CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

# NOTIFICATION D'UNE VIOLATION DE DONNÉES PERSONNELLES

## NOTIFICATION COMPLÉMENTAIRE / MODIFIÉE

## RÉFÉRENCES DE LA NOTIFICATION INITIALE

| | |
|---|---|
| **N° de la notification initiale** | FR2509011600006 |
| **Date et heure de la notification initiale** | 01/09/2025 à 16h |

## ORGANISME(S) CONCERNÉ(S) PAR LA VIOLATION

### ORGANISME RESPONSABLE DE TRAITEMENT

| | |
|---|---|
| **N° SIREN** | 834652612 |
| **Dénomination de l'organisme** | GROUPEMENT DE COOPERATION SANITAIRE NORMAND'E-SANTE |
| **Numéro de TVA intracommunautaire** | FR7834652612 |
| **Adresse postale** | 7 LONGUE VUE DES ASTRONOMES<br>14111 LOUVIGNY |
| **Pays** | France |

### RESPONSABLE LÉGAL

| | |
|---|---|
| **Nom du représentant légal** | Monsieur JÉRÔME RIFFLET |
| **Adresse de messagerie** | contact@normand-esante.fr |

CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

## PERSONNE À CONTACTER

| | |
|---|---|
| **Nom, prénom du contact** | Madame MATHILDE STINES |
| **Fonction** | DPO externe |
| **Adresse de messagerie** | dpo@lexagone.fr |
| **Téléphone** | 06 62 23 60 35 |
| **Adresse postale** | 7 LONGUE VUE DES ASTRONOMES<br>14111 LOUVIGNY |
| **Pays** | France |

## AUTRES ORGANISMES IMPLIQUÉS

**Autres organismes impliqués** ☑

396 structures utilisatrices des services de NES ont été impactées par cette violation.

15 structures ont des données personnelles administratives de patient qui ont été compromises.

# NATURE DE LA VIOLATION

## DATE DE LA VIOLATION

| | |
|---|---|
| **Date et heure de la violation** | - |
| **Date et heure du début de la violation** | 22/10/2024 09:00 |
| **Date et heure de la fin de la violation** | 10/01/2025 18:00 |
| **Date et heure de prise de connaissance de la violation** | 29/08/2025 16:00 |
| Date et heure de notification par le prestataire | 29/08/2025 16:00 |
| La violation s'est étendue sur une période déterminée | ☑ |
| La violation est-elle toujours en cours ? | ☒ |

**Commentaires sur les dates**

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

**Circonstances de la découverte de la violation**

Le GRADeS Normand'e-santé (NES) a reçu une alerte du CERT Santé le 29/08 matin concernant la découverte dans le darknet d'informations démontrant que des acteurs malveillants avaient pu avoir accès aux plateformes des GRADeS depuis des adresses IP qualifiées de « compromises ».

La revue des traces techniques a permis de déterminer que 3 comptes avaient réalisé des accès légitimes au sens applicatif (utilisation d'un compte utilisateur valide) avec les adresses IP identifiées par le CERT Santé.

NES a également réalisé une déclaration au CERT Santé et une plainte a été déposée auprès du service compétent.

**Indiquez les raisons du retard**

Alerte du CERT SANTE le 29/08 matin sur des adresses IP qualifiées de « compromises » par rapport aux infrastructures de l'ensemble des GRADeS.

## A PROPOS DE LA VIOLATION

### NATURE DE LA VIOLATION

Perte de la confidentialité ☑

Perte de l'intégrité ☒

Perte de la disponibilité ☒

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

## ORIGINE(S) DE L'INCIDENT

| | |
|---|---|
| Equipement perdu ou volé | ☒ |
| Papier perdu, volé ou laissé accessible dans un endroit non sécurisé | ☒ |
| Courrier perdu ou ouvert avant d'être retourné à l'envoyeur | ☒ |
| Piratage, logiciel malveillant (par exemple rançongiciel) et/ou hameçonnage | ☑ |
| Mise au rebut de documents papier contenant des données personnelles sans destruction physique | ☒ |
| Mise au rebut d'appareils numériques contenant des données personnelles sans effacement sécurisé | ☒ |
| Publication non volontaire d'informations | ☒ |
| Données de la mauvaise personne affichées sur le portail du client | ☒ |
| Données personnelles envoyées à un mauvais destinataire | ☒ |
| Informations personnelles divulguées de façon verbale | ☒ |
| Autre | ☒ |

**Autres origines**

-

**Descriptif détaillé de la violation**

L'analyse approfondie par les équipes support de l'éditeur Maincare a relevé, pour 2 des comptes, une énumération de l'annuaire patient pouvant permettre une extraction des données administratives de ceux-ci.

