RGDP : ce qu'un médecin doit savoir

C'est une directive européenne concernant les données personnelles - publiée en 2016 et entrée en application le 25 mai 2018 - qui s'impose à tous les acteurs qui traitent ce type de données, sous forme informatisée ou non.

Cette directive partage le même objectif que la loi « informatique et Libertés » de 1978, en cours de modification.
Il s'agit de concilier protection de la vie privée des citoyens et innovation, ainsi que de garantir que tout traitement de données personnelles se fasse avec le consentement des personnes concernées.
Le médecin et son personnel détiennent des données sensibles, médicales ou autres - ils sont donc soumis au décret européen.

Ce que nous devons retenir

Données sensibles

Toute information se rapportant à une personne physique identifiée ou identifiable est une donnée personnelle – cela concerne les données médicales (dossier patient), mais aussi les données du cabinet (prises de rendez-vous, données concernant le personnel et les fournisseurs).
La collecte des données doit se limiter aux informations nécessaires, adéquates et pertinentes.

Protection des données

- Respect des règles de base de sécurité informatique - voir le site de la CNIL ou le site URPSML-NA,
- Si hébergement extérieur des données, travailler avec un prestataire agréé ou certifié pour l'hébergement de données de santé,
- Cryptage des données lors de transfert ou d'opération de maintenance.

Les règles de protection des dossiers s'appliquent aussi aux dossiers non informatisés (accès uniquement aux personnes autorisées, sécurité des locaux d'archivage, ...).

Durée de conservation des données

Les dossiers et informations ayant atteint la durée de conservation préconisée doivent être supprimés.
Cette durée est variable selon le type d'information. L'ordre des médecins préconise de s'aligner sur les délais de conservation prévus pour les dossiers médicaux des établissements de santé :

- 20 ans à compter de la date de la dernière consultation du patient,
- si le patient est mineur et que ce délai de 20 ans expire avant son 28ème anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date,
- dans tous les cas, si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à compter de la date du décès,
- en cas d'action tendant à mettre en cause la responsabilité du médecin, il convient de suspendre ces délais.

Les doubles des feuilles de soins doivent être conservés 3 mois.
Les données relatives à la prise de rendez-vous peuvent être supprimées lorsqu'elles ne sont plus nécessaires.

Ce que nous devons réaliser pour être en conformité

Information en salle d'attente

Le patient doit être informé de l'archivage de données sensibles le concernant et de son droit de consulter, modifier voire faire effacer des données le concernant.
Il existe un modèle d'affichage rédigé par le CNOM.

Protection des données lors des échanges avec d'autres professionnels de santé

Utilisation recommandée d'une messagerie médicale sécurisée.
Toutefois, les échanges avec certains professionnels et avec les patients ne sont pas possibles ainsi - utilisation conseillée alors d'une messagerie «hébergée en France», avec chiffrage des données jointes (GNU Privacy Guard conseillé par la CNIL).
L'utilisation de toute messagerie ne chiffrant pas les données et hébergeant les données dans un pays ou auprès d'un prestataire qui ne garantit pas la protection des données conformément aux règles européennes est à proscrire.

Registre des activités de traitement des données personnelles

Objectif : recensement de l'ensemble des activités de traitement des données personnelles au sein du cabinet, avec rédaction d'une fiche standard de modalité de traitement pour chaque activité.
Contenu : les cabinets médicaux (car moins de 250 salariés) bénéficient d'une dérogation en ce qui concerne la tenue de registres.
Ils doivent inscrire au registre les seuls traitements de données suivants :

- bien sûr, les dossiers médicaux,
- les traitements réguliers d'informations sensibles (agenda, gestion de la paie, gestion des clients/prospects et des fournisseurs, …),
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance,...),
- signalement de violation de données, si problème.

Désignation d'un délégué à la protection des données, conseillé uniquement pour les cabinets à fichier de données partagé.
Le registre est à constituer progressivement, sur le modèle proposé par la CNIL ou votre prestataire de services informatiques - il faut néanmoins être en capacité de justifier, au moins dans un premier temps, de votre engagement dans la procédure de mise en conformité....
Enfin, ce type de traitement remplace la classique « déclaration CNIL simplifiée de détention de données informatisées ».

Conduite à tenir en cas de « fuite » de données »

En cas de violation de données, analyser l'étendue du problème et inscription dans le registre des activités de traitement des données personnelles.
Si nécessaire, notification à la CNIL et aux personnes concernées…

Tout médecin détient des informations confidentielles et doit les protéger – le dossier est vaste et complexe - le CNOM et la CNIL ont bien préparé le travail du médecin libéral, mais il reste à mettre tout cela en pratique au sein de chaque cabinet médical ...

Dr Philippe DURANDET