FICHE D'INFORMATION DE VOTRE PRATICIEN

Île-de-France URPS Chirurgiens-Dentistes

TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL destinés à la gestion des CABINETS MÉDICAUX ET PARAMÉDICAUX

Les BONNES PRATIQUES

USB et attaques locales :

- N'accepter aucun cadeau informatique (clefs USB, souris, haut-parleur externe, etc.).
- Protéger physiquement les équipements informatiques.
- Utiliser un filtre de confidentialité.
- Verrouiller son PC est indispensable en toutes circonstances.

Mots de passe :

- Utiliser un gestionnaire de mots de passe (Keepass/Lastpass/Dashlane par exemple).
- Vérifier si votre adresse email ou votre numéro de téléphone. a été compromis : https://haveibeenpwned.com/
- Utiliser Yopmail ou un équivalent SMS.
- Utiliser l'authentification multifacteur.
- Utiliser sa carte CPS, e-CPS ou Pro Santé Connect (cf. les délégués numériques en santé) = Le « **2e facteur** » une authentification forte déjà à la disposition des professionnels de santé.

SÉCURITÉ des périphériques nomades

LES ERREURS COURANTES

- Pas de chiffrement d'un périphérique nomade.
- Destruction non sécurisée des données.
- Reposer uniquement sur un stockage d'un périphérique amovible.
- Mixer les utilisations personnelles et professionnelles.

LES BONS RÉFLEXES

- Chiffrement total des supports susceptibles d'être perdus / volés / accédés.
- Utiliser les modes sécurisés de suppression ou des outils dédiés.
- Multiplier les sauvegardes.
- Séparation physique des appareils pro/perso.

Les LOGICIELS MALVEILLANTS / RANSOMWARE

Comment réagir ?

- Ne pas éteindre la machine concernée.
- Débrancher le câble Ethernet ET couper le Wi-Fi immédiatement.
- Prévenir un expert en informatique.
- Se rendre sur https://www.cybermalveillance.gouv.fr/
- Prévenir la Police/Gendarmerie ou le CERT Santé.
- Obligation de prévenir la CNIL dans certains cas.

Comment se protéger ?

- Utiliser un antivirus.
- Installer les mises à jour.
- Se méfier des emails.
- Ne pas installer de logiciel non fiable (chercher les sources officielles et éviter les versions « gratuites » de logiciels payants).

Comment gérer SES SAUVEGARDES ?

L'idéal

Règle du 3-2-1 :

- Au moins 3 copies des données (production et 2 backups).
- Au moins 2 supports différents pour les données (disques durs, cloud ou bandes).
- Au moins 1 copie hors site (cloud, autre site).

En pratique

Avoir des sauvegardes (testées et à jour) :

- Sous Windows : sauvegarder mon PC.
- Sous macOS : Time Machine.
- Utiliser un prestataire dédié.
- Le cloud oui, mais attention à la synchronisation !

INGÉNIERIE SOCIALE

LES ERREURS COURANTES

- Céder à « l'urgence ».
- Faire confiance à l'expéditeur.
- Ne pas utiliser de 2e facteur d'authentification.
- Réutiliser son mot de passe sur tous les services.
- Ouvrir des macros de sources inconnues.
- Croire aux trop bonnes affaires.
- Utiliser une boîte Gmail/Hotmail pour des usages pros (illégal - Article L1111-8 - Code de la santé publique).

LES BONS RÉFLEXES

- Être proactif et ne pas suivre de lien (exemple : aller soi-même sur son compte Netflix).
- « Changer de canal » (exemple : j'ai reçu un mail, je demande une confirmation par SMS) en utilisant un numéro de téléphone **que l'on possède déjà** dans ses dossiers, et non celui qui pourrait être écrit dans le mail suspect (qui pourrait être celui du pirate).
- Traiter tous les mails comme suspects.
- Si c'est trop tard : changer son mot de passe le plus vite possible.
- Utiliser la **Messagerie Sécurisée de Santé** (possibilité d'avoir une boite aux lettres organisationnelle).

IA GÉNÉRATIVE ET AGENTS

LES ERREURS COURANTES

- Saisir des données patients identifiantes dans un outil IA.
- Suivre aveuglément une recommandation IA.
- Donner des accès larges à un agent IA.
- Faire confiance à une voix au téléphone (deepfake).

LES BONS RÉFLEXES

- Anonymiser strictement les données ("Patient X").
- Utiliser des solutions HDS ou souveraines.
- Vérifier systématiquement les informations : L'IA est un assistant, pas une autorité médicale.
- Appliquer la règle du double canal pour toute demande sensible.

RISQUES SPÉCIFIQUES liés à l'IA

Confidentialité

- Risque de fuite de données de santé : Ne jamais entrer de données identifiantes.

Hallucinations

- Risque d'erreurs médicales : Toujours vérifier.

Deepfake

- Imitation de voix (fraude) : Contre-appel systématique.

Agents IA

- Injection de prompt / actions malveillantes : Limiter les droits + surveiller les logs.

RGPD et organisation

À ne pas oublier :

- Tenir un registre des traitements.
- Sensibiliser **tout le personnel.** (assistants, secrétariat = première ligne).