CLM et le RGPD
Principaux conseils au médecin

Sécurisation de votre poste de travail

- Verrouillez votre clavier lorsque vous quittez votre ordinateur
- Choisissez un mot de passe complexe (recommandé : 12 caractères, majuscules, minuscules, chiffres caractères spéciaux minimum 8 caractères) et changez le régulièrement et si possible tous les mois ;
- Conservez le mot de passe confidentiel; Si vous avez un doute sur la confidentialité du mot de passe, changez le ;
- Conservez vos dossiers papier dans un espace sécurisé
- Pensez à gérer l'accès aux données patients par des tiers (personnel du cabinet ou prestataire, sur site ou à distance) conformément aux règles de sécurité et confidentialité

Conservation –Sauvegarde

- Si vous avez opté pour un logiciel web
  - Vérifiez que votre logiciel est hébergé en secteur HDS : Hébergement de Données de Santé Agréé par l'Asip Santé
  - Sauvegarde et archivage assurées dans le cadre de l'hébergement
- Si vous hébergez vous-mêmes vos données
  - Utilisez un outil dédié à la sauvegarde
  - Identifiez un responsable de la sauvegarde au sein de votre cabinet
  - Stockez les supports de sauvegardes dans un lieu différent de celui des données d'origine
  - Sauvegardez régulièrement les données (selon leur importance, la vitesse de modification, la quantité...) mais aussi les logiciels servant au traitement

IMPORTANT - MIGRATION

Lorsque vous changez de logiciel et êtes amené à fournir une sauvegarde de vos données à un tiers, vérifiez que la personne à qui vous remettez la sauvegarde respecte bien les règles du RGPD.

IMPORTANT - RETRAITE

Lorsque vous partez en retraite, récupérez et archivez les données. Au même titre que le dossier médical, les données personnelles informatiques doivent être conservées au minimum 20 ans. Le mieux est d'opter pour un Hébergeur de Données de Santé Agréé (HDS).

Accès distant - Infogérance

A des fins de simplifications de maintenance informatique, vous faites héberger votre serveur et vos données, voire vos sauvegardes chez un prestataire : celui-ci doit être conforme à l'obligation HDS et respecter les obligations RGPD.

De même lorsque vous donnez un accès distant permanent à votre propre réseau pour son infogérance, vous êtes responsables des accès et devez donc exiger le respect du RGPD de votre prestataire.

NOTRE CONSEIL - ACCES DISTANT

Ne donnez que des accès ponctuels sécurisés par un mot de passe et en votre présence.

Collecte et information patients

Le médecin responsable du recueil et du traitement de données à caractère personnel est lui-même soumis à une obligation de secret médical. Le patient doit être informé que vous allez traiter ses données de manière informatisée. Il est fortement recommandé d'afficher dans le cabinet les affichettes publiées par la CNIL pour cet usage.

Télécharger le modèle d'affiche pour votre salle d'attente et informer vos patients

Communication

Veillez à respecter les règles en vigueur pour la communication de dossiers patients à des tiers ou au patient lui-même.

IMPORTANT - MESSAGERIE

Attention à l'utilisation des messages électroniques : Il est très fortement recommandé de ne pas utiliser sa messagerie personnelle pour l'envoi de données patients.

L'utilisation d'une messagerie sécurisée de santé (MSS), intégrée dans de nombreux logiciels, assure la sécurité et la confidentialité de vos échanges. Vos messages pourront alors uniquement être lus par des professionnels de santé titulaires de leur carte CPS.

Responsabilité : le principe *d'accountability* pour votre cabinet

- Vous devez mettre en œuvre des mécanismes et procédures dans le cabinet médical qui permettent de protéger les données à caractère personnel, afin d'être prêts à démontrer que vous respectez le RGPD.
- En pratique : retracez, la façon dont vous protégez votre mot de passe, les règles relatives au verrouillage du clavier de votre ordinateur, à l'envoi de mails...
- Prévoyez également comment le cabinet va s'organiser en cas de piratage informatique ou de destruction accidentelle de données (information des patients par courrier par ex.).
- Vous devez également prévoir, pour vos patients, quelles sont les modalités d'accès à leurs données, les modalités de rectification, voire de portabilité de celles-ci vers un autre médecin en cas de changement.