7. Assurer la sécurité des données

Comment améliorer ma sécurité organisationnelle ?

Chaque Responsable du Traitement doit protéger toutes les données qu'il traite et ce, en prenant toutes les précautions en termes de sécurité organisationnelle et technique (fiche 6 Sécurité Technique).

En ce qui concerne la sécurité organisationnelle, le Responsable du traitement devra :

Principes de base

- **Sensibiliser au traitement des données** à caractère personnel toute personne engagée dans son cabinet et qui traitera des données à caractère personnel
- **Sensibiliser sur le secret professionnel**
- **Sensibiliser régulièrement** (par exemple: une fois par an) tout le personnel
- Choisir un **login et un mot de passe individuel :**
  - Opter pour un mot de passe : complexe et non communicable aux autres (cfr. fiche 6). *Attention : Il ne faut pas afficher ou coller les mots de passe sur votre ordinateur*
  - Changer tous les mots de passe de vos accès (+/- chaque année) (cfr. fiche 6).
- **Emplacement de l'imprimante** : cette dernière ne doit pas être dans un endroit accessible aux patients. *Exemple : dans la salle d'attente, couloir de passage vers les sanitaires*
- Les **documents imprimés doivent être récupérés directement après l'impression**. *Par exemple, choisir une imprimante avec accès par nom d'utilisateur et mot de passe par utilisateur ou badge*
- Les **documents obsolètes** : détruire les documents contenant des données sensibles à l'aide d'une **déchiqueteuse**.
- Les ordinateurs (ou tout autre outil informatique) non utilisés : ne pas oublier de détruire le disque dur (cfr. fiche 6).
- **Sécuriser le lieu de travail** : fermeture des portes, fenêtres et armoires en quittant le bureau. Ne pas laisser des dossiers à portée de main de tout le monde
- Faire un **back-up régulier** et le stocker dans un endroit autre que le lieu de travail : car, en cas d'incendie ou d'inondation du cabinet, ou dans le cas de la destruction du système, votre back up doit être à l'abri des dégâts (cfr. fiche 6).

Choisir un canal de communication professionnel et sécurisé

- **S'assurer du destinataire**
- Se demander si **l'information** qui va être communiquée est **importante/nécessaire ou non**
- **Opter pour un cryptage end-to-end** lors de l'envoi d'une information via un canal informatique. *Par exemple l'utilisation de la eHealthBox, du Réseau Santé Bruxellois*

Dans le cas où le patient demande de communiquer avec lui via un moyen dont la sécurité n'est pas garantie, inscrire la demande dans son dossier médical local en complétant le document « Moyen de communication » téléchargeable ici.

Faire attention au transfert d'information

- **Déterminer les coordonnées du destinataire**
- **Les vérifier avant envoi** (faire attention au remplissage automatique de l'adresse électronique du destinataire). *Attention au transfert de données hors UE.*

Notifier tout incident dans son registre d'incidents

- Le responsable de traitement est dans l'obligation de tenir à jour un registre d'incidents dans lequel il doit y notifier toute violation (voir fiche 8). *Pour rappel : violation de données est la perte, le vol, la divulgation ou la destruction d'une donnée à caractère personnel, de manière intentionnelle ou accidentelle, mais également l'indisponibilité de la donnée. Si la violation de données à caractère personnel engendre un risque pour la vie privée du patient il y a, le cas échéant, lieu de la notifier à l'Autorité de Protection de Données (APD), dans un délai de 72 heures calendaires*

Toutes les données doivent être archivées minimum pendant 30 ans (maximum 50 ans)

- Ces données doivent être archivées de façon sécurisée et accessibles en cas de besoin (cfr. fiche 9).

Conclure des contrats avec des sous-traitants

- Ces contrats doivent offrir des garanties au niveau de la sécurité au regard du RGPD (cfr. fiche 3).

Concrètement

Respecter les principes de base listés ci-dessus

Choisir un canal de communication professionnel et sécurisé

Faire attention au transfert des données

Obligation de notifier tous les incidents dans un registre

Archiver les données pendant minimum 30 ans et maximum 50 ans

Conclure des contrats avec tous les sous-traitants