Lignes directrices pour les médecins concernant le Règlement général sur la protection des données

Doc	a165001
Date de publication	27/04/2019
Origine	NR
Thèmes	Vie privée Secret professionnel RGPD

Lignes directrices pour les médecins concernant le Règlement général sur la protection des données

Le 27 avril 2016, le Parlement européen et le Conseil de l'Europe ont adopté un règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, soit le Règlement général sur la protection des données (RGPD) qui est entré en vigueur le 25 mai 2018.

Puisque les médecins traitent des données de santé et des données sensibles de leurs patients dans l'exercice de leur profession, il convient qu'ils intègrent les prescriptions de cette législation dans leur pratique quotidienne et qu'ils suivent les développements en la matière.

Étant donné que la déontologie médicale(1) concerne notamment le respect de la vie privée du patient qui est traitée dans plusieurs articles du code de déontologie médicale, le Conseil national de l'Ordre des médecins a rédigé cet avis et a prévu de donner aux médecins la possibilité de poser des questions via l'adresse électronique : privacy@ordomedic.be.

1. Généralités

Le RGPD approfondit la législation existant en matière de vie privée. Le médecin qui respecte la législation existante en matière de vie privée ne devra que légèrement modifier ses pratiques

Les principes généraux de la réglementation liés au droit à la vie privée, concernant certains droits du patient(2) et le secret professionnel, restent inchangés.

Un médecin individuel ou une pratique de groupe n'aura pas à investir beaucoup pour la mise en œuvre de la nouvelle législation. Le Conseil national tient à mettre en garde les médecins contre les entreprises qui proposent des services onéreux pour la mise en œuvre du RGPD dans leur pratique.

La nouvelle réglementation impose cependant de nouvelles mesures, comme la désignation d'un « délégué à la protection des données »(3) et la tenue d' un « registre des activités de traitement ».

2. Désignation d'un délégué à la protection des données

Le délégué à la protection des données (ci-après « DPD ») informe et conseille le responsable du traitement des données ou le sous-traitant de leurs obligations découlant du RGPD ou d'autres mesures de protection des données. Il veille au respect de la réglementation et de la politique en la matière, comme l'attribution de responsabilités, la conscientisation et la formation des personnes concernées par le traitement des données à caractère personnel(4). En outre, le DPD collabore avec l'autorité de contrôle et intervient comme point de contact(5).

Un médecin individuel ou une pratique de groupe ne doit pas désigner de DPD. La désignation est uniquement obligatoire dans le cas du traitement d'une quantité considérable de données de santé, comme dans les hôpitaux ou dans les structures qui comptent au moins 250 employés.

3. Registre des activités de traitement

Chaque médecin doit tenir un registre des activités de traitement des données. Ce registre est un fichier dans lequel le médecin décrit les données à caractère personnel qu'il collecte, comment il les sécurise, pour quelles raisons il les recueille, où il les conserve, pour quelle durée et s'il les transfère.(6)

La création de ce registre impose au médecin de réfléchir à la façon dont il gère les données à caractère personnel des patients et/ou du personnel qu'il emploie. C'est une amorce de restructuration de la gestion des données. Si le médecin constate qu'il ne sécurise pas bien certaines données à caractère personnel ou qu'il n'en a plus besoin pour l'exercice de sa profession de médecin, il devra prendre les mesures qui s''imposent.

Le Conseil national mettra prochainement à disposition un modèle de registre des activités de traitement des données.

4. Personnes autres que le médecin à avoir accès aux données à caractère personnel du patient

Le médecin indique les catégories de personnes ayant accès aux données à caractère personnel de ses patients. Leur statut vis-à-vis du traitement des données concernées est précisément décrit et documenté(7). Cette information est ajoutée au registre des activités de traitement des données.

Le médecin veille à ce que les personnes concernées par une obligation légale ou statutaire ou par une disposition contractuelle équivalente s'engagent à respecter le caractère confidentiel des données concernées. Toute personne ayant accès aux dossiers des patients doit avoir signé une clause de confidentialité dans son contrat de travail de collaboration.

