



L'IA peut faire gagner un temps précieux au cabinet — synthèses, courriers, reformulations. Mais une donnée de santé reste une donnée ultra-sensible : la moindre saisie imprudente peut constituer une violation. Voici ce qu'il faut faire... et ne jamais faire.

La règle d'or

Aucune donnée permettant d'identifier un patient ne doit être saisie dans une IA non maîtrisée. En cas de doute : on anonymise, ou on s'abstient.

✓ Les bonnes pratiques

Anonymiser avant tout usage

Retirez nom, prénom, date de naissance, NIR et tout identifiant avant de soumettre un texte à une IA. Pas de donnée identifiante, jamais.

Utiliser un outil au cadre validé

Privilégiez une IA avec contrat, hébergement maîtrisé et conditions RGPD claires (idéalement HDS pour la santé).

Garder la décision humaine

L'IA assiste, elle ne décide pas. Le professionnel de santé relit, valide et reste responsable du contenu produit.

Vérifier chaque résultat

Une IA peut inventer (hallucination). Contrôlez les faits, posologies, références et chiffres avant toute réutilisation.

Informier et tracer les usages

Mentionnez le recours à l'IA dans vos pratiques, inscrivez le traitement au registre et définissez qui peut l'utiliser et pour quoi.

Limiter au strict nécessaire

Ne transmettez que l'information utile à la tâche. Principe de minimisation : moins de données, moins de risque.

Sécuriser les accès

Compte nominatif, mot de passe fort, double authentification. Ne partagez pas un compte IA entre collègues.

Former l'équipe

Tout le monde doit connaître ce qui est permis et interdit. Une erreur d'usage suffit à exposer des données patients.

✗ Ce qu'il ne faut JAMAIS faire

Coller un dossier patient complet

Jamais de compte rendu nominatif, d'ordonnance ou d'identité dans une IA grand public.

Croire l'IA sur parole

Ne reprenez pas un diagnostic, une dose ou une référence sans vérification : le risque clinique est réel.

Utiliser une IA gratuite « tout-venant »

Les outils sans contrat peuvent réutiliser vos saisies pour s'entraîner. Vos données vous échappent.

Envoyer une photo ou un document brut

Image médicale, carte Vitale, courrier : ces fichiers contiennent des données sensibles non maîtrisées.

Laisser l'historique activé

Désactivez la conservation/entraînement quand c'est possible ; sinon, n'y mettez aucune donnée réelle.

Déléguer une décision médicale

Aucune décision de soin ne doit reposer uniquement sur une sortie d'IA, sans contrôle humain.

Oublier le secret professionnel

Le secret médical s'applique aussi face à un outil IA : une fuite reste une violation grave.

Ignorer le volet RGPD

Pas de traitement IA de données patients sans base légale, registre, sécurité et contrat adapté.

À retenir en 2026

L'EU AI Act et le RGPD encadrent désormais l'usage de l'IA sur les données personnelles, avec une vigilance renforcée pour la santé. Avant de déployer un outil IA dans votre structure : vérifiez la base légale, le contrat de sous-traitance, l'hébergement des données et inscrivez le traitement à votre registre. En cas de fuite : notification CNIL sous 72 h si risque.

La sécurité comme fondation.

Fiche fournie par Cerberis Conseil · cerberis-conseil.fr

© 2026 Cerberis Conseil · Licence CC BY-NC-ND 4.0 | Ne remplace pas une assistance individualisée