Quelles sont les conséquences du RGPD pour les professionnels de santé ?

Par Caroline KAMKAR, Docteur en droit, Avocat au Barreau de Lille

Le [règlement général sur la protection des données](#) (RGPD ou GDPR, pour General data protection regulation en anglais), est une nouvelle réglementation, commune à tous les pays européens, qui s'applique en France depuis le 25 mai 2018.

Il concerne le traitement de toute information numérique ou non, qui permette d'identifier une personne physique, directement ou indirectement, par son nom, un mail, un numéro de sécurité sociale ou même une adresse IP.

Les professionnels de santé sont amenés à traiter quotidiennement de nombreuses informations médicales personnelles (le nom, le numéro de sécurité sociale ...) et confidentielles (le dossier médical...). Le traitement des données personnelles est entendu au sens large et correspond à toutes les opérations telles que la collecte, l'enregistrement, la conservation, la modification, la transmission...

Le RGPD fixe un principe général d'information et de consentement explicite des personnes dont les données personnelles sont traitées. Les professionnels de santé exerçant en libéral au sein de leur cabinet échappent cependant à ce principe : selon les [recommandations de la CNIL](#), le recueil du consentement des patients pour le traitement de données de santé les concernant n'est pas nécessaire, dans la mesure où leur collecte et leur conservation sont nécessaires à l'élaboration du diagnostic médical et à leur prise en charge. Dans ce cas, l'information des patients peut être réalisée de façon générale, au moyen notamment d'un affichage dans la salle d'attente.

Cet affichage devra notamment porter sur le droit des patients d'obtenir la **suppression des données personnelles les concernant**. Cette suppression devra en outre pouvoir être garantie et démontrée en cas de demande expresse d'un patient. Il est toutefois recommandé de préciser au patient que la suppression des données de son dossier médical n'aura lieu que dans un délai de 20 ans.

Chaque médecin traitant et sauvegardant des données personnelles devra par ailleurs être en mesure de les sécuriser et de les conserver. Les règles de conservation se calquent sur celles de la responsabilité civile : une durée de 10 ans après la consolidation du dommage est habituellement recommandée.

Le RGPD impose que soit assuré en permanence un haut niveau de protection des données personnelles par la mise en place de procédures internes et les médecins devront pouvoir justifier la conformité de leurs pratiques à la réglementation en vigueur. À cette fin, un [exemple de registre](#) est disponible sur le site internet de la CNIL.

Pour mémoire, le recueil d'informations concernant un patient doit toujours être limité à ce qui est nécessaire à sa prise en charge médicale appropriée.

À noter qu'un [guide pratique, rédigé par la CNIL en partenariat avec le Conseil National de l'Ordre des Médecins vient d'être publié](#) face aux nombreuses demandes des professionnels de santé libéraux.