ufsbd
UNION FRANÇAISE POUR LA SANTE BUCCO-DENTAIRE

FICHE
Cybersécurité au cabinet dentaire

Enjeux

Cette fiche vise à aider les équipes à prévenir les cyberattaques et à réagir efficacement en cas d'incident.

Un cabinet dentaire manipule des **données de santé sensibles** (logiciel métier et base de données patients, DMP, radios, chaîne numérique, comptes-rendus, informations administratives). Une faille peut entraîner…

- **Perte d'accès aux dossiers patients** (ransomware).
- **Fuite de données** → sanctions CNIL / préjudice patients.
- **Paralysie du cabinet** (agenda, paiements, chaîne numérique, imagerie).
- **Atteinte à la réputation.**

Un cabinet dentaire manipule des données de santé sensibles : prévenir les cyberattaques et réagir efficacement en cas d'incident.

Les menaces principales

- **Phishing/mails frauduleux :** messages imitant CPAM, URSSAF, banques, fournisseurs, demandant un clic ou une pièce jointe.
- **Ransomware (rançongiciel) :** logiciel bloquant les données contre rançon.
- **Intrusion réseau :** mot de passe faible, wifi non sécurisé.
- **Vol/perte de matériel :** ordinateur, disque de sauvegarde ou clé USB contenant des données patients.
- **Logiciels non à jour :** failles de sécurité exploitées par des pirates.

Les bonnes pratiques essentielles

SÉCURITÉ DES POSTES INFORMATIQUES

- Verrouiller son ordinateur dès qu'on s'éloigne (manuellement Windows+L ou par économiseur délai court).
- Utiliser un **antivirus professionnel** et un **pare-feu activé**.
- Activer l'authentification à deux facteurs (2FA) quand elle est disponible.
- Faire toutes les **mises à jour** (Windows/Mac OS/Linux..., logiciels métiers, navigateurs et en premier lieu l'antivirus).
- Ne pas laisser les cartes CPS, CPE ou CPA dans les lecteurs en cas d'absence des titulaires respectifs.
- Changer les mots de passe en cas de départ d'un salarié ou prestataire.

GESTION DES MOTS DE PASSE

- Un mot de passe **unique**, long (12–16 caractères), complexe.
- Ne jamais réutiliser le même sur plusieurs sites.
- Utiliser un **gestionnaire de mots de passe**.
- Changer les mots de passe en cas de départ d'un salarié ou prestataire.
- Activer l'**authentification à deux facteurs (2FA)** quand elle existe.

VIGILANCE FORTE FACE AUX E-MAILS ET SUR LES SITES INTERNET

- Les ordinateurs du cabinet ne sont jamais utilisés pour des usages privés, notamment la navigation internet.
- Vérifier l'expéditeur réel (adresse réelle complète).
- Ne jamais cliquer sur un lien ni ouvrir une pièce jointe suspecte.
- Se méfier des urgences artificielles (« votre compte sera fermé », « régularisation immédiate » visant à vous faire réagir en stress sans réfléchir).
- Les organismes officiels ne demandent jamais de mot de passe par mail.
- En cas de doute : **ne pas répondre et signaler**.

Sécurité des données patients

- Sauvegarde **quotidienne** des dossiers patients, radios, imagerie :
  - > sur support chiffré ou serveur sécurisé ;
  - > avec **au moins 3 copies** dont une hors site ;
  - > tester régulièrement les sauvegardes.
- Chiffrer les données sensibles lorsque c'est possible.
- N'utiliser **que des services conformes RGPD** (hébergeur de données de santé agréé HDS pour le stockage en ligne).
- Ne jamais transférer de données patients par e-mail non sécurisé : entre professionnels de santé, sur les plateformes mail telles que Mailiz (MSsanté), les échanges se font en toute sécurité.

Sécurisation du réseau du cabinet

- Séparer le **wifi patients** du **wifi professionnel**.
- Mot de passe wifi complexe, à changer régulièrement.
- Arrêter les accès distants inutiles (surtout si le niveau de sécurité des « distants » est moindre).
- Firewall installé et configuré (box professionnelle ou firewall dédié).

Gestion des appareils

- Smartphones, tablettes, PC :
  - > verrouillage par code/biométrie ;
  - > chiffrement activé ;
  - > synchronisation via des services sécurisés.
- Interdiction d'utiliser des **clés USB personnelles** non vérifiées.
- En cas de perte ou vol → **déclaration immédiate**, effacement à distance, changement de mots de passe.

