de confidentialité

Les médecins doivent prendre toutes les mesures nécessaires de sécurisation des données qu'ils traitent afin d'en éviter l'accès à une personne non autorisée (on parle alors de « fuite de données ») qui pourrait les altérer ou les perdre. Pour ce faire, les médecins veilleront à utiliser des outils informatiques appropriés, des mots de passe sécurisés, des



antivirus, des locaux sécurisés avec des armoires fermées, etc. L'Autorité de protection des données publie des recommandations concrètes à ce sujet^e.

Les sous-traitants (service informatique, comptable, gestion administrative, etc.), traitant les données à caractère personnel pour le compte et sur instruction du ou de la médecin, doivent présenter des garanties suffisantes pour la protection des données et doivent conclure avec le ou la médecin un contrat conforme aux exigences de l'article 28 du RGPD. Ce contrat doit donc mentionner entre autres :

- l'objet, la durée, la nature et la finalité du traitement des données ;
- le type de données traitées ;
- les catégories de personnes concernées ;
- les obligations et les droits du responsable du traitement.

Le transfert de données par les médecins à l'INAMI, à des confrères ou aux organismes assureurs doit se faire par un moyen sécurisé et ne peuvent donc pas être transmis par e-mail non sécurisé. Les données ne peuvent être transférées numériquement que par des systèmes avec authentification à plusieurs facteurs (Réseau de santé Wallon, Abrumet, Cozo, boîte mail eHealthbox) ; l'Ordre des médecins met également à disposition de ses membres une « transfer-box » sécurisée dont l'accès peut se faire via le site www.ordomedic.be dans la section « se connecter ».

Les médecins doivent pouvoir rappeler à leurs collaborateurs les principes RGPD du traitement des données à caractère personnel cités plus haut auxquels ils sont également soumis.

Les fuites de données doivent être signalées à l'Autorité de protection des données dans un délai de 72 heures via formulaire électronique^f.

Principe de conservation limitée

Le dossier médical, en version électronique ou papier, doit être conservé pendant minimum 30 ans et maximum 50 ans à compter du dernier contact avec le ou la patient-e.

e. <https://www.autoriteprotectiondonnees.be/professionnel/themes/securite-de-l-information>. Voir également le guide de bonne pratique « renforcer votre politique de sécurité » sur le site <http://e-santewallonie.be/rgpd/>.

f. <https://autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles>

Information des patient-es quant à leurs droits en matière de protection des données

Les patient-es doivent avoir accès à certaines informations concernant le traitement de leurs données :

- l'identité du responsable du traitement ;
- la finalité du traitement ;
- les catégories des données traitées ;
- les destinataires des données ;
- la source d'où proviennent les données ;
- la durée de conservation des données.

Les patient-es doivent également pouvoir être informé-es de leurs droits, de façon concise, transparente, compréhensible et facilement accessible, notamment :

- le droit d'accéder à leurs données (dossier patient) et d'en recevoir une copie ;
- le droit de savoir quelles données de santé ont été consultées, par qui et à quelle fin ;
- le droit de rectification ou d'effacement des données^g ;
- le droit de limitation du traitement, de retirer leur consentement au traitement ou de s'opposer au traitement ;
- le droit à la portabilité des données (recevoir les données sur un support informatique couramment utilisé) ;
- le droit d'introduire une réclamation auprès de l'Autorité de protection des données.

Un-e médecin ne peut exiger de paiement s'il doit fournir ces informations ou répondre aux demandes des patient-es qui découlent de leurs droits. Cependant, si les demandes sont infondées ou excessives (notamment en cas de demandes répétées), le ou la médecin peut exiger le paiement de frais raisonnables pour les coûts administratifs ou refuser de donner suite à ces demandes.

L'Ordre des médecins se tient à disposition de ses membres afin d'apporter une aide juridique dans le cadre de l'exercice par les patient-es de leurs droits.

g. Le droit de suppression des données n'est pas absolu, notamment en raison de la loi imposant la conservation des dossiers de patients (voir le principe 6 de conservation limitée). Les données ne sont pas effacées lorsqu'elles sont nécessaires à la dispense de soins de santé, pour le respect d'une obligation légale du responsable du traitement, pour la constatation, l'exercice ou la défense des droits en justice, ou si le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique.



Tenue d'un registre des activités de traitement

Un·e médecin ou le groupe de médecins doit tenir un registre des activités de traitement des données décrivant les données qu'il collecte, leur sécurisation, les raisons pour lesquelles il les recueille, où il les conserve, pour quelle durée, s'il les transfère, etc. Ce registre doit être tenu à disposition de l'Autorité de protection des données si elle en fait la demande.

Un modèle pré-rempli de registre conçu pour les médecins est disponible sur le site e-santewallonie.

Désignation d'un·e délégué·e à la protection des données

Le ou la délégué·e à la protection des données est chargé·e de veiller au respect de la réglementation RGPD. Un·e médecin en pratique individuelle n'en a cependant pas l'obligation mais peut solliciter les conseils d'un·e délégué·e à la protection des données qu'il ou elle aura volontairement désigné·e.