Accès ne signifie pas que ces personnes travaillent réellement avec les dossiers patients. La simple possibilité de consulter ces dossiers suffit. La signature de ce contrat est un moment propice pour informer les collaborateurs de leurs droits et devoirs lors du traitement de données à caractère personnel.

5. Mesures à prendre (général)

Pour l'exercice de sa profession, le médecin collecte des données sur la santé de ses patients. Il s'agit d'une catégorie particulière de données à caractère personnel(8). Les données concernant la santé sont des données à caractère personnel relatives à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.(9)

Le médecin prend toutes les mesures nécessaires pour respecter le droit à la vie privée

du patient, pour sécuriser les données sensibles de façon optimale et éviter les « fuites de données ».

6. Transmission des données à caractère personnel

Il arrive régulièrement que le médecin ait à transmettre des données de santé de ses patients : soit au patient lui-même(10), soit à des tiers(11).

En cas de transfert des données de santé, le médecin doit toujours évaluer s'il peut envoyer les données à un destinataire tiers. Le secret professionnel ne permet pas au médecin de fournir les données de santé de ses patients à des tiers. Le médecin peut donc seulement transmettre les données de santé s'il existe une base légale.

En cas de transfert de données de santé à des tiers, à la demande du patient, le médecin doit apprécier si le patient n'est pas le mieux placé en raison de son droit à l'autodétermination pour décider quelles informations il souhaite partager et avec qui.

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.

7. Logiciel (Software)

Le médecin qui utilise un logiciel ou achète un nouveau logiciel destiné à la gestion de sa pratique ou à la sécurisation des données à caractère personnel doit toujours se renseigner auprès du fournisseur sur les paramètres de confidentialité. Ce fournisseur doit respecter le RGPD et doit communiquer en toute transparence à ce propos. Le médecin reste cependant responsable au cas où le software ne satisferait pas aux conditions légales.

En cas d'intervention de tiers lors du traitement de données à caractère personnel sous la responsabilité du médecin, la collaboration, la sécurisation et le déroulement du traitement doivent être fixés contractuellement dans un contrat de traitement des données. De nombreuses entreprises ont déjà développé des modèles et ont adapté leurs conditions générales. Il est recommandé de vérifier si ces dispositions sont adéquates.

8. Sensibilisation à la nouvelle réglementation

Le médecin conscientise ses collaborateurs aux mesures de sécurité qui protègent les données des patients et il détermine qui a accès et à quelles données.

Si une personne non compétente a toutefois accès aux données de santé de patients ou à d'autres données sensibles que le médecin détient dans le cadre de ses activités, on parle alors de « fuite de données »(12).

Les fuites de données doivent être enregistrées et signalées, selon la gravité, à l'autorité de protection des données et aux personnes concernées(13) endéans un délai de 72 heures.

9. Avenir

Les autorités, institutions et autres acteurs impliqués dans le traitement des données de santé prennent en compte ce nouveau règlement européen. À l'avenir, de nouvelles

directives européennes devraient préciser comment les acteurs des soins de santé doivent traiter les données des patients.

---

(1) Il s'agit essentiellement du chapitre 2, « Respect », du Code de déontologie médicale

(2) Articles 9 et 10 de la loi du 22 août 2002 relative aux droits du patient (droit à un dossier patient conservé en lieu sûr, droit à la protection de la vie privée)

(3) La dénomination anglaise souvent utilisée est « Data Protection Officer » ou « DPO »

(4) Par exemple le secrétariat, le personnel soignant qui assiste le médecin

(5) Article 39, Règlement général sur la protection des données

(6) Article 30, Règlement général sur la protection des données

(7) Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

(8) Article 9, Règlement général sur la protection des données

(9) Article 4, 15, Règlement général sur la protection des données

(10) Par exemple les résultats d'un examen ou lors de l'exercice du droit à la consultation du dossier patient

(11) Par exemple à des confrères-médecins qui traitent le patient dans le cadre du secret professionnel partagé, à l'INAMI sur la base d'une législation particulière, etc.

(12) Par exemple, cambriolage, piratage, données de santé envoyées à la mauvaise personne, etc.

(13) Article 33, Règlement général sur la protection des données