Organisation interne

- **Procédure interne écrite** pour : sauvegardes, gestion des incidents, mise à jour, règles d'accès.
- Nommer un **référent cybersécurité** du cabinet.
- Former régulièrement l'équipe : revoir les procédures d'urgence tous les mois.
- Limiter les droits utilisateurs : pas d'administrateur pour les postes standard.

ufsbd
UNION FRANÇAISE POUR LA SANTÉ BUCCO-DENTAIRE

La cybersécurité n'est pas un choix mais une obligation légale et déontologique. Avec quelques réflexes simples, un cabinet peut éviter 95 % des attaques.

En cas d'incident

1. **Déconnecter** immédiatement l'ordinateur d'internet ou du réseau.
2. **Ne pas payer** de rançon.
3. Appeler un spécialiste informatique/prestataire cybersécurité.
4. Les données des patients sont soumises au RGPD. *En cas de violation de données, une déclaration à la CNIL doit être effectuée dans les 72h.*
5. Déclarer à la CNIL sous 72h si des données patients sont exposées.
6. Prévenir l'assurance *(souvent une cyberprotection est incluse dans les contrats pro)*.
7. Informer les patients si nécessaire.

OUTILS UTILES

> Gestionnaires de mots de passe (pro).
> Antivirus/Endpoint protection (endpoint : point faible des réseaux d'entreprise porte d'entrée fréquente des attaques).
> Services HDS pour l'hébergement (HDS = hébergeur de données de santé agréé).
> Solution de sauvegarde automatisée (local + cloud HDS).
> Formations libres (exemple : ANS).

https://esante.gouv.fr/se-former-a-la-e-sante#:~:text=L'accès%20à%20ANS%2DFormation,écosystème%20du%20numérique%20en%20santé

Une cybersécurité renforcée protège vos patients et votre activité.

SÉCURITÉ DES ACCÈS
VERROUILLER LES POSTES, MOTS DE PASSE FORTS, 2FA

VIGILANCE E-MAILS
IDENTIFIER PHISHING, NE PAS CLIQUER SUR LIENS SUSPECTS

SAUVEGARDES
SAUVEGARDES QUOTIDIENNES RÈGLE 3-2-1, SUPPORTS CHIFFRÉS

RÉSEAU
SÉPARER WIFI PATIENTS/PRO, MOT DE PASSE COMPLEXE, FIREWALL

MATÉRIEL
CHIFFREMENT, VERROUILLAGE MOBILE/PC, ÉVITER CLÉS USB

FORMATION ÉQUIPE
SENSIBILISATION RÉGULIÈRE AUX BONNES PRATIQUES

ufsbd
UNION FRANÇAISE POUR LA SANTÉ BUCCO-DENTAIRE

Exemple de fiche récapitulative à compléter pour votre cabinet

En cas d'incident informatique

1. **Déconnecter** immédiatement l'ordinateur d'internet ou du réseau ..... ☐
2. **Ne pas payer** de rançon ..... ☐
3. Appeler un spécialiste informatique/prestataire cybersécurité ..... ☐
4. Les données des patients sont soumises au RGPD ..... ☐
   En cas de violation de données, une déclaration à la CNIL doit être effectuée dans les 72h.
5. Déclarer à la CNIL sous 72h si des données patients sont exposées ..... ☐
6. Prévenir l'assurance (souvent une cyberprotection est incluse dans les contrats pro)..... ☐
7. Informer les patients si nécessaire ..... ☐

Contacts utiles en cas de cyberincident

- ☑ **Prestataire informatique** .....
- ☑ **Délégué à la protection des données du cabinet** .....
- ☑ **Assureur** .....
- ☑ **Site Cyber 17**
  Site gouvernemental d'assistance et de prévention www.cybermalveillance.gouv.fr
- ☑ **CNIL** *déclaration* https://signalement.social-sante.gouv.fr/espace-declaration/guidage?profil=PROFESSIONNEL_SANTE
- ☑ **CERT Santé** *informations/aide* www.cyberveille.esante.gouv.fr

Check-list cybersécurité
vérification trimestrielle

ÉLÉMENTS À VÉRIFIER	OUI	NON	COMMENTAIRES
Les mots de passe respectent les règles de sécurité	☐	☐	
Les logiciels sont à jour (vérifier Windows update et Windows Defender)	☐	☐	
Les sauvegardes sont testées et fonctionnelles	☐	☐	
L'équipe a été sensibilisée à la cybersécurité	☐	☐	
Un contact d'urgence est disponible et à jour	☐	☐	

Date du contrôle : .....

Signature du responsable :