Autoévaluation cybersécurité - profil cabinet sécurisé

Méd'In Occ

Vos réponses indiquent que les principaux réflexes de cybersécurité sont globalement en place dans votre cabinet. Les accès semblent maîtrisés, les pratiques numériques sont plutôt structurées et les points essentiels de protection sont en grande partie couverts.

L'enjeu est de maintenir ce niveau dans la durée et de vérifier régulièrement les points sensibles : accès utilisateurs, sauvegardes, mises à jour et conduite à tenir en cas d'incident.

Votre plan d'action

Vérifier régulièrement les accès

- Contrôlez une à deux fois par an les comptes actifs sur vos outils professionnels.
- Supprimez les accès devenus inutiles et conservez des accès nominatifs pour chaque utilisateur.

Tester les sauvegardes

- Vérifiez que vos données essentielles sont bien sauvegardées automatiquement : dossiers patients, agenda, documents médicaux.
- Demandez à votre prestataire si une restauration a déjà été testée.

Entretenir les bons réflexes

- Gardez visible le contact à appeler en cas d'incident, rappelez les bons réflexes face aux messages suspects et mettez à jour votre fiche réflexe au moins une fois par an.

Checklist vérification pour sécuriser vos pratiques

- **Données critiques identifiées** – dossiers patients, agenda, documents médicaux, facturation/télétransmission.
- **Sauvegarde maîtrisée** – La sauvegarde est automatique, récente et surveillée.
- **Copie protégée** – Une copie est protégée ou inacessible depuis le poste de travail au quotidien.
- **Restauration testée** – La reprise des données a déjà été testée et le délai de retour à l'activité est connu.
- **Procédure connue** – Chaque membre du cabinet sait quoi faire et qui contacter en cas d'incident.