Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/25/258

DÉLIBÉRATION N° 25/126 DU 1ER JUILLET 2025 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ ENTRE LES PRESTATAIRES DE SOINS, LES INSTITUTIONS DE SOINS RÉGIONALES ET LES ORGANISMES ASSUREURS, VIA LA PLATEFORME NIPPIN DU COLLÈGE INTERMUTUALISTE NATIONAL, DANS LE CADRE DU PROJET E-AGREEMENT

Vu le règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, en particulier l'article 42, § 2, 3°, modifié par la loi du 5 septembre 2018 ;

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment les articles 5 et 15 ;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth* ;

Vu la demande d'autorisation du Collège Intermutualiste National ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 20 juin 2025 ;

Vu le rapport de monsieur Michel Deneyer ;

Émet, après délibération, la décision suivante, le 1er juillet 2025 :

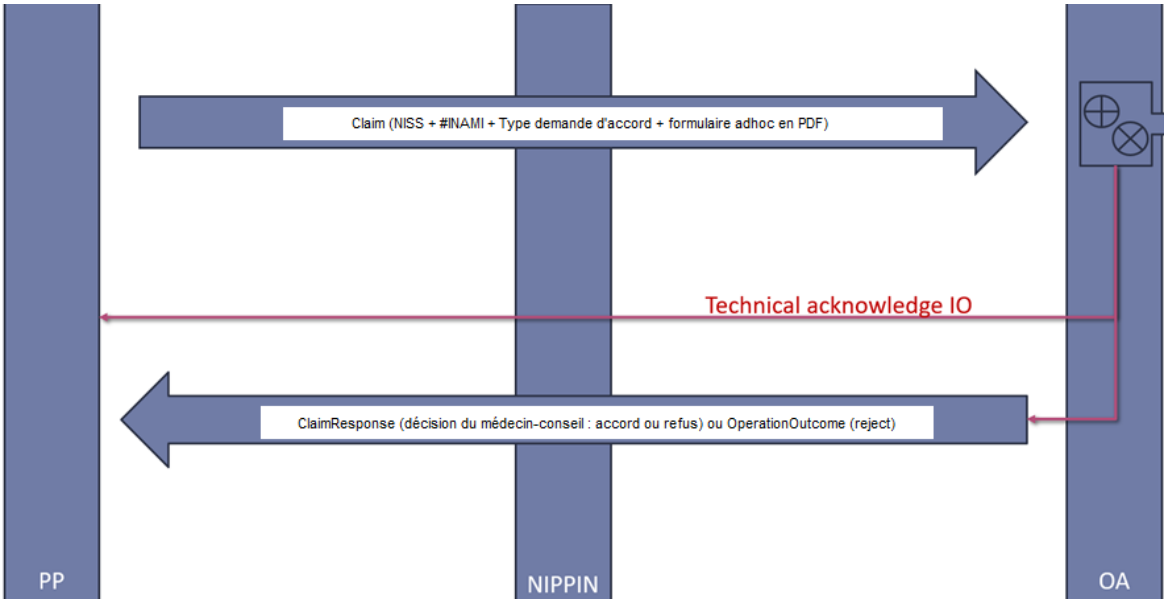
I. OBJET DE LA DEMANDE

1. Le Collège intermutualiste national a introduit une demande relative à la partie fédérale du projet eAgreement, un projet visant à digitaliser l'admission des personnes concernées au sein de certaines institutions de soins régionales. Les spécificités de chaque flux régional sont traitées dans une délibération *ad hoc*.

2. Au niveau fédéral, les personnes concernées sont tous les patients parmi la population belge en ordre d'assurabilité concernées par une demande d'admission dans une institution de soins régionale.

3. Les données à caractère personnel relatives à la santé sont communiquées au Collège intermutualiste national par les 7 organismes assureurs (Alliance nationale des mutualités chrétiennes, Union nationale des mutualités neutres, Union nationale des mutualités socialistes, Union nationale des Mutualités Libérales, Union nationale des mutualités libres, Caisse auxiliaire d'assurance maladie-invalidité) et la Caisse des soins de santé de HR Rail.

