

FICHE RÉFLEXE

SÉCURISATION DES OUTILS DE TRANSCRIPTION ET DE DICTÉE VOCALE



Les outils de dictée vocale facilitent la rédaction des comptes rendus médicaux et des observations cliniques. Toutefois, ces outils soulèvent des enjeux de confidentialité et de sécurité des données sensibles.

#1

CE QU'IL FAUT FAIRE

- Utiliser uniquement des logiciels agréés par l'hôpital pour les dictées vocales.
- Effectuer les dictées dans un lieu privé pour éviter toute écoute non autorisée.
- Protéger l'accès aux enregistrements avec un mot de passe ou un chiffrement.
- Stocker les fichiers audios dans le répertoire spécifique à cet effet, et non sur son dossier personnel.
- Effacer les fichiers audios une fois qu'ils ont été transcrits et validés, si possible.

#2

CE QU'IL FAUT ÉVITER

- Utiliser un smartphone personnel pour enregistrer des dictées médicales.
- Partager des fichiers audios par email non sécurisé ou via des applications non autorisées.
- Laisser un appareil d'enregistrement actif sans surveillance.



EXEMPLE CONCRET

Après avoir demandé l'accord signé de chaque interlocuteur présent lors d'une réunion ou d'un rendez-vous médical sur la possibilité d'être enregistré, cet enregistrement audio peut être utilisé dans la solution de dictée vocale afin de produire un compte rendu rapide et complet.

SIGNALEZ IMMÉDIATEMENT

- Tout vol ou perte d'enregistrement qui impliquerait la divulgation d'éléments sensibles
- Tout dysfonctionnement ou interrogation concernant l'utilisation de la solution



Avertir le service informatique
1017 ou 05 55 43 10 17



Ou nous contacter sur
informatique@ch-esquirol-limoges.fr