MINISTÈRE
DU TRAVAIL
DE LA SANTÉ
ET DES SOLIDARITÉS
Liberté
Égalité
Fraternité

ORDRE NATIONAL DES MEDECINS
Conseil National de l'Ordre

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Les bonnes pratiques de cybersécurité pour les médecins libéraux

« Des cabinets médicaux contraints de payer une rançon à des hackers »

« On n'avait plus aucune trace des rendez-vous, mais aussi des règlements, de l'historique des patients... On avait tout perdu ! »

Témoignages
de professionnels de santé
victimes d'une cyberattaque
en 2022

Voici quelques règles d'hygiène informatique à s'approprier :

01 Préservez la confidentialité des données de vos patients

Sécurisez
les accès à votre lieu de travail (porte fermée, serrure, alarme,...)

Verrouillez
votre poste de travail en cas d'absence

Pour verrouillez rapidement votre poste de travail : raccourci touches Windows + L ou Cmd + Ctrl + Q sur Mac.

02 CPx et e-CPS, des moyens de connexion sécurisés

- Respecter le caractère **personnel et strictement incessible** de ces cartes.
- Garder **secret** le code PIN de la carte
- Maintenir la carte dans un **lieu sûr** lorsqu'elle n'est pas utilisée, et dans votre champ de vision quand vous l'utilisez.

Si vous recevez, par téléphone, une demande d'authentification e-CPS qui ne correspond à aucune sollicitation de votre part, refusez l'accès ou ignorez-la et rapprochez-vous de l'ANS ou de votre CPAM au 36 08.

03 Mot de passe : ZHsj3#1&-El15°

Votre mot de passe doit être...

1 Robuste !

Au moins 12 caractères, combinaison de minuscules, majuscules, chiffres et caractères spéciaux,...)

2 Non prédictible !

Exemple : pas de date de naissance

3 Unique !

Pensez au gestionnaire de mots de passe.

MOYENS MÉMOTECHNIQUES

Les premières lettres :
« Un tiens vaut mieux que deux tu l'auras »

→ **1tvmq2tl'A**

La phonétique :
« J'ai acheté huit CD pour cent euros cet après-midi »

→ **ght8CD%E7am**

04 Qu'en est-il des données de mes patients envoyées par mail ?

Les messageries gratuites (type Gmail, Yahoo,...) ne sont pas sécurisées !

Vos mails peuvent être interceptés par des tiers et votre fournisseur (Gmail, Yahoo,...) peut les consulter et se servir de vos données à des fins commerciales. Il est également facile de créer un faux compte pour se faire passer pour un confrère.

→ **La Messagerie Sécurisée de Santé est le moyen le plus fiable et sécurisé pour vos échanges entre confrères et avec vos patients.**

NB : Vos patients disposent désormais d'une messagerie sécurisée au sein de Mon Espace Santé où vous pouvez leur communiquer en toute sécurité des documents et des données de santé.
L'adresse est **matriculeINS@patient.mssante.fr**
(l'INS est le N° de sécurité sociale pour les ouvrants droits)

Pour signaler un spam ou courrier indésirable :

www.signal-spam.fr

05 Mettre à niveau le système et les outils logiciels

Les mises à jour proposées par votre logiciel visent souvent à corriger les failles de sécurité de votre outil informatique, cessez de fermer la fenêtre et **acceptez la mise à jour !**

06 Attention à cette clé USB que l'on vous a offerte !

Les **supports amovibles** (clé USB, disque dur externe,...), dont l'origine est inconnue (trouvés dans un lieu public, dans la salle d'attente, ...) ou reçus en cadeau peuvent contenir un virus.

→ **Privilégiez l'envoi des documents par MSS.**

07 Sauvegardez les données

- Ceci permet de **restaurer le système** en cas d'incident.
- **Tester la restauration** pour s'assurer qu'elle fonctionne.
- Les sauvegardes doivent être **déconnectées** dans la mesure du possible afin de les protéger de toute atteinte suite à une cyberattaque (notamment chiffrement).
- En cas d'utilisation d'un **disque dur externe**, veiller à ce qu'il soit **chiffré**. Idéalement, le support des sauvegardes doit être **dupliqué** et **conservé à deux endroits différents** (au cabinet et au domicile par exemple).

08 Séparer les usages professionnels des usages personnels

N'accéder à des données de patients que depuis **un terminal à usage exclusivement professionnel**.

09 Sécuriser son WIFI

Masquer le nom de son réseau
(Dans les paramètres Wi-Fi > choisir Wi-Fi invisible/masqué ; le code SSID ne sera plus visible).

À noter

D'autres solutions existent et sont proposées par des professionnels (ex : solutions de type cloud).

Bien veiller à ce que le stockage soit réalisé sur un hébergement certifié HDS (Hébergement de Données de Santé).

En tant que médecin, il est de votre responsabilité d'assurer la sécurité des données de vos patients.

Votre logiciel est indisponible ?

En cas d'indisponibilité de votre logiciel de cabinet, l'accès via navigateur (y compris sur smartphone) au site dmp.fr avec votre carte CPS ou e-CPS permet de retrouver les documents clés de vos patients et de pouvoir continuer à les prendre en charge !

Vous pensez être victime d'une cyberattaque ?

1. **N'arrêtez pas ou ne redémarrez pas votre ordinateur.**
2. **N'interagissez plus avec le poste afin de conserver l'information utile pour l'analyse de l'attaque.**
3. **Déconnectez le câble réseau ou désactivez le WIFI sur le poste.**
4. **Prévenez le fournisseur informatique et / ou le Responsable de la Sécurité.**
5. **Décrivez l'incident de sécurité sur le site cybermalveillance.gouv.fr et suivre les conseils proposés**
6. **En cas de violation de données à caractère personnel, rendez-vous sur : http://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles**

Liens utiles

- Checklist des mesures d'hygiène informatique à mettre en œuvre qui, si elles sont appliquées strictement et régulièrement, vous prémunissent contre la majorité des attaques :

  Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

- Guide listant les précautions à appliquer pour respecter le RGPD dans les différents contextes de travail :

  Guide pratique sur la protection des données personnelles

- Fiche pratique à destination des patients concernant le traitement des données personnelles présentes sur Mon Espace Santé :

  Mon Espace Santé et les données personnelles