Les bases de la sécurité informatique

RGPD : nous sommes tous concernés

La dématérialisation des données médicales est un apport important dans la qualité et le confort de travail du médecin (accès immédiat à l'information, diminution du volume de stockage, partage des données), mais elle expose au risque de perte brutale et parfois irréversible des données, ainsi qu'à leur piratage ou à leur corruption.

Le médecin libéral est responsable de la conservation des données médicales, de leur intégrité et de leur confidentialité pour une durée légale variable selon les recommandations du Conseil National de l'Ordre (https://conseil-national.medecin.fr).

Cette dématérialisation amène de nouvelles contraintes dont nous devons être conscients :

- « disparition du matériel », par panne ou vol – réfléchir aux moyens de protection matérielle, assurances, matériel de substitution...
- « perte de données », par problème matériel ou logiciel - sauvegarde régulière des données essentielles.
- « piratage de données ou blocage avec demande de rançon », avec l'accès ouvert des postes à l'internet...

Il est du devoir du médecin d'avoir une notion de sécurité concernant son outil informatique. Le Règlement Général pour la protection des Données Personnelles (RGDP) entré en application en mai 2018.

Systèmes d'exploitation

- **Faire les mises à jour** (cocher « mise à jour automatique » si vous n'y pensez jamais)
- **Utiliser un OS (Opérating System) non obsolète** (Windows XP n'est plus soutenu par Microsoft)

Protection

- **Utiliser un antivirus** et le mettre à jour
- **Utiliser un firewall** (celui de Microsoft au minimum)
- **Mots de passe, à l'allumage du PC** et à l'accès aux logiciels sensibles – choix d'un mot de passe « fiable » et unique pour chaque service, modifié de temps en temps et stocké en lieu sûr – combinaison de lettres et chiffres/majuscules et minuscules/caractères spéciaux
- **Ne pas cocher la case « rester connecté »** lors d'une connexion à un espace privé
- **Utiliser un wifi « sécurisé »**
- **Clef USB :** utiliser ses propres clefs réservées exclusivement à cet usage et désactiver le mécanisme « autorun » (paramètres Windows/périphériques/exécution automatique).

Messagerie

- **Eviter de mélanger ses messageries** professionnelle et personnelle
- **Privilégier les échanges par messagerie médicale sécurisée**
- Ne pas ouvrir les mails d'origine inconnue ou de contenu suspect
- Attention aux pièces jointes

Logiciels

- **Mettre à jour** son logiciel métier
- **Ne pas installer** de logiciel d'origine incertaine
- Sur internet, **ne pas cliquer** sur n'importe quel lien

Sauvegarde

- Elément primordial, permettant une reprise d'activité rapide et avec un minimum de perte en cas de problème
- Au moins sur deux supports en alternance, dont 1 stocké hors du cabinet
- Différents moyens : disque dur externe/USB/DVD ou par internet (cloud – site autorisé à stocker des données médicales)
- Vérification périodique de leur qualité technique
- Au moins une fois par semaine, idéalement toutes les nuits

Dr Philippe DURANDET