Compte-rendu de réunion du 17/09/2025

Ordre du jour / objet du document :	Date : 19/09/2025 Date diffusion : 22/09/2025
Violation de données GRADeS	
Émetteur : GCS NeS	**Destinataire(s) : DPO**

DIFFUSION RESTREINTE

Personnes présentes	
ANGOT Olivier	NeS
VALMY Théo	NeS
CHEVALIER Emmanuel	NeS
SAMARCQ Nicolas	LEXAGONE (DPO NeS)
GUICHET Hélène	ARS Normandie
LEGARDIEN Emilie	GHT Collines de Normandie
DENIS Marlene	CH Le Havre
PIGEON Guillaume	Fondation Bon Sauveur 50
TISON Sandrine	CRLCC Henri BECQUEREL
MILLORIT Florence	CH Eure-Seine
PRETERRE Séverine	CHU Rouen
PROVENDIER Bertrand	CH Avranches-Granville
JOLIVALDT Franck	CHU Caen
DUBOIS Brice	CRLCC Francois BACLESSE
LECAT Christophe	CHICAM
LOUVET Morgane	GHT Caux-Maritime
BOUTEL Jeremy	GHT Val de Seine et Plateaux de l'Eure
Personnes absentes ou excusées	
FENIOU Florence	OCD

1. Rappel du contexte (Note 11/09/2025)

Les GRADeS ont été contactés par le CERT Santé vendredi 29 Août 2025 après 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".

Cette liste d'IP a été transmise aux GRADeS afin de confirmer des potentiels accès.

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.

Normand'e-santé a réalisé une déclaration au CERT Santé, à la CNIL et une plainte a été déposée auprès du service compétent.

La déclaration initiale CNIL porte le n° FR2509011600006, elle a été réalisée le 01/09/2025 à 16h.

NeS s'est mis en contact direct avec la CNIL et leur a indiqué, que suite aux premières investigations, il s'avérait que la violation impactait les données administratives de nombreux patients.

La déclaration sera donc actualisée dès qu'un état des lieux complet et stabilisé aura été fait.

NeS a proposé une réunion d'information le 17/09/2025, avec l'ensemble des DPO/RSSI et DSI des établissements concernés.

2. Réunion du 17/09/2025

2.1. Rappel concernant les violations et leur périmètre (note du 11/09/2025)

Rappel des dates de violations : 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.

Rappel technique des modalités de ces violations (à partir de comptes de professionnels de santé compromis (vol mot de passe et identifiant).

Dans la note d'information du 11/09/2025, un premier tableau de répartition a été fourni par le GRADeS, récapitulant le nombre total d'identités compromises identifiées : 163 813 identités sur environ 420 000, dont 4 044 identifiées comme « patients décédés » et 514 identités de test + un test « Patients décédé ».

