FICHE PRATIQUE

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

...

CE QUE VOUS DEVEZ SAVOIR

Fédération Nationale des Médecins Radiologues

RGPD

Le RGPD : une obligation pour le radiologue

Vous entendez beaucoup parler de cette obligation nouvelle qui concerne depuis peu toutes les sociétés françaises, et recevez déjà de nombreuses notifications de diverses sociétés qui utilisent vos propres données personnelles. En votre qualité de professionnel de santé, vous-êtes, vous aussi, amené à prendre les précautions nécessaires vis-à-vis de vos patients, pour être en conformité avec la loi.

1 Qu'est ce que le RGPD ?

C'est un règlement européen dont l'anagramme signifie Règlement Général sur la Protection des Données, qui est entré en application en France depuis le 25 mai 2018. Il renforce la loi Informatique et Liberté qui s'appliquait déjà dans notre pays depuis de nombreuses années, et s'impose à toutes les sociétés publiques ou privées qui traitent les données communiquées par leurs clients.

En quoi concerne-t-il les radiologues ? Comme tout médecin, nous hébergeons des données de santé, mais aussi des données personnelles (adresse, numéro de téléphone,…). Nous sommes déjà soumis au respect du secret professionnel. Le RGPD vient renforcer les droits de nos patients et nos obligations de protection de leurs données que nous collectons dans nos activités quotidiennes, à travers nos outils informatiques (gestion des rendez-vous, tenue du dossier patient dans nos RIS et PACS, sociétés de maintenance, sociétés de service, fournisseurs, messageries, téléradiologie, etc.).

2 De quoi parle-t-on à propos des données à protéger ?

En pratique, de très nombreuses informations telles que les identifiants du patient (nom, prénom, etc.), mais aussi ses informations personnelles (nombre d'enfants,…) ou concernant sa santé, ses antécédents, et son numéro de sécurité sociale par exemple.

3 De quels droits disposent nos patients ?

Par le RGPD, ils peuvent demander à accéder à leurs données, à les rectifier en cas d'erreur, à s'opposer au traitement de ces données pour des raisons particulières, ou qui leur sont propres, ou demander également à effacer des données non adéquates ou conservées trop longtemps.

4 Qui est responsable ? Qui se charge de le mettre en œuvre ?

Le radiologue est le responsable légal. La mise en œuvre du RGPD peut s'avérer complexe surtout pour de grandes structures. Elle devra être exhaustive, suivie et rigoureuse, d'autant qu'elle exposera à des contrôles inopinés par la CNIL (Commission Nationale de l'Informatique et des Libertés), voire à des sanctions administratives et pénales. Dans l'immédiat et pour les deux années suivantes, les premières interventions seront à visée pédagogique. L'essentiel est de pouvoir démontrer que vous êtes engagé dans cette démarche de mise en conformité, dont nous vous donnons les grands principes.
Si vous traitez des données à grande échelle, il vous est conseillé de désigner un **délégué à la protection des données de santé (DPO)**. Il peut être choisi en interne si vous disposez d'un collaborateur qualifié dans ce domaine, sinon solliciter un DPO externe (qui peut être proposé par un cabinet d'avocat, un consultant, ou un fournisseur de RIS/PACS en veillant à ne pas générer de conflit d'intérêt).

5 Comment faire en pratique ?

La personne responsable de cette mise en œuvre devra procéder par étapes.

Il devra :

- **Cartographier vos traitements de données :** les recenser, ainsi que leurs durées de conservation, identifier les sous-traitants …
- **Mettre en évidence les traitements des données à risque** afin de mettre en œuvre des mesures de protection.
- **Sensibiliser vos collaborateurs** aux réflexes de protection dans leurs pratiques quotidiennes.
- **Etablir un REGISTRE,** outil essentiel pour assurer une traçabilité des actions de protection que vous seront mises en place.
- **INFORMER** les patients de leurs droits et de la mise en conformité de votre établissement avec les obligations du

RGPD : par exemple par affichage en salle d'attente, ou au moyen d'un dépliant.

6 Le dossier des patients : comment respecter le RGPD ?

- En limitant les informations à celles qui sont nécessaires (telles que l'historique de santé, et selon les besoins les habitudes de vie, les habitudes alimentaires, la vie professionnelle.) à l'exclusion de celles qui n'auraient pas de lien avec le motif médical présent (religion, orientation sexuelle, ...) et en supprimant celles qui dépassent les durées préconisées (selon le CNOM 20 ans pour les dossiers médicaux à compter de la date de la dernière consultation et 10 ans pour les patients décédés). Les utilisations personnelles ou commerciales sont naturellement prohibées.
- En limitant l'accès des données aux personnes autorisées.
- En établissant un contrat de sous-traitance si vous travaillez avec un prestataire (tel un hébergeur de données qui devra être agrée ou certifié et qui devra vous certifier son propre engagement au respect du RGPD).
- En sécurisant votre système informatique (au moyen de mots de passe efficaces, d'anti-virus, de sauvegardes régulières, de chiffrement des données sensibles, etc.) que vous ferez préciser à votre éditeur de logiciel.

