



La Cyber-Lettre de la **GENDARMERIE** **RÉGION GRAND EST**



Année 2025 – Hors Série n° 03

💥 Cyberattaque, fuite de données Le secteur médical concerné

DIFFUSION
LIBRE

Dans la nuit du 10 au 11 novembre 2025, l'éditeur **Weda** et le 28 novembre 2025, le site **Médecin Direct**, tous 2 certifiés **HDS** (*Hébergeur agréé de Données de Santé*), le niveau attendu pour protéger les données de santé, ont détecté des activités suspectes sur leurs plateformes respectives. L'éditeur Weda a coupé immédiatement ses accès. La **CNIL** (*Commission Nationale de l'Informatique et des Libertés*) est avisée des faits dans la foulée.

👨‍⚕️ Plus de **23 000** des 85 000 **professionnels de santé** se retrouvent brutalement privés de leur outil quotidien. Pendant trois jours, certains cabinets ont dû recourir au **papier et au crayon** avant qu'un accès dégradé soit remis en place.

🔍 L'**article 4 (15)** du **RGPD** (*Règlement Européen sur la Protection des Données*) nous rappelle ce qu'est une **donnée de santé**. L'**article 9**, lui, précise qu'un médecin **peut traiter ces données sans consentement explicite** lorsqu'il s'agit des soins ou du suivi médical, dans le respect du **secret médical** et avec des **mesures de sécurité adaptées**

📢 Selon le communiqué de Weda, les données concernées seraient :

- nom ;
- prénom ;
- adresse e-mail ;
- numéro de téléphone ;
- adresse postale ;
- des données de santé....

N'oubliez pas d'aviser vos patients.



Quels risques pour un professionnel

- Les données stockées pourraient être tronquées ;
- Un escroc pourrait se faire passer pour le service technique Weda ;
- Réception de phishing personnalisé ;
- Fausse facture,


Quels risques pour un particulier

- Phishing ciblé (faux remboursement, rendez-vous, CPAM...) ;
- Tentative de connexion à des services administratives ou privées ;
- Tentative d'ouverture de faux compte (usurpation d'identité),

Nos Conseils

- Changer vos mots de passes ;
- Activer la double authentification ;
- Rester vigilant.

Vous êtes victime ?

Appelez immédiatement le  **17** ou  contacter :



LE 17 CYBER

Une cyberattaque, échangez avec un cybergendarme - 24h/24 7j/7
<https://17cyber.gouv.fr/>



GRAND EST CYBERSECURITE

Assistance cyberattaque gratuite
Tel : 0 970 512 525
www.cybersecurite.grandest.fr



LA CNIL

Prévenir en cas de fuite de données personnelles, réelle ou supposée.



CYBERMALVEILLANCE

Pour vous faire assister, vous informer ou vous former
www.cybermalveillance.gouv.fr



LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7



L'ANSSI

Assiste les entités essentielles et les entités importantes, fournit des guides
<https://cyber.gouv.fr>



THÉSÉE

Déposer plainte en ligne pour les victimes d'e-escroqueries



APPLICATION MA SÉCURITÉ

Trouver des informations de prévention et les démarches en ligne.

+ D'INFO



**Vous souhaitez joindre un Référent Cyber
de la Région de Gendarmerie du Grand-Est
ou vous abonner à la Cyber-lettre**
prevention-ggdXX@gendarmerie.interieur.gouv.fr
(Remplacez les XX par votre département)



01010010 01001001 01010011 01000011 01001000