Notification de violation de données

Madame, Monsieur,

A date du 14 Novembre 2025, notre prestataire éditeur d'une solution logicielle de gestion de dossier médical nous a informé avoir subi un incident de sécurité informatique.
Notre prestataire a subi une attaque informatique ayant permis la consultation éventuelle de certaines données de votre dossier médical, et ayant pour conséquence une perte de confidentialité des données présentes sur le serveur concerné.
Si cet incident de sécurité est désormais clos, certaines de vos données à caractère personnel ont potentiellement été impactées par cet acte malveillant.

Les données personnelles concernées sont les suivantes :

- Votre nom
- Votre prénom
- Votre adresse email
- Votre numéro de téléphone
- Votre adresse postale
- Certaines de vos données de santé potentiellement impactées par l'incident.

Dans un premier temps, nous tenons à vous présenter nos excuses pour cet incident :
notre prestataire est actuellement en contact avec les autorités et sont en train de déployer les mesures techniques et juridiques nécessaires.
Nous avons procédé à une notification de cet incident auprès de la Commission Nationale de l'Informatique des Libertés (CNIL) conformément aux dispositions réglementaires applicables.
Concernant les conséquences probables de la violation, vos données à caractère personnel sont susceptibles d'être potentiellement utilisées à des fins malveillantes, et notamment afin de réaliser des tentatives d'attaques de type « phishing » ou « credential stuffing » : vous pouvez en savoir plus sur ces types d'attaques en consultant le site de la CNIL :
https://www.cnil.fr/fr/definition/credential-stuffing-attaque-informatique
En conséquence, nous vous recommandons fortement d'appliquer les recommandations suivantes de sécurité :

- Soyez particulièrement vigilants si vous recevez des emails et/ou SMS dont vous ne connaissez pas l'identité de l'émetteur : ne cliquez sur aucun lien et ne répondez pas à ces messages suspects ;
- Ne cliquez pas sur des liens hypertextes contenus dans des messages semblant suspicieux ;
- Ne renseignez jamais de coordonnées, et notamment de coordonnées bancaires, même si le message semble émaner de votre Banque. En cas de doute, contactez directement votre organisme bancaire ;
- Si vous avez reçu un spam sur votre messagerie électronique, ou si le message paraît être une tentative de phishing, ne répondez pas et n'ouvrez pas les pièces jointes, les images ou les liens contenus dans le message. Signalez-le à la plateforme Signal Spam.o Inscrivez-vous gratuitement sur www.signal-spam.fr;

o Téléchargez une extension pour votre logiciel de messagerie (Thunderbird, Outlook ou Mail pour Mac) ou votre navigateur web si vous consultez votre boîte de messagerie sur un site internet (Chrome, Safari, Firefox).
o Signalez en un clic.

- Concernant la gestion de vos mots de passe :

o Changer tous les mots de passe identiques ou similaires utilisés sur vos autres comptes personnels (réseaux sociaux, espace bancaire, etc…) par un mot de passe différent ;
o N'utilisez que des mots de passe robustes. Pour en savoir plus, vous pouvez générer un mot de passe solide sur le site de la CNIL en cliquant ici :
https://www.cnil.fr/fr/generer-un-mot-de-passe-solide
o Vérifier l'intégrité de vos données sur chaque compte en ligne concerné et surveillez toute activité suspecte sur tous les comptes.
D'une façon générale, nous vous invitons à une vigilance particulière concernant toute activité suspecte identifiée sur vos données à caractère personnel.
Nous nous tenons bien naturellement à votre entière disposition pour toute information complémentaire sur cet incident : vous pouvez nous contacter sur ce sujet à l'adresse suivante coordinatricemspno@gmail.com.

Cordialement.