Les données et leur traitement : de quoi s'agit-il ?

Méd'in Occ

Donnée personnelle ou à caractère personnel

C'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement. Peu importe que ces informations soient confidentielles ou publiques.

Exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, une adresse IP, un identifiant de connexion informatique, etc.

Données de santé

Ce sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

3 catégories :

- Les données de santé par nature : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
- celles qui croisées avec d'autres données, deviennent des données de santé car elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne.
- celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Le traitement de données

C'est **toute opération portant sur des données personnelles et de santé**, quel que soit le procédé utilisé, que cela touche des fichiers papiers ou numériques.

Exemple : La collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, l'effacement ou la destruction des données.

Attention

- S'il est possible par recoupement de plusieurs informations d'identifier une personne, les données sont toujours considérées comme personnelles.
- Un traitement n'est pas uniquement un fichier ou une base de données. Il peut s'agir aussi d'un système de paiement par carte bancaire ou de reconnaissance biométrique, d'une application pour smartphone, etc. ;

Méd'in Occ

Les recommandations de base pour la sécurisation du système informatiques

Séparation des usages

- N'utilisez pas le même appareil pour les usages professionnels et personnels
- N'hébergez pas de données professionnelles sur vos drives/clouds personnels
- Segmentez les comptes mails
- N'utilisez pas de wifi public ou non sécurisé
- Minimiser les connexions d'appareils non professionnels sur le réseau

Important

Les mots de passe

- Utilisez un mot de passe conforme aux recommandations de la CNIL : **12 caractères (chiffres, lettres majuscules et minuscules, caractères spéciaux), renouvelé régulièrement**
- Ne partagez pas votre mot de passe
- N'utilisez pas le même mot de passe sur différents comptes
- Ne l'écrivez pas sur un post-it
- Programmez le verrouillage de votre session après 30 secondes d'inactivité

Les sauvegardes

- Dupliquez et mettez en sécurité vos données critiques
- Chiffrez les données sensibles
- Créez 3 exemplaires des données sauvegardées
- Utilisez 2 supports de sauvegarde différents
- Au moins sur un support déconnecté du réseau internet
- Le drive ou le cloud peut être utile, mais assurez-vous que l'hébergeur soit certifié HDS

Les mises à jour et antivirus

- Mettez à jour régulièrement vos systèmes et applicatifs
- Activez les mises à jour automatiques
- Utilisez un antivirus et vérifiez sa mise à jour
- Ne désactivez pas les pares-feux
- N'ignorez pas les messages d'alerte
- Programmez les mises à jour pendant vos périodes d'inactivité

Les bonnes pratiques pour les dossiers patients et les prises de rendez-vous

Méd'in Occ

Général

- Tenir un registre à jour de ses « traitements » : Accès au modèle de registre de la CNIL
- Informer les patients et s'assurer du respect de leurs droits : Accès au modèle de notice d'information aux patients pour votre cabinet médical en page 27

Dossier des patients

- Limiter les informations collectées au nécessaire et utiliser les dossiers patients conformément aux finalités définies (ex : suivi des patients).
- Supprimer les dossiers patients et de manière générale toute information ayant dépassé la durée de conservation préconisée.

Prise de rendez-vous

- Limiter les informations collectées par le secrétariat ou par le prestataire à qui est confié la prise de rendez-vous, notamment le motif de la consultation si la consultation ne nécessite pas de préparation.
- Vérifier la conformité du prestataire avec la réglementation et notamment la présence des mentions obligatoires dans le contrat de sous-traitance.

Les recommandations quant aux outils numériques utilisés dans la pratique

Méd'in Occ

Messagerie Electronique

Utilisation d'un service de messagerie sécurisée de santé pour les échanges avec d'autres professionnels de santé

Si utilisation de messagerie électronique standard ou messageries instantanées, qui ne garantissent pas la confidentialité des messages :

- S'assurer que ces messageries sont bien sécurisées et adaptées à l'utilisation professionnelle ;
- Chiffrer les pièces jointes, le cas échéant ;
- A défaut, aucune information relative à un patient ou à un professionnel de santé intervenant dans sa prise en charge ne peut être échangée.

Supports mobiles (clés USB, disque dur externe)

Utilisation fortement déconseillée

Si malgré tout, leur utilisation est nécessaire, il convient de chiffrer les données sensibles qui y sont conservées.

Téléphones et tablettes

Sécurisation de l'accès à son téléphone ou à sa tablette et à son contenu (mot de passe, chiffrement, etc.) et de l'accès au logiciel de dossiers-patients sur le téléphone portable ou la tablette

- Aucun stockage d'informations médicales relatives aux patients sur le téléphone portable ou la tablette ;
- Consultation du logiciel de dossiers-patients avec précaution.

Télémédecine

Vérification de la conformité avec la règlementation du prestataire choisi

- Contrôle que le patient est informé de la conformité ;
- Vérification de la présence des mentions obligatoires dans le contrat du prestataire.

Les mentions recommandées pour un contrat de télémédecine - RGPD

Important

Votre prestataire doit vous permettre de vérifier qu'il respecte la règlementation RGPD.

Le contrat doit indiquer qu'il :

- Ne traite les données à caractère personnel que sur votre instruction ;
- Veille à la signature d'engagements de confidentialité par le personnel ;
- Prend toutes les mesures de sécurité requises ;
- Utilise un hébergeur de données de santé agréé ou certifié ;
- Ne recrute pas de sous-traitant sans votre autorisation écrite préalable ;
- Coopère avec vous pour le respect de vos obligations en tant que responsable de traitement, notamment lorsque des patients ont des demandes concernant leurs données ;
- Supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- Collabore dans le cadre d'audits.

Outils

L'agence du numérique en santé (ANS) propose des questionnaires pour les professionnels de santé à destination des prestataires de service en fonction du service assuré.

Dans la mesure où vous êtes en responsabilité quant à la protection et l'usage des données, ces questionnaires vous permettent de vous assurer que vos fournisseurs sont en conformité avec les exigences légales et réglementaires applicables.

Accès aux questionnaires