Autoévaluation cybersécurité - profil cabinet à renforcer

Méd'In Occ

Plusieurs réflexes utiles sont déjà présents dans votre cabinet, mais que certains points méritent d'être consolidés.
L'objectif n'est pas de tout reprendre, ni de tout traiter immédiatement. Il s'agit d'identifier les pratiques les plus exposantes et de les corriger dans le bon ordre, en commençant par ce qui protège la continuité du cabinet et les données patients.

Quelques actions ciblées peuvent déjà réduire fortement le risque : sécuriser les accès, vérifier les sauvegardes et formaliser la conduite à tenir

Votre plan d'action

Sécuriser les accès sensibles

- Vérifiez les accès aux outils essentiels du cabinet : logiciel métier, messagerie, agenda, Ameli Pro.
- Chaque utilisateur doit disposer de son propre accès.
- Évitez les mots de passe identiques entre plusieurs outils et activez la double vérification dès qu'elle est disponible.

Vérifier les sauvegardes et les mises à jour

- Assurez-vous que les données utiles au fonctionnement du cabinet sont bien sauvegardées : dossiers patients, agenda, documents médicaux.
- Vérifiez aussi que les postes, logiciels et téléphones utilisés pour l'activité sont mis à jour régulièrement.

Préparer la réaction en cas d'incident

- Identifiez le bon contact à appeler en cas de problème informatique.
- Affichez ce contact au cabinet et prévoyez une consigne simple : isoler le poste suspect si possible, éviter les manipulations hasardeuses et appeler le référent.

Un repère simple pour les sauvegardes : 3-2-1

3 copies – Avoir les données du cabinet + au moins deux copies exploitables.

2 supports – Avoir deux supports ou espaces différents, pour éviter un point de défaillance unique.

1 copie protégée – Avoir une copie déconnectée, isolée ou protégée contre l'écrasement