7 Les données des salariés

Comme tout employeur, le radiologue est aussi responsable des données personnelles et confidentielles de ses salariés.

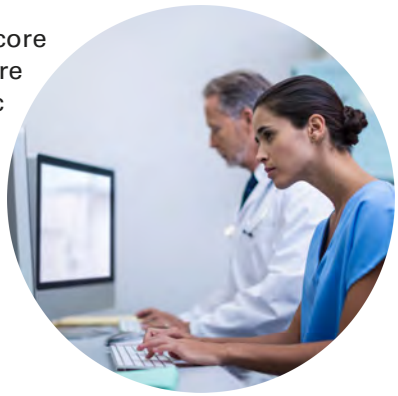
8 Les autres postes sensibles des cabinets de radiologie

La prise des rendez-vous : le radiologue reste responsable du traitement des informations. Par exemple, une plate-forme de rendez-vous en ligne est considérée comme un sous-traitant et ne peut utiliser que les informations utiles au strict accomplissement de sa mission, par les seules personnes autorisées, et pendant une durée limitée (les données sont supprimées quand elles ne sont plus nécessaires, selon une durée à faire préciser). Cela sera mentionné dans le contrat de sous-traitance (tout prestataire devant lui-même respecter le RGPD).

La messagerie électronique : il est recommandé d'utiliser une messagerie sécurisée, de type messagerie cryptée (Apicrypt est maintenant certifié).

Les téléphones portables et les tablettes : (ainsi que les clés USB, et les disques durs externes) veiller à prendre toutes les précautions quant à l'utilisation de ces outils quotidiens. Il vous est fortement déconseillé d'y conserver des informations médicales. De même, prenez les précautions nécessaires pour les accès à distance aux dossiers patients (sécuriser les accès par authentification, chiffrement des données sensibles etc.). Prenez aussi des précautions concernant l'utilisation des **fax** qui ne sont pas sécurisés, et sources d'erreurs de destinataire.

La téléradiologie : là encore s'assurer que le prestataire est bien en conformité avec la loi sur le RGPD, en vérifiant les mentions obligatoires dans le contrat de sous-traitance, et vérifier que le patient a bien autorisé la mise en œuvre d'une interprétation à distance.



Conclusion

Le RGPD est une nouvelle obligation légale qui s'impose à nos centres de radiologie.
Elle donne des droits de regard à nos patients et nous oblige à de nouvelles obligations pour sécuriser les informations qu'ils nous confient.
La loi s'impose en France depuis le 25 mai 2018, toutefois sa mise en œuvre nous laisse le temps d'engager nos procédures durant les deux années qui suivent. Les premiers contrôles de la CNIL seront à visée pédagogique mais à terme cette obligation engagera fortement notre responsabilité.
Les centres qui gèrent des volumes importants de données disposeront d'un responsable DPO qui assurera la formation, la mise en œuvre et le suivi du RGPD, au moyen de la tenue d'un registre, soit par désignation interne à l'établissement, soit par délégation de service extérieure.
Si vous souhaitez en savoir davantage sur le sujet, n'hésitez pas à vous inscrire sur le site de FORCOMED, qui propose une formation en e-learning sur le RGPD, assurée avec la collaboration d'un avocat et d'un informaticien spécialisés.

Bibliographie

Le code pénal - Le code civil

Guide pratique sur la protection des données personnelles (Edition juin 2018) par :
le CNOM (conseil de l'ordre des médecins) : https://www.conseil-national.medecin.fr
la CNIL : https://www.cnil.fr

A RETENIR

- UNE OBLIGATION NOUVELLE ET INCONTOURNABLE
- COMMENCER A SE METTRE EN CONFORMITÉ
- S'AIDER D'UN PRESTATAIRE
- DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES
- TENIR A JOUR UN REGISTRE
- INFORMER VOS PATIENTS

RGPD

FORCOMED

Formation RGPD : impacts et actions à mener pour le radiologue

Dans cette formation dispensée par Forcomed, vous traitez en moins de 60 minutes tous les aspects du RGPD liés à l'activité des centres d'imagerie médicale. Nous réunissons un avocat, un informaticien et un radiologue pour comprendre concrètement la nouvelle donne et lancer les actions de mise en conformité. Tarif : 119 €

www.forcomed.fr