Une nouvelle fuite d'ampleur inédite touche le système de santé français. Selon des révélations concordantes de *TF1-LCI*, *Libération* et *Franceinfo*, entre **10 et 15 millions de données médicales de patients** auraient été compromises à la suite d'un piratage informatique visant un prestataire du secteur.

Une base de données de santé exfiltrée

Les informations exposées proviendraient d'un sous-traitant informatique de laboratoires d'analyses médicales, chargé notamment de la gestion de rendez-vous et de comptes patients. Les données potentiellement concernées incluraient :

- identité (nom, prénom, date de naissance)
- coordonnées (adresse, téléphone, email)
- numéro de sécurité sociale
- informations médicales et examens biologiques

Selon les premiers éléments, les fichiers auraient été **exfiltrés puis diffusés sur des forums clandestins**, pratique classique dans l'économie cybercriminelle.

Une des plus grandes fuites de données de santé en France

Avec jusqu'à 15 millions d'enregistrements, l'incident se rapprocherait de la fuite de 2021 touchant les laboratoires français (près de 500 000 patients), mais à une échelle bien supérieure. Les experts évoquent déjà l'une des plus importantes violations de données de santé en France.

Risques élevés d'usurpation d'identité

Les données de santé comptent parmi les plus sensibles juridiquement. Leur diffusion expose les victimes aux fraudes à la sécurité sociale, aux escroqueries ciblées (phishing médical), à l'usurpation d'identité ou au chantage ou à la discrimination. La combinaison identité et numéro de sécurité sociale constitue en effet une clé d'accès à de nombreux services administratifs.

Enquête en cours et alerte des autorités

La CNIL et les autorités judiciaires ont été saisies. Une enquête vise à déterminer :

- l’origine exacte de l’intrusion
- les failles de sécurité du prestataire
- l’étendue réelle des données compromises
- les responsabilités juridiques

Le RGPD impose aux acteurs de santé des obligations renforcées en matière de cybersécurité et de notification des violations de données.

Un système de santé sous pression cyber

Depuis plusieurs années, les hôpitaux et laboratoires français sont des cibles privilégiées :

- rançongiciels hospitaliers
- vols de dossiers patients
- piratages de plateformes médicales

La valeur des données de santé sur le marché noir dépasse souvent celle des données bancaires, en raison de leur caractère durable et exploitable.

Ce que doivent faire les patients

Les autorités recommandent aux personnes susceptibles d’être concernées :

- vigilance accrue face aux emails ou SMS médicaux
- surveillance des remboursements Assurance maladie
- signalement de toute fraude
- changement de mots de passe médicaux

À retenir

- 10 à 15 millions de données médicales compromises
- Prestataire de laboratoires d’analyses visé
- Données hautement sensibles (NIR, santé)
- Enquête CNIL et judiciaire ouverte

Partager :