🚨 Note d'Information Importante concernant un Incident de Sécurité Informatique

Madame, Monsieur, Chers Patients,

Nous vous informons par la présente d'un **incident de sécurité informatique** survenu chez notre prestataire éditeur de la solution logicielle de gestion de votre dossier médical.

À la date du **14 Novembre 2025**, cet éditeur nous a confirmé avoir été victime d'une attaque informatique. Bien que cet incident soit désormais clos, il a pu permettre la consultation éventuelle de certaines données de votre dossier médical, entraînant une **perte de confidentialité** des données présentes sur le serveur concerné.

Données Personnelles Potentiellement Impactées

Nous tenons à vous informer que les données à caractère personnel ci-dessous ont potentiellement été compromises :

- **Votre Nom et Prénom**
- **Votre Adresse Postale**
- **Votre Numéro de Téléphone**
- **Votre Adresse Email**
- **Certaines de vos données de santé** potentiellement impactées par l'incident.

Mesures Prises et Conséquences Probables

Nous vous prions tout d'abord d'accepter nos plus sincères excuses pour les désagréments que cet incident pourrait occasionner.

- **Gestion de l'Incident :** Notre prestataire est en contact avec les autorités compétentes et déploie actuellement toutes les mesures techniques et juridiques nécessaires pour renforcer sa sécurité.
- **Autorité de Contrôle :** Conformément à la réglementation en vigueur (RGPD), nous avons procédé à la **notification de cet incident auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).**
- **Risques Potentiels :** Vos données pourraient être utilisées à des fins malveillantes, notamment pour des tentatives d'attaques de type **"phishing"** (hameçonnage) ou **"credential stuffing"** (utilisation de couples identifiants/mots de passe volés sur d'autres sites). Vous pouvez consulter le site de la CNIL pour en savoir plus sur ces attaques :
    - https://www.cnil.fr/fr/definition/credential-stuffing-attaque-informatique

---

Recommandations de Sécurité (À Appliquer Urgemment)

Nous vous recommandons **fortement** d'appliquer les mesures de sécurité suivantes :

I. Vigilance contre les Attaques (Phishing/Spam)

- **Soyez vigilants** si vous recevez des emails ou SMS dont vous ne connaissez pas l'émetteur : **ne cliquez sur aucun lien et ne répondez pas** à ces messages.
- **Ne cliquez jamais** sur des liens hypertextes contenus dans des messages qui semblent suspicieux.
- **Ne renseignez jamais de coordonnées bancaires** en réponse à un message, même s'il semble émaner de votre Banque. En cas de doute, contactez votre organisme bancaire directement.
- **Signalez les spams et tentatives de phishing** sur la plateforme nationale Signal Spam :
    - Inscrivez-vous gratuitement sur www.signal-spam.fr.
    - Téléchargez l'extension pour votre logiciel de messagerie ou votre navigateur web.
    - Signalez les messages suspects en un clic.

II. Gestion de vos Mots de Passe

- **Changez immédiatement** tous les mots de passe **identiques ou similaires** que vous utilisez sur d'autres comptes personnels (réseaux sociaux, banque, etc.) par un mot de passe **différent** et **unique** pour chaque service.
- **Utilisez uniquement des mots de passe robustes.** Pour générer un mot de passe solide, consultez le site de la CNIL :
    - https://www.cnil.fr/fr/generer-un-mot-de-passe-solide
- **Surveillez toute activité suspecte** sur vos comptes en ligne.

Contact

D'une façon générale, nous vous invitons à une **vigilance particulière** concernant toute activité suspecte relative à vos données à caractère personnel.

Nous nous tenons bien entendu à votre entière disposition pour toute information complémentaire sur cet incident.

L'équipe de la Maison de Santé de Coulondres