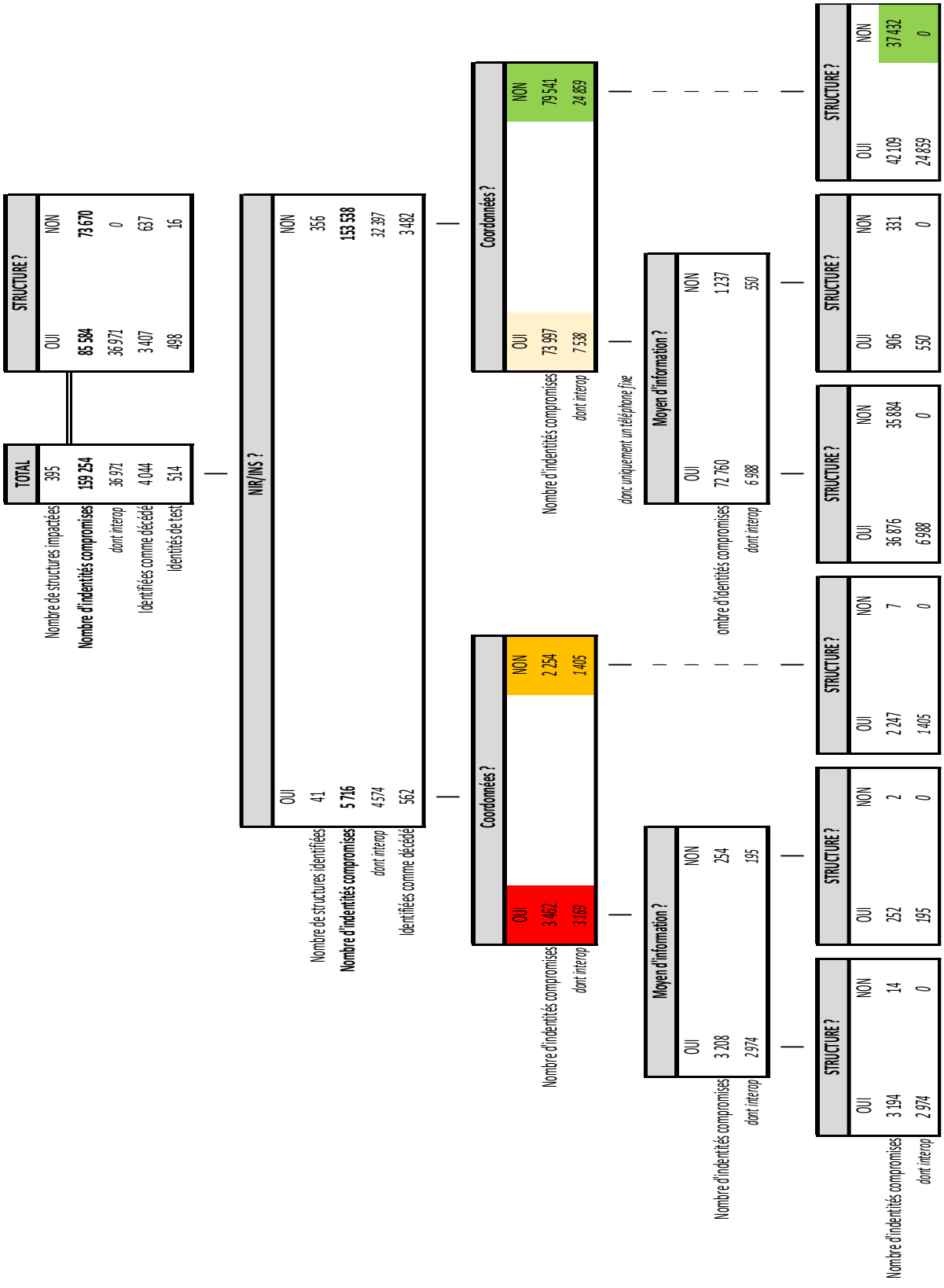
Sur les 159 254 identités (Hors patients décédés et identités de test), était précisé le pourcentage d'identités concernées pour chaque type de données :

Donnée	Nombre	%
Nom de naissance	146 415	91,94%
Nom d'usage	76 790	48,22%
Prénom	159 094	99,90%
Sexe	159 171	99,95%
Date de naissance	159 254	100,00%
Ville de naissance	21 073	13,23%
NIR ou INS	5 716	3,59%
Présence de coordonnées	77 459	48,64%
Informable	75 968	47,70%

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

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

En ce qui concerne la Normandie, pas de données de santé compromises à date.



2.2. Responsabilités

NeS est responsable de traitement seulement en ce qui concerne l'exploitation, c'est-à-dire la mise en œuvre, la conception, l'ergonomie et le déploiement des Services de l'ENRS.

Les Structures adhérentes demeurent responsables des traitements de données à caractère personnel qu'elles réalisent et notamment les traitements des données liées à la prise en charge de leur patient.

Toutefois, selon les modes organisationnels de certains Services de l'ENRS, NeS peut se trouver en situation de responsabilité conjointe de traitement au sens de la Règlementation. Dans ce cas une convention distincte sera alors signée entre les Parties concernées.

Autrement dit, à défaut de convention distincte, les utilisateurs des Services de l'ENRS sont RT au sens de la règlementation, en tant que sous-traitant, NeS met tout en œuvre pour informer au mieux chaque structure impactée sur les patients et les données concernées par la violation.

En outre, au-delà de ses obligations strictement réglementaire, NeS apportera, dans la mesure du possible, l'assistance nécessaire à ses adhérents impactés, en vue de gérer au mieux cette crise.

2.3. Sujets échangés pendant la réunion

2.3.1. Transmission de l'information

La majorité des DPO présents ont relevé qu'ils n'avaient eu l'information concernant la violation de données que par voie de presse.

C'est lors de ces remontées que M. ANGOT a pu détailler les contraintes de recoupement des données en vue d'identifier qui contacter pour notifier la violation (cf. §2.2.2), ainsi que la possibilité d'intégrer les DPO au réseau existant des RSSI/SI.

En effet, l'alerte initiale (vendredi 29/08/2025) ne permettait pas encore d'identifier l'important volume de données concernées.

Ce n'est que le mardi 02/09/2025, suite à des investigations de l'éditeur MAINCARE DOCAPOST, en lien avec le GRADeS, que l'important volume de données concernées s'est précisé.

