Cybersécurité – Comment protéger mon activité ?

Méd'in Occ

Menaces externes

Cyberattaques : les cabinets médicaux sont des cibles privilégiées pour les pirates informatiques en raison de la valeur élevée des données de santé sur le marché noir.

Phishing : les tentatives d'hameçonnage visant à obtenir des identifiants d'accès sont fréquentes.

Ransomware : les attaques par rançongiciel peuvent bloquer l'accès aux dossiers patients et paralyser l'activité du cabinet.

Vulnérabilités internes

Erreurs humaines : le manque de formation du personnel aux bonnes pratiques de sécurité est un facteur de risque majeur.

Mots de passe faibles : l'utilisation de mots de passe peu sécurisés facilite les intrusions.

Systèmes obsolètes : les logiciels et équipements non mis à jour présentent des failles de sécurité.

Défis technologiques

Adoption du cloud : la migration vers des solutions cloud nécessite de nouvelles mesures de protection.

Appareils mobiles : l'utilisation croissante de smartphones et tablettes augmente les risques de fuite de données.

Interopérabilité : le partage sécurisé des données entre différents systèmes est complexe.

Conformité RGPD

Le respect des obligations légales en matière de protection des données personnelles est exigeant.

Bonnes pratiques essentielles

- Utilisez des mots de passe uniques, complexes et personnels pour chaque compte.
- Ne stockez pas de données sur des supports amovibles comme des clés USB ou téléphones portables.
- Mettez régulièrement à jour vos logiciels et systèmes d'exploitation.
- N'ouvrez jamais d'emails ou pièces jointes suspects.
- Utilisez une messagerie sécurisée de santé pour les échanges professionnels, plutôt que des applications grand public comme WhatsApp.

Protection des données

Installez et maintenez à jour un antivirus sur tous les appareils.
Activez le pare-feu sur vos ordinateurs et équipements réseau.
Chiffrez les disques durs de vos appareils, surtout les portables.
Sécurisez votre réseau Wi-Fi avec un mot de passe fort.

En cas d'incident

Ayez un plan d'action prédéfini en cas d'attaque informatique.
Déconnectez immédiatement l'appareil infecté du réseau.
Contactez rapidement votre prestataire informatique ou l'équipe d'experts en cybersécurité de votre fournisseur de logiciel médical.

Sécurisation du système informatique

Sauvegardez vos données auprès d'un hébergeur certifié Hébergeur de Données de Santé (HDS).
Stockez les sauvegardes dans un endroit sûr, de préférence hors site.
Sensibilisez tout le personnel du cabinet à la protection des données de santé.

Aspects réglementaires

Respectez le Règlement Général sur la Protection des Données (RGPD).
Utilisez le Dossier Médical Partagé (DMP) pour stocker les informations de santé des patients.
Vérifiez que vos prestataires informatiques respectent les normes de sécurité requises.