LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Pour bien respecter le RGPD, il faut être soi-même sécurisé. C'est l'enjeu de la cybersécurité.

QU'EST-CE QUE LE RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) est une nouvelle réglementation européenne qui vise à renforcer la protection des données personnelles. Il crée un cadre de la protection des données tenant compte des récentes évolutions technologiques (Big Data, objets connectés, Intelligence artificielle).

Nos cabinets médicaux, avec nos dossiers patients traitent des données à caractère personnel. Cette protection des données est déjà efficiente dans notre profession par le secret médical et notre colloque singulier patient-médecin.

Des améliorations sont à apporter sur la sécurité informatique : sécurisation des mots de passe, envoi de mails cryptés, gestion des sauvegardes…

POURQUOI ÊTES-VOUS CONCERNÉ PAR LE RGPD ?

En tant que médecin en exercice libéral, nous sommes amenés à recevoir ou à émettre des informations sur nos patients pour assurer leur suivi, que ce soit dans le dossier « patient » (papier ou informatique), dans le cadre de l'utilisation d'une plateforme en ligne de gestion des rendez-vous ou encore de la réalisation d'actes de télémédecine.
De manière plus globale, nous collectons également des informations pour gérer notre cabinet (ex : gestion des fournisseurs, des personnels que nous employons, etc.).
Ces informations que nous recevons et/ou émettons à l'occasion de notre activité professionnelle, sont considérées comme des données personnelles.

En pratique, il peut s'agir de données d'identification comme les nom, prénom, adresse, ou numéro de téléphone, d'informations sur la vie personnelle du patient (ex : nombre d'enfants), sa couverture sociale (ex. : Assurance maladie obligatoire, Assurance maladie complémentaire, etc.), et surtout d'informations relatives à sa santé (pathologie, diagnostic, prescriptions, soins, etc.), les éventuels professionnels qui interviennent dans sa prise en charge. Nous détenons également, dans le cadre de notre exercice, le numéro de sécurité sociale des patient (Numéro d'Inscription au Répertoire des Personnes Physiques - NIR) pour facturer les actes réalisés.

Pour toutes ces situations où nous utilisons ces données personnelles, nous sommes concernés par le RGPD.

QU'EST-CE QUE LE DPO ET LE REGISTRE DES ACTIVITÉS ?

Si vous exercez au sein d'un réseau de professionnels, maison de santé, EHPAD, ou si vous partagez des dossiers patients avec plusieurs professionnels de santé…, vous devez désigner un **délégué à la protection des données (DPO)** en interne ou en externe (cabinet d'avocats, consultants). Alors que si vous exercez à titre individuel, vous n'avez pas d'obligation de DPO.
Un registre des activités de traitement (toute action réalisée sur des données personnelles et ce, dès la collecte des données) doit être tenu à jour.
Vous trouverez un exemplaire de ce registre dans le guide pratique sur la protection des données personnelles CNIL–CNOM : https://bit.ly/2MQIb34. À découvrir également le document 'RGPD : se préparer en 6 étapes' : https://bit.ly/2BeJJ4J.

Afin de répondre aux obligations mises en place par le RGPD, tous les professionnels de santé doivent informer leurs patients de leurs droits de suppression ou de modification de leurs données à caractère personnel. Pour cela, une affiche doit être visible dans votre salle d'attente. Vous trouverez un exemple d'affiche à cette adresse : https://bit.ly/2QeQrMh.

Informatique et libertés

Ce cabinet médical dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients et à assurer la facturation des actes et la télétransmission des feuilles de soins aux caisses de Sécurité sociale.

Sauf opposition de votre part, les informations recueillies lors de votre consultation feront l'objet d'un enregistrement informatique réservé à l'usage de ce cabinet.

En application du **Règlement général sur la protection des données (RGPD)** entré en vigueur le 25/05/2018, **vous pouvez accéder à vos données personnelles, les modifier ou les supprimer** en vous adressant à (Nom et coordonnées du responsable du traitement des données : le médecin et/ou le DPO) :

.....

