GDPR : Suite Document N° 4

Quelques recommandations pratiques ….

Lors de l'enregistrement d'un nouveau patient, il est nécessaire d'enregistrer un nombre de données à **caractère personnel**, basées notamment sur le chapitre 7 du AR du 21 janvier 2009, à savoir :

- Nom, prénom du prescripteur ;
- Nom, prénom du patient ;
- Numéro d'identification à la sécurité sociale (NISS) ; ….

Des données supplémentaires peuvent uniquement être recueillies que si le patient donne son accord et si ces données sont pertinentes dans le cadre professionnel et dans celui de l'obligation de minimalisation des données.

Ex : l'adresse, le N° de téléphone, ….

La lecture de la carte d'identité (EID) permet bien sur d'identifier le patient lors d'une délivrance et établit l'accord du patient au niveau du recueillement des données personnelles.

Dans le cadre de la délivrance des médicaments qui ne sont pas soumis à prescription et de la délivrance d'autres produits du type « parapharmaceutiques », le pharmacien peut enregistrer uniquement les données que si le patient y a marqué son accord.

Les données à caractère personnel et sensibles ne sont normalement jamais supprimées du système informatique.

À tous moments, vous devez pouvoir communiquer au patient ses données. Vérifier les opportunités au niveau de votre soft : « Imprimer » page données personnelles ou « Print screen » écran, ….

Exactitude des données :

Enregistrer la carte d'identité (EID) est une mesure proactive du pharmacien lui permettant de garantir que les données d'assurabilité sont à jour. Il est souhaitable de reparcourir cette procédure tous les 6 mois.

Recommandation : vérifier avec les maisons de soft s'il est possible de définir un rappel automatique après un délais de 6 mois pour relecture d'enregistrement de la carte d'identité.

Sources : APB, Spot iT

Transfert de données ou participation à des études scientifiques :

En cas de transfert de données à des tiers dans le cadre de gestion financière ou d'études scientifiques, les points d'attention doivent être respectés :

Les formulaires de consentement **explicites** doivent être vérifiés : le patient doit donner explicitement son accord pour ce transfert de données personnels et sensibles. Il existe des formulaires de consentement explicite sur différents sites : site APPL rubrique GDPR

Ce consentement est d'habitude recueilli par l'administrateur de bien ou par la cellule médicale qui procède aux études scientifiques.

En transférant les données à des parties tiers pour des gestions financières ou des études scientifiques, les recommandations suivantes sont d'application :

- Informer le patient si les données seront transférées sous un format **non-anonyme** ;
- Vérifier que cette information est précisée dans le formulaire de consentement ou dans la déclaration de protection des données avant la signature du formulaire ;
- Inscrire les garanties nécessaires dans un **contrat** (voir site APPL GDPR) avec la partie que s'occupe de la gestion financière ou l'étude scientifique. Ce contrat doit être conclu avant que le transfert des données ne soit effectué ;
- Il est judicieux que le pharmacien dispose d'une copie du consentement explicite qui sera conservé dans la pharmacie de manière sécurisé.

IT et sécurité :

MOTS DE PASSE

L'utilisation d'un nom d'utilisateur et mot de passe pour démarrer le système informatique évite l'accès au système informatique gestionnaire des données, à des personnes non-autorisées. Il permet aussi de garantir la traçabilité des manipulations.

Dans la plupart des systèmes de gestions de données, on distingue le compte de l'administrateur de celui d'un utilisateur normal.

Pour garantir un niveau de sécurité élevé, il est nécessaire de déterminer les personnes et leurs droits respectifs dans une application, il est nécessaire d'introduire un système de rôles selon le principe du moindre privilège.

Documents physiques et « bureau propre »

Sources : APB, Spot iT

Les documents (conventions, consentements, schéma de médication, …) doivent être gardés dans une armoire fermée ou un espace clos qui n'est pas accessible pour des personnes non-autorisées.

- Evitez des documents sur papier et, si possibles, digitalisez les documents ;
- Evitez d'imprimer les documents ;
- Obligez l'emploi **d'un destructeur de papiers** ou l'emploi d'une corbeille à papier fermée (destrabox) ;
- Verrouillez toujours le poste de travail en se levant et quittant l'espace pour éviter que des personnes non autorisées puissent voir des données à caractère personnel;
- Eteignez toujours le poste de travail en fin de journée ;
- Veillez à la fin de la journée à ce que tous les documents soient conservés de manière sécurisée ;
- Exercez des contrôles fréquents afin de garantir que la politique est suivie.

Les Back Up

Les backups des données doivent également être au maximum sécurisés. La sécurisation est possible par des mesures techniques d'un côté, mais également en sécurisant physiquement les backups.

Utilisation des e-mails :

L'utilisation d'e-mail pour la communication entre les prestataires de soins est largement répandue. Bien qu'il soit impossible d'éliminer entièrement l'utilisation d'e-mail étant donné les risques, il va de soi qu'il faut l'éviter autant que possible.

Recommandation : limitez l'utilisation d'e-mails pour l'envoi des données à caractère personnel ou confidentiel et utilisez des plateformes comme eHealth, et l'eHealth box.

Essayez de réduire les risques inhérents au trafic d'e-mails en :

- Choisissant une application d'e-mails sécurisée ; ex déployer Office 365
- Appliquer « Secure e-mail » pour chiffrer les e-mails et le trafic ;
- Eviter l'usage des boîtes aux lettres « **groupe** ».

Sources : APB, Spot iT