Autoévaluation cybersécurité - profil cabinet exposé

Méd'In Occ

Vos réponses font apparaître plusieurs points de fragilité qui peuvent exposer le cabinet à un blocage d'activité, une perte de données ou une fuite de données patients.

L'objectif n'est pas de tout régler seul, ni de tout corriger immédiatement. Il s'agit d'abord de sécuriser les points essentiels, dans le bon ordre : pouvoir récupérer les données, savoir qui appeler, puis renforcer les accès aux outils du cabinet.

Les premières actions à engager sont simples, mais elles ne doivent pas être différées.

Votre plan d'action

Vérifier les sauvegardes sans attendre

- Vérifiez si les données utiles au fonctionnement du cabinet sont bien sauvegardées : dossiers patients, agenda, documents médicaux.
- Demandez à votre prestataire si les sauvegardes sont automatiques, récentes, protégées et si une restauration a déjà été testée.

Identifier un contact d'appui en cas d'incident

- Identifiez le bon contact à appeler : prestataire informatique, référent interne ou assistance cyber.
- Affichez ce contact au cabinet et partagez-le avec les personnes concernées.

Sécuriser les accès essentiels

- Reprenez les accès aux outils les plus sensibles : logiciel métier, messagerie, agenda, Ameli Pro.
- Changez les mots de passe réutilisés, évitez les accès partagés et activez la double vérification dès qu'elle est disponible.

En cas d'incident : 3 réflexes essentiels

Préserver – Ne pas restaurer immédiatement (sans avis technique), ne pas écraser les sauvegardes disponibles et conserver les traces utiles.

Prioriser – Identifier les données indispensables à la continuité des soins et organiser leur reprise.

Signaler – Si des données patients sont compromises, documenter l'incident et effectuer les déclarations réglementaires lorsque nécessaire.

En cas de violation de données à caractère personnel présentant un risque pour les personnes concernées, la notification à la CNIL doit intervenir dans les **72 heures** : https://www.cybermalveillance.gouv.fr/signalement

Les personnes concernées doivent également être informées lorsque le risque est élevé.