RGPD – Comment protéger vos données ?

Méd'in Occ

Le respect du Règlement Général sur la Protection des Données (RGPD) est essentiel pour maintenir la confiance de vos patients et éviter des sanctions potentiellement sévères en cas de non-conformité.

Droits des patients & consentement

Informez vos patients de leurs droits : accès, rectification, suppression, limitation du traitement, portabilité des données…. Assurez-vous qu'ils comprennent pourquoi vous avez besoin des données et leurs utilisations.

Le support d'information est libre : par oral, par écrit ou par tout autre moyen - Notre conseil : affichage dans les lieux de soins, secrétariats, salle d'attente

Accès Guide pratique - Exemple Affichage (page27)

Identification des données sensibles

Identifiez les types de données personnelles sensibles que vous collectez, stockez et traitez : informations médicales, identifiants personnels, informations de contact…

Accès aux données

Établissez des politiques de contrôle d'accès et limitez l'accès aux dossiers médicaux aux membres du personnel qui en ont besoin (soins) et en fonction de leur mission.

Conservation des données

Les dossiers médicaux doivent être conservés activement pendant 5 ans à compter de leur dernière consultation puis archivés 15 ans. Assurez-vous ensuite de les détruire de manière sécurisée.

Minimisation des données

Ne collectez que les données strictement nécessaires à des fins médicales. Évitez de collecter des données excessives ou non pertinentes.

Sécurité des données

Mettez en place des mesures de sécurité appropriées : chiffrement des données, accès restreint aux dossiers médicaux, pare-feu et antivirus, formation …

Notifications de violation de données

En cas de violation de données, signalez-la aux autorités de protection des données dans les délais prévus par le RGPD et informez également les personnes affectées

Vérifier vos solutions informatiques : l'hébergeur de données doit se conformer à un référentiel établi par l'Agence du Numérique en Santé et répondre aux exigences de normes de qualité ISO.

Pour déclarer :
https://www.cybermalveillance.gouv.fr

Pour aller plus loin :

- QUESTIONS / RÉPONSES pour les médecins libéraux
- Référentiel CNOM cabinets médicaux

Évaluation d'impact sur la protection des données (DPIA)

Réalisez une évaluation d'impact sur la protection des données lorsque cela est nécessaire, par exemple, lors de la mise service d''un logiciel.

Responsable de la protection des données (DPO)

Désignez une personne responsable de la protection des données, s'il est nécessaire en vertu du RGPD.

Nécessaire pour MSP, CPTS, réseau… :

A titre individuel, vous n'êtes pas soumis à l'obligation de **désigner un DPO**. Néanmoins, si vous traitez des données de santé à grande échelle vous devez soit désigner un DPO en interne, soit solliciter les services d'un DPO externe.

La constitution et le maintien d'un registre des activités est une obligation prévue par le RGPD. Elle s'applique à toutes les structures qui traitent des données personnelles de façon régulière dans le cadre de leurs activités.

Dans le même esprit vous devez mener une **analyse d'impact** pour les traitements concernés. Vos logiciels métiers peuvent disposer directement de cette option.