Document 13/12/2018

Pour vous aider à intégrer progressivement les principes du GDPR/RGPD dans votre pratique quotidienne, l'APB rédige une série de conseils pratiques.

Quelques **mesures organisationnelles** simples, qui ont trait au respect, d'une part, du droit à l'information (point 1) et, d'autre part, des principes d'intégrité et de confidentialité (points 2,3 et 4).

1) Obligation d'information: Avez-vous placé dans votre officine l'**affiche visant à informer vos patients** que vous respectez la législation sur la protection de la vie privée et des données à caractère personnel? Cette affiche peut être téléchargée sur le site APB (ou AUP www.aup-net.be).

Informez-vous également vos patients des autres finalités éventuelles pour lesquelles vous traitez leurs données (par ex. si vous travaillez avec des cartes clients)? Vous pouvez toujours utiliser les modèles disponibles sur MyAPB, dans la **Toolbox RGPD**.

2) Clean desk: Laissez-vous parfois traîner des ordonnances ou d'autres documents qui contiennent des données à caractère personnel ou des données de santé sur les bureaux ou les comptoirs? Les classez-vous immédiatement (par ex. dans un tiroir, une armoire, etc.) afin de les rendre inaccessibles à des personnes non autorisées? Veillez à ce que ces documents ne puissent être consultés que par des personnes habilitées à y avoir accès pour des raisons professionnelles (« need to know«) telles que votre adjoint(e) ou assistant(e).

3) Documents papier: Conservez-vous des documents papier qui ne sont plus utiles et qui ne sont donc pas soumis à une obligation de conservation légale (par ex. tickets de caisse non emportés par les patients)? Vous pouvez soit déchiqueter (directement) ces tickets ou documents, soit les stocker et les sauvegarder dans un endroit sûr, fermé, jusqu'à leur enlèvement pour destruction.

4) Imprimantes: *Retirez-vous directement les documents imprimés de votre imprimante?* Vous évitez ainsi que d'autres personnes – non autorisées – aient accès à des documents (confidentiels).

Quelques **mesures concernant l'aspect informatique**

5) Sécurité des postes de travail

Votre ordinateur est-il protégé et verrouillé lorsque vous le laissez sans surveillance?

- Si vous utilisez un mot de passe, celui-ci doit être solide (c.-à-d. contenir au moins 8 caractères) et être changé régulièrement (par ex. après 3 mois).
- Verrouillez toujours votre poste de travail (touches Windows + L) lorsque vous vous levez et quittez la pièce pour empêcher des personnes non autorisées de voir des données personnelles.
- Vous pouvez également utiliser un système de badge qui permet de (dé)verrouiller un ordinateur et de se connecter au système.

6) Sauvegarde

Votre système dispose-t-il d'une sauvegarde récente (de préférence sur un disque externe, une clé USB ou le « cloud ») en cas de panne?

- Veillez à faire des sauvegardes régulières (par ex. 2x/jour). Cryptez les données lors de la sauvegarde (la plupart des logiciels de sauvegarde prennent le cryptage en charge).
- Choisissez de conserver toute sauvegarde – quel que soit le support (lecteur SD, CD, DVD, clé USB, disque dur externe, etc.) – dans un environnement physiquement sécurisé et ne la laissez jamais sans surveillance.

7) Envoi de mails

Si vous envoyez des courriels à un grand nombre de destinataires, les ajoutez-vous en BCC (Blind Carbon Copy) – Cci?
De cette façon, les destinataires ne voient pas à qui le courriel a été envoyé.

8) Connexion sécurisée

Le site Web de votre pharmacie est-il sécurisé?

En optant pour le protocole « https », les données du site sont transmises de manière sécurisée, ce qui réduit le risque de fuites de données. Vous pouvez vérifier si votre site est sécurisé en consultant son URL (son adresse).

9) Surveillance par caméra

Votre pharmacie est-elle équipée d('un)e caméra(s) de surveillance? Si vous avez déjà déposé une déclaration de surveillance par caméra par le passé, l'avez-vous refaite?
Vous pouvez déclarer votre caméra à la police via **www.declarationcamera.be**. Pour les caméras déjà notifiées, la procédure doit être reconduite avant le 25 mai 2020. De plus, n'oubliez pas d'afficher le pictogramme réglementaire et d'effacer les images (enregistrées) après une période de 30 jours.

A propos des **contrats de sous-traitance**

En tant que responsable du traitement des données, vous faites appel à différents tiers qui traitent un certain nombre de données à votre place : les plus évidents étant votre **maison de soft**, votre **office de tarification** et **Farmaflux**.

10) Dans le cadre de votre relation contractuelle avec ces tiers, le RGPD impose la **signature d'un contrat de sous-traitance** qui définit notamment les obligations et la responsabilité de votre sous-traitant.
Pas de panique toutefois: en ce qui concerne les OT et FarmaFlux, vous recevrez des contrats de sous-traitance spécifiques qu'il ne vous restera plus qu'à signer. Votre maison de soft a peut-être déjà fait une démarche similaire. Et si vous travaillez avec d'autres sous-traitants, vous pouvez toujours utiliser le modèle de contrat mis à votre disposition dans notre toolbox APB
RGPD sur MyAPB. Nous abordons dans cette tollbox trois autres cas de figure concrets où vous pouvez faire appel à des tiers qui vont sous-traiter des données personnelles dans l'exercice de leurs missions (Mailing lists, service de messagerie/livraison et le secrétariat social).

A propos du **transmission et partage des données via un tiers**

11) Administrateur
Que faire pour les patients mis sous tutelle? Puis-je, sans autre formalité, partager leurs données (par ex. des antécédents médicaux) avec leur administrateur?

Si un administrateur vous demande ce type de données, il doit être en mesure de prouver qu'il peut les traiter sur la base d'une autorisation ou de l'exécution d'un contrat. Il agit alors lui-même en qualité de responsable du traitement. Que ce soit une autorisation du patient, une obligation légale, une autorisation du juge..., il devra vous la fournir lors de sa demande.

12) CPAS

Le CPAS intervient dans les frais de santé de certains de mes patients. Comment traiter ces cas particuliers?

Dans ce cas, le patient lui-même a demandé un soutien financier. En d'autres mots, il a ainsi donné l'autorisation au CPAS de traiter ses données personnelles. Lorsque le CPAS vous demande l'historique médical ou un autre détail d'une facture, vous pouvez considérer que le patient a donné son accord. Vous pouvez donc partager ces informations.

13) Partage de données

Comment procéder lorsque je suis autorisé(e) à partager des données avec des tiers?

Vous devez toujours vous assurer que les données sont envoyées de manière sécurisée. Pour ce faire, vous pouvez les anonymiser. Ainsi, elles ne pourront pas être directement associées à un patient donné. Vous pouvez également sécuriser les données sensibles en protégeant le document qui les contient (dans Word, par ex. la marche à suivre est: Fichier > Info > Protéger le document > Chiffrer avec un mot de passe). Ce document peut alors être envoyé en pièce jointe et vous communiquerez ensuite le mot de passe par téléphone à votre interlocuteur.

Si vous avez des questions en lien avec le RGPD et son application en officine, vous pouvez toujours nous les envoyer par mail au service APB, à **gdpr@apb.be**.