4. Les échanges de données sont réalisés via la plateforme NIPPIN du Collège Intermutualiste National.



NB : PP = Prestataire/institution de soins
NIPPIN = plateforme du CIN

5. Le projet eAgreement Light se déroulera en deux phases :
Phase 1 (en cours)
- Le message aller est structuré : le prestataire de soins envoie une demande via la plateforme NIPPIN vers les organismes assureurs.
- Le message retour, en revanche, se fait via courrier papier.

Phase 2 (prévue pour fin 2026)
- Le principe du message aller reste identique.

- Le message retour deviendra structuré et sera transmis électroniquement.

Bien que le message soit structuré, son contenu ne l'est pas nécessairement. Il contient, par exemple, un PDF reprenant la demande d'accord destinée au médecin-conseil.

II. COMPÉTENCE

6. En vertu de l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, la chambre sécurité sociale et santé du Comité de sécurité de l'information est en principe compétente pour l'octroi d'une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé.

7. La chambre sécurité sociale et santé du Comité de sécurité de l'information s'estime dès lors compétente pour se prononcer sur la présente demande.

III. EXAMEN

A. ADMISSIBILITÉ

8. En vertu de l'article 9, 1er du RGPD, le traitement de données à caractère personnel relatives à la santé est interdit.

9. Néanmoins, cette interdiction n'est pas d'application lorsque le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 (art. 9, §2, h) du RGPD).

10. L'article 53, § 1er de la loi *relative à l'assurance obligatoire soins de santé et indemnités coordonnée le 14 juillet 1994* prévoit que les dispensateurs de soins dont les prestations donnent lieu à une intervention de l'assurance sont tenus de remettre aux bénéficiaires ou, dans le cadre du régime du tiers payant, aux organismes assureurs, une attestation de soins ou de fournitures ou un document équivalent dont le modèle est arrêté par le Comité de l'assurance, où figure la mention des prestations effectuées; pour les prestations reprises à la nomenclature visée à l'article 35, § 1er, cette mention est indiquée par le numéro d'ordre à ladite nomenclature (ou de la manière déterminée dans un règlement pris par le Comité de l'assurance sur la proposition du Conseil technique compétent en fonction de la nature des prestations). Que le dispensateur de soins effectue les prestations pour son propre compte ou pour compte d'autrui, le montant payé par le bénéficiaire au dispensateur de soins pour les prestations effectuées est mentionné sur la partie reçu de l'attestation de soins donnés ou de fournitures ou sur le document équivalent.

11. A la lumière de ce qui précède, le comité de sécurité de l'information est par conséquent d'avis qu'il existe un fondement admissible pour le traitement des données à caractère personnel pseudonymisées relatives à la santé envisagé.

B. PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

1. FINALITÉ

12. Selon l'article 5 du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

13. Dans le chef des prestataires et institutions de soins, le traitement a pour but de permettre aux prestataires et institutions de soins d'envoyer leurs demandes d'accord aux médecins-conseils des Organismes Assureurs.

14. Dans le chef des Organismes Assureurs, le traitement a pour but d'évaluer la demande en la validant ou la refusant sur base des règles de l'INAMI (et des règles de nomenclature…)

15. Au vu des objectifs du traitement tels que décrits ci-dessus, le Comité de sécurité de l'information considère que le traitement des données à caractère personnel envisagé poursuit bien des finalités déterminées, explicites et légitimes.

2. PROPORTIONNALITÉ

16. L'article 5, §1er du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).

17. Les **données d'identification** le NISS de la personne concernée, le numéro d'affiliation à un organisme assureur, le numéro INAMI du prestataire de soins ou de l'institution de soins régionale concernée.

18. Les données a caractère personnel relatives à la santé contenues dans les formulaires d'admission spécifiques.

3. LIMITATION DE LA CONSERVATION

19. Conformément à l'article 5, e) du RGPD, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public,

à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, §1er, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation).

20. Les délais de conservation que les OA doivent respecter leur sont imposés par l'INAMI. La dernière circulaire en la matière est la circulaire n° 2024/269, intitulée : "Liste des pièces, documents ou données qui doivent être