Concrètement, les identités des patients des services connectés ou alimentant le Serveur Régional d'Identité (SRI) sont susceptibles d'avoir été consultées ou subtilisées par le(s) cyberattaquant(s).

Ces opérations d'extraction se sont déroulées les 22/10/2024, 26/12/2024, 09/01/2025 et 10/01/2025, dernière date constatée par la cyberattaque.

Depuis cette date, aucun accès frauduleux au système d'information de l'ENRS (Espace Numérique Régional de Santé : le portail d'accès aux services mis à disposition par NES) n'a été identifié.

CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

## CAUSE(S) DE L'INCIDENT

| | |
|---|---|
| Acte interne malveillant | ☒ |
| Acte interne accidentel | ☒ |
| Acte externe malveillant | ☑ |
| Acte externe accidentel | ☒ |
| Inconnu | ☒ |
| Autre | ☒ |

**Autres causes**

-

## NATURE DES DONNÉES CONCERNÉES PAR LA VIOLATION

| | |
|---|---|
| Etat civil (ex : nom, sexe, date de naissance, âge...) | ☑ |
| NIR (Numéro d'Inscription au Répertoire) | ☑ |
| Coordonnées (ex : adresse postale ou électronique, numéros de téléphone fixe ou portable...) | ☑ |
| Données d'identification ou d'accès (ex : identifiant, mot de passe, numéro client...) | ☒ |
| Données relatives à des informations financières (ex : revenus, numéro de carte de crédit, coordonnées bancaires), économiques | ☒ |
| Documents officiels (Passeports, pièces d'identité, etc.) | ☒ |
| Données de localisation | ☒ |
| Données relatives à des infractions, condamnations, mesures de sûreté | ☒ |
| Les données concernées ne sont pas connues pour le moment | ☒ |
| La violation concerne d'autres données | ☒ |

**Autres données**

-

DONNÉES SENSIBLES

| | |
|---|---|
| Origine raciale ou ethnique | ☒ |
| Opinions politiques | ☒ |
| Opinions philosophiques ou religieuses | ☒ |
| Appartenance syndicale | ☒ |
| Orientation sexuelle | ☒ |
| Données de santé | ☒ |
| Données biométriques | ☒ |
| Données génétiques | ☒ |

| | |
|---|---|
| **Nombre approximatif d'enregistrements concernés par la violation** | 804 972 |

## CATÉGORIES DE PERSONNES CONCERNÉES PAR LA VIOLATION

| | |
|---|---|
| Employés | ☒ |
| Utilisateurs | ☒ |
| Adhérents | ☒ |
| Etudiants / élèves | ☒ |
| Personnel Militaire | ☒ |
| Clients (actuels ou potentiels) | ☒ |
| Patients | ☑ |
| Mineurs | ☒ |
| Personnes vulnérables | ☒ |
| Pas déterminé pour le moment | ☒ |
| Autres | ☒ |

**Autres Personnes**

-

**Nombre approximatif de personnes concernées par la violation** 159 254

**Mesures de sécurité préalables à la violation**

Gestion des annuaires utilisateurs avec des habilitations permettant des accès limités aux données strictement nécessaires à leurs fonctions.

Cycle de vie des mots de passe : expiration tous les 6 mois.

Revue des comptes (désactivation au bout de 15 mois d'inactivité, puis suppression 12 mois après).

Déploiement partiel du MFA.

## CONSÉQUENCES POTENTIELLES (IMPACTS SUR LES DONNÉES)

### EN CAS DE PERTE DE CONFIDENTIALITÉ

| | |
|---|---|
| Les données ont été diffusées plus que nécessaire et ont échappé à la maîtrise des personnes concernées | ☒ |
| Les données peuvent être corrélées avec d'autres informations relatives aux personnes concernées | ☑ |
| Les données peuvent être exploitées à d'autres fins que celles prévues et/ou de manière non loyale | ☑ |
| Autre | ☒ |