Une première information a été partagée le jeudi 04/09 pendant le comité technique des DSI. Une seconde information a été faite le soir, par mail du DGARS, aux Directeurs des ETS sanitaires. En fin de semaine, des échanges ont eu lieu avec les autres régions sur les différents impacts et les modalités de réponse régionales.

La communication officielle a été faite le lundi 08/09/2025.

2.3.2. Recoupement des données

Suite à un important travail de tri effectué par NeS du volume d'information recueilli, M. ANGOT a présenté un état des lieux provisoire de la situation permettant une première vision affinée « par établissement ».

Les structures les plus impactées sont les CHU de Caen et Rouen.

M. ANGOT a évoqué les contraintes et le temps nécessaire au recoupement efficace des données afin d'identifier, quand cela est possible, les personnes concernées, établissement par établissement, avec la granularité par type de données évoqué plus haut.

Cela aux fins :

- D'identifier les Responsables ou Co-Responsables de traitement concernés,
- D'informer les établissements concernés avec des informations précises
- De valider, en accord avec l'ARS, la stratégie régionale d'information des patients concernés.

Du travail restait encore à faire, au moment de la réunion, considérant que certains patients ne sont pas rattachés à un établissement, mais également pour identifier, avant toute prise de contact, les identités concernant des personnes décédées.

Un fichier anonymisé de répartition des identités par structure sera fournit aux structures.

Le mécanisme d'affectation d'une identité à une structure est le suivant :

- Dans le cas d'une identité crée par un flux d'interopérabilité, l'identité est affectée à l'établissement émetteur du flux.
- Dans les autres cas, le flux est, quand c'est possible, affecté au dernier lieu d'exercice du créateur de l'identité. **Limite de cette affection, en cas de changement de lieu d'exercice depuis la date de création de cette identité, l'affectation ne correspond pas à la structure créatrice de l'identité.**

2.3.3. Déclaration CNIL

Le DPO du GRADeS a procédé dans les délais impartis (72h maxi après la connaissance de la violation) à la déclaration CNIL.

Une réunion entre NeS et les services de la CNIL s'est tenue le vendredi 12/09/2025, afin d'évoquer la possibilité d'effectuer une notification de violation unique pour l'ensemble de ses membres et utilisateurs impactés afin de faciliter les démarches auprès de leurs services et ainsi obtenir une meilleure cartographie de la situation.

Pour des raisons de conformité RGPD et de bon traitement de chaque dossier, la CNIL a indiqué que, malgré les contraintes, pour les structures impactées comme pour ses propres services, chaque Responsable de Traitement doit procéder à sa propre déclaration.

Par conséquent, NeS et les services de la CNIL ont validé le principe, pour chaque établissement concerné, d'une déclaration CNIL « hors délai », faisant explicitement référence au numéro d'enregistrement de la déclaration initiale du GRADeS.

Cela afin de tenir compte des délais de recoupement des données de log, pour déterminer, par structure, les taux d'exhaustivité des données compromises, et fournir aux différentes structures le nombre d'identités, qui les concerne et le taux de complétude des différents items subtilisés.

2.3.4. Relevé de décisions

Il a été convenu que le DPO du GRADeS allait fournir un modèle de :

- Notification à destination des établissements afin de faciliter et uniformiser les déclarations CNIL de ces derniers.
- D'information patient

NeS s'engage également à fournir dans les plus brefs délais :

- La note d'information / Point de situation actualisée
- Le fichier anonymisé de répartition des identités par structure

Chaque responsable de traitement doit procéder à une déclaration CNIL.

Chaque responsable de traitement doit procéder à une communication adaptée auprès des patients dont le NIR/NIS a été piraté dès réception des fichiers EXCEL du GRADeS.

Pour mettre en place les mesures d'information appropriées, l'Identification des risques et l'évaluation de leur vraisemblance et de leur gravité sont laissées à l'appréciation de chaque direction d'établissement.

Pour faciliter l'information des patients, NeS mettra à disposition des structures l'ensemble des informations disponibles (Mail, Téléphone, IPP local …).

NeS va également évaluer la possibilité d'usage de son CRM pour « industrialiser » les mécanismes d'information.

Comme DPO ARS, Hélène GUICHET a précisé les points suivants :

- Pas de pertinence, à ce stade, de la mise en place d'un numéro vert ;
- Accord pour relire les propositions de communication ciblée du DPO du GRADeS (proposition de modèle pour les établissements) ;
- Rappel des missions du pôle E-santé d'accompagner, notamment, les établissements dans la prévention de ces cyber attaques.