LA CYBERSÉCURITÉ

Si le RGPD est un texte réglementaire, l'outil du RGPD est la sécurité informatique. Nous vous proposons trois actions pour sécuriser votre poste informatique :

ACTION N° 1

Objectifs RGPD : Sécuriser les comptes par des mots de passe robustes et les renouveler régulièrement. Ne pas mélanger messagerie personnelle et professionnelle

Idéalement, l'accès au bios du poste informatique (le système qui permet de démarrer le poste, avant de lancer le système d'exploitation, Windows, Mac ou Linux) est protégé par un mot de passe. En effet, dans le cas contraire, un individu mal intentionné peut modifier la séquence de démarrage de façon à « booter » sur une clé USB sur laquelle est installé un système qui permet de faire sauter les mots de passe (de Windows par exemple).
Les mots de passe de l'utilisateur du poste et de l'administrateur devraient être changés régulièrement. Idem pour les mots de passe des logiciels installés sur le poste (gestion de cabinet, comptabilité, feuilles de soins électroniques), au moins à chaque changement de remplaçant…
Le partage du poste est déconseillé : un poste inutilisé et allumé devrait être verrouillé afin que personne ne puisse prendre la main sur la session. Si nécessaire, différencier les utilisateurs avec chacun son mot de passe. Le système garde les traces de l'activité de chacun…
Il convient également d'éviter le mélange des genres : travail, messagerie Internet professionnelle et privée (préférer l'utilisation d'un logiciel « client » de messagerie, genre *thunderbird*, plutôt que de consulter vos courriels dans le navigateur), production personnelle, jeux, fureter sur Internet…
Il est donc intéressant d'éditer une « charte » informatique, signée de chaque utilisateur, qui les informe de leurs droits, surtout de leur devoir, qui les met en garde contre le non-respect de la charte et des sanctions.

Consultez les deux fiches suivantes :
- Gérer ses mots de passe : https://bit.ly/2ppEc4c
- Sécurité des usages pro-perso : https://bit.ly/2QMg1JC

ACTION N° 2

Objectifs RGPD : Version maintenue des systèmes d'exploitation, équipements de tous les postes de travail par des antivirus, les postes nomades étant équipés d'un pare-feu local

Ce point est très controversé : combien d'utilisateurs se sont vus « plantés » par la mise à jour du système ou de leurs logiciels « métier » ! Pensez aux mises à jour imposées par la CPAM, sans l'aval des syndicats, et qui vous imposent des pratiques tarifaires non souhaitées. Assurez-vous également que les bugs de la mise à jour du logiciel métier soient corrigés dans la version n (voire n+1 en pratique).

Les logiciels dont la mise à jour ne se discute pas sont **l'antivirus**, gratuit ou non, et le **pare-feu**, *firewall* en anglais. Les règles de filtrage de pare-feu devraient être régulièrement vérifiées (règles de sécurité pour les flux entrants et sortants). Et sauvegarder les pièces jointes sur le disque avant de les ouvrir (ce que fait un logiciel de messagerie). L'antivirus les contrôle alors avant l'ouverture…

ACTION N° 3

Objectif RGPD : Mise en œuvre de la sauvegarde régulièrement testée

La préservation des données et des logiciels se fait en les copiant, compressés ou non, cryptés ou non, sur bande, clé USB, disque dur externe, ou sur un NAS, mais pas sur le Cloud. En effet Donald Trump impose l'accès par l'administration étatsunienne aux informations et données produites, exploitées ou stockées par des logiciels étatsuniens, même à l'étranger. Les grands de l'Internet (GAFA : Google, Amazon, Facebook, Apple) ont applaudi : enfin un cadre juridique clair pour répondre aux injonctions de l'administration. Tout le monde sait que Microsoft le faisait bien avant. Cela pose également le problème des logiciels en ligne, les informations hébergées par des serveurs utilisant un système d'exploitation étatsunien devant pouvoir être consultées par l'administration sus-citée. Ces sauvegardes peuvent être complètes ou partielles, « incrémentielles ».

L'URPS Médecins Libéraux AuRA met à votre disposition, sur son site Internet, rubrique 'En bref', un poster sur les bonnes pratiques de la cybersécurité (https://bit.ly/2N5zzW1) et se propose d'organiser des conférences sur ce thème (cf. conférence de juin 2018).

Drs Eric TEIL & Didier ANNE