**Autres conséquences liées à la perte de confidentialité**

-

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

## PRÉJUDICES POTENTIELS POUR LES PERSONNES CONCERNÉES

### NATURE DES IMPACTS POTENTIELS POUR LES PERSONNES

| | |
|---|---|
| Perte de contrôle sur leurs données personnelles | ☒ |
| Limitation de leurs droits | ☒ |
| Discrimination | ☒ |
| Vol d'identité | ☒ |
| Fraude | ☒ |
| Levée non autorisée de pseudonymisation | ☒ |
| Pertes financières | ☒ |
| Atteinte à la réputation | ☒ |
| Perte de la confidentialité de données protégées par un secret professionnel | ☑ |
| Autre (merci de préciser) | ☒ |

**Autres impacts**

-

### ESTIMATION DU NIVEAU DE GRAVITÉ

| | |
|---|---|
| Négligeable | ☒ |
| Limité | ☑ |
| Important | ☒ |
| Maximal | ☒ |

**Mesures techniques et organisationnelles appliquées au traitement suite à la violation**

Mesures techniques
☐ Blacklist des IP fournies par le CERT Santé
☐ Recherche des IP identifiées sur les logs Firewall, Reverse proxy, connexion applicative et SSO => Réalisée au fil de l'eau
Recherche des e-mail et numéros de téléphone compromis sur l'annuaire
☐ Actions en cours chez l'éditeur Maincare :
• Mécanisme de limitation du nombre de requêtes
• Amélioration de la détection de l'usage anormal des requêtes
☐ Dans le SIEM de l'hébergeur de l'ENRS, mise en place d'une supervision, du nombre anormal de requêtes légitimes sur une faible durée et un même utilisateur / IP
• Opérationnel depuis le 08/09/2025
• La granularité de la sonde est en cours de réglage

Mesures organisationnelles
☐ Désactivation des 3 comptes compromis
☐ Durcissement des procédures création/modification/validation de comptes et information des acteurs concernés
☐ Désactivation des comptes non utilisés depuis le 01/04/2025 => Réalisée le mardi 09/09/2025 au soir
Remarque : actuellement la politique de revue de comptes prévoit une désactivation après 13 mois d'inactivité puis une suppression 12 mois plus tard
☐ Expiration des mots de passe des comptes utilisés depuis le 01/04/2025 => Réalisée le mardi 09/09/2025 au soir
☐ Généralisation de la mise en place d'une connexion à double facteur
• La connexion à double facteur était :
o En place sur l'application mobile
o En cours de déploiement sur les accès web de certains services mis à disposition par NES
o Accélération de la généralisation :
• Réalisation d'une Note d'information / Notice permettant aux utilisateurs de renseigner les modalités de contacts OTP
• Envoi de la Note d'information / Notice aux utilisateurs actifs depuis le 01/04/2025 => mercredi 10/09/2025
• Suppression des accès par simple Login / Mot de Passe : 01/10/2025

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

## COMMUNICATION AUX PERSONNES CONCERNÉES

### FOURNITURE D'UNE INFORMATION AUX PERSONNES CONCERNÉES

Oui, les personnes ont été informées ☒

Non, mais elles le seront ☒

Non ils ne le seront pas ☒

Non déterminé pour le moment ☑

## NOTIFICATIONS TRANSFRONTIÈRES ET AUTRES NOTIFICATIONS

### CETTE NOTIFICATION CONCERNE UN TRAITEMENT TRANSFRONTALIER CIBLANT DES PERSONNES DE DIFFÉRENTS ÉTATS MEMBRES

Oui ☒

Non ☑

**Pays concerné(s)**

### LA VIOLATION A OU VA ÊTRE NOTIFIÉE À UNE **AUTRE AUTORITÉ EUROPÉENNE** EN CHARGE DE LA PROTECTION DES DONNÉES ?

Oui ☒

Non ☑

**Autorité(s) concernée(s)**

### LA VIOLATION A OU VA ÊTRE NOTIFIÉE À UNE **AUTRE AUTORITÉ NON-EUROPÉENNE** EN CHARGE DE LA PROTECTION DES DONNÉES ?

Oui ☒

Non ☑

**Autorité(s) concernée(s)**

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

**NOTIFICATION N° FR2509231200002**
**DATE ET HEURE :**
**23/09/2025 À 11H**

LA VIOLATION A OU VA ÊTRE NOTIFIÉE À UNE **AUTRE AUTORITÉ AFIN DE RESPECTER UNE AUTRE EXIGENCE LÉGALE (NIS, EIDAS, ETC.) ?**

Oui ☒

Non ☑

**Autorité(s) concernée(s)**