6. Assurer la sécurité des données

Comment améliorer ma sécurité technique ?

La sécurité englobe tant la sécurité technique vue dans la présente fiche que la sécurité organisationnelle qui est présentée dans la fiche 7.

Il faut d'une part, garantir la pérennité des données et d'autre part, avoir un environnement IT sain et une bonne gestion des accès.

Voici quelques astuces :

1-Afin de pérenniser les données et d'éviter la perte de celles-ci, il faut :

- Créer une **sauvegarde régulière** de données
- **Garder cette sauvegarde dans un endroit sécurisé,** autre que votre cabinet. *Exemple : en cas de vol, d'incendie ou d'inondations de votre cabinet, ou dans le cas de la destruction de votre système, votre back up doit être à l'abri des dégâts/du vol.*
- **Avoir un plan de secours** en cas de coupure d'électricité ou de panne de réseau

2-Prévoir une bonne gestion des accès :

- **Choisir un login et un mot de passe individuel**
  - Opter pour un **mot de passe complexe** : pas une date de naissance ou un mot de passe usuel, comme le prénom de votre conjoint.e ou des enfants, mais qqch dont vous pouvez vous rappeler facilement (exemple : nom d'un lieu ou un souvenir)
  - **Ne pas partager votre mot de passe** : ne le communiquer à personne ! Attention : Il ne faut pas afficher ou coller les mots de passe sur votre ordinateur ou sous votre clavier
  - **Changer les mots de passe pour les accès régulièrement,** mais pas tous les trois mois afin de pouvoir s'en souvenir
  - Opter pour une **authentification forte** (à double facteurs) afin de diminuer les risques. Des applications peuvent aider (ex Itsme, myID.be,…)
- **Supprimer tous les accès obsolètes**: veillez à ce que les accès de toutes personnes, ayant quitté ou ne travaillant plus pour votre organisation (employés, sous-traitants, etc), soient coupés et supprimés.
- Avoir un **système de verrouillage automatique** de votre session après une durée, par exemple, de 5 min d'inactivité.
- **Verrouiller l'ordinateur** lorsque vous quittez votre bureau ou lorsque vous n'avez plus de vue sur votre PC et ne permettez à personne d'utiliser votre session qui doit rester personnelle. *Par exemple, si vous êtes connecté aux réseaux d'eSanté, tous les accès sont tracés. Dans le cas où quelqu'un d'autre accède aux données via votre session restée ouverte sur votre ordinateur, vous serez tenu responsable car ce seront vos identifiants qui seront tracés (log d'accès consultation).*

2-Gérer l'infrastructure IT :

- S'assurer d'avoir un **pare-feu** et un **antivirus** performant
- Activer l'**automatisation des mises à jour** de l'ordinateur (pare-feu, antivirus, logiciels, Windows, …). Vous pouvez déléguer cette tâche à vos sous-traitants. Dans ce cas, pensez à inclure une clause spécifique concernant le renouvellement de contrats des logiciels ainsi que la gestion de vos mises à jour, afin que vos logiciels et votre infrastructure IT restent performants
- Avant de signer un contrat avec un sous-traitant (software, logiciel, autre) , penser à **tester les systèmes/ logiciels pour veiller à ce qu'ils soient conformes** aux besoins (liés au domaine d'activité considéré) et à la performance de sécurisation des données
- **Protéger le réseau Wifi avec un mot de passe** (changer le mot de passe de départ). Si mise à disposition du Wifi pour la patientèle, création de 2 réseaux wifi distincts:
    - l'un privé pour les activités du cabinet, sécurisé avec mot de passe fort et uniquement pour ce réseau (pour vous et vos éventuels confrères/consœurs et/ou collègues)
    - un autre public dédié à votre patientèle, avec mot de passe partagé entre vos patients uniquement (pensez à mettre une affiche dans la salle)
- Si **doutes sur la sécurité d'un mail ou d'un site : vérifier sur** SafeOnWeb
- Utilisation de **matériel informatique** (tablettes/ Gsm /Clé USB/ Disque dur, etc…) :
    - Il faut **limiter le stockage de données sensibles** sur ces outils, car ils sont susceptibles de perte ou de vol
    - Choisir une **sécurisation optimale** pour vos outils informatique avec sécurisation en mettant un mot de passe, ou utilisation biométrique (empreinte, reconnaissance faciale)
- Un **outil défectueux :**
    - Détruire toutes les informations du disque dur (forer des trous dans le disque dur) avant de le jeter. Ne jamais revendre du matériel en seconde main qui a servi à héberger des données à caractère personnel qu'elles soient sensibles ou pas.
    - Se débarrasser du matériel (ainsi détruit – points Récupel) .
    - Autre option : faire appel à une société de destruction de matériel IT.

Attention *: certains outils bien utiles sont néanmoins déconseillés (sécurité pauvre à ce jour), et il faudrait également vérifier les conditions générales qui peuvent évoluer (lieu des stockages des données, respect RGPD, etc.)*

Concrètement

Pérenniser les données et éviter leurs pertes

Avoir une bonne gestion des accès

Gérer l'infrastructure IT