



RGPD

Ni affolement ni détachement

Plus d'une société vous aura contacté ces derniers jours pour vous jurer que vos données personnelles seront traitées dans le respect du RGPD¹. Mais vous, en tant que prestataire de soins individuel, que devez-vous faire pour vous mettre en conformité avec ce fameux Règlement européen ? Y a-t-il des actions à entreprendre vis-à-vis de votre patientèle ? Du non-dit à expliciter ? Des précautions à (re)prendre ?

Petit préalable dédramatisant : le RGPD, Règlement général sur la protection des données, s'inscrit dans la droite ligne de la loi belge « vie privée » de 1992, en accentuant certains aspects. Moralité, pour un médecin ou un acteur de soins, coutumier du secret professionnel, déjà attentif aux principes de cette loi (comme par exemple veiller à l'intégrité et la confidentialité des données de santé et des renseignements personnels qu'il recueille dans sa tâche de

Oui, le prestataire de soins est concerné !

Le RGPD concerne individuellement les prestataires de soins, en ce sens qu'ils tiennent un dossier comportant des renseignements permettant l'identification du patient et des données personnelles : diagnostics, traitements, rapports, courriers, données administratives, etc. L'informatisation confère bien sûr une toute autre dimension à la protection des données, mais les prestataires sont concernés quand bien même ils gèrent leurs dossiers sur papier.

gestion du dossier médical), la nouveauté n'a rien d'insurmontable. Les règles à suivre sont des règles de bonne pratique.

Le RGPD stipule notamment que les informations collectées doivent être traitées de *façon loyale et transparente* : on doit dire ce que l'on en fait, et s'y tenir. **Il est conseillé au prestataire d'informer explicitement sa patientèle, par exemple au moyen d'une affiche apposée en salle d'attente qui rappelle qu'il tient un dossier médical (informatisé).** Un cabinet de groupe spécifiera les règles d'application entre consœurs/ confrères en ce qui concerne le partage des dossiers.

Le RGPD affirme encore le principe de *minimisation des données*. Un prestataire se limitera au recueil des données personnelles qui sont strictement nécessaires pour mener à bien sa mission de soins. Ces données doivent en outre être exactes et, si nécessaires, mises à jour. Ce qui suppose une vérification en collaboration directe avec le patient. Un exemple concret de bon réflexe pour un généraliste : checker l'exactitude du contenu de ses sumehrs - ses dossiers résumés -, avec le premier intéressé.

Par ailleurs, comme le voulait déjà la loi vie privée, un prestataire de soins doit *sécuriser les données qu'il gère* en prenant un certain

Droits des personnes et impératifs médicaux

Le RGPD renforce les droits des citoyens par rapport à leurs données personnelles : être informé de leur traitement, pouvoir y accéder, demander des rectifications, s'opposer à leur exploitation, à leur communication à des tiers... Quelques nuances sont à apporter dans la sphère de la santé. Il peut y avoir, dans un dossier de santé, des rectifications sous la responsabilité du prestataire (qui doivent être réversibles et documentées). Notamment concernant le dossier médical, des éléments pertinents pour la tenue du dossier et la qualité des soins prodigués ne peuvent en être supprimés. Le droit à l'effacement - aussi dit droit à l'oubli - ne peut s'exprimer pleinement puisqu'en Belgique un dossier médical est conservé jusqu'à 30 ans, ce que le médecin signalera à son patient. Le droit d'opposition à l'enregistrement et à l'actualisation de données dans le dossier médical cède devant des motifs impérieux et légitimes : pour offrir au patient une prise en charge de qualité, le médecin doit pouvoir s'appuyer sur un dossier complet et à jour.



nombre de précautions. Par exemple travailler sur un ordinateur protégé par un mot de passe, des antivirus et des firewalls, faire des back-ups à fréquence régulière, les stocker de façon sûre, n'utiliser que des messageries cryptées et sécurisées pour échanger les données de santé, ne les partager que sur des réseaux reconnus et adaptés, comme le Réseau Santé Wallon par exemple.

Enfin, le RGPD soumet les prestataires de soins à *quelques obligations nouvelles*. La première est de tenir un « registre ». Il s'agit d'un document à usage interne qui fait l'inventaire des activités de traitement de données. Doivent y figurer les catégories de données gérées, leur finalité, le responsable du traitement, les sous-traitants éventuels (avec lesquels il faudra prévoir contractuellement des garanties de confidentialité), les flux et destinations des données etc.²

La seconde contrainte est de réaliser une analyse d'impact des risques. Elle consiste à identifier tout ce qui menace les données à caractère personnel qu'on possède : le vol, la perte (surtout si on les place sur support mobile), la destruction, l'accès non autorisé... et à s'en prémunir très concrètement. On rejoint ici les précautions énoncées plus haut, d'ordinateur couvert par mot de passe, de back-ups réguliers, etc.

Un prestataire individuel n'est pas concerné par l'obligation de désigner un « DPO », un « data protection officer ».

Il n'est pas supposé transférer en dehors de l'Union européenne des données médicales, sans s'être assuré que le pays destinataire offre des garanties équivalentes à celles du RGPD. Un aspect à garder en tête, s'il participe à des études cliniques ou emploie le cloud pour stocker ses dossiers.

Notes

1. RGPD = [Règlement Général sur la Protection des Données](#)
2. Un modèle existe sur le site de l'ex-Commission vie privée, devenue depuis l'Autorité de protection des données, dans le [dossier thématique registre](#)

Faites preuve de bonne volonté

Le RGPD responsabilise les acteurs concernés en attendant d'eux qu'ils mettent tout en œuvre, proactivement, pour assurer la protection des données au sens du Règlement. Un prestataire de soins, dit le « responsable du traitement » en jargon RGPD, n'a pas d'obligation de résultat, mais devra avoir mis en place des moyens raisonnables pour y arriver (et tenir disponible une documentation attestant de ces efforts).



Informez vos patients

e-santé Wallonie a créé une [affiche](#) que vous pouvez télécharger, imprimer et placer dans votre salle d'attente pour informer vos patients.

En savoir plus

Un [document](#) élaboré avec l'éclairage d'une juriste par le Dr Thierry Defour, médecin spécialiste en gestion de données de santé, DPO hospitalier et collaborateur d'e-santé Wallonie fournit quelques conseils pratiques pour les prestataires, sans prétendre à l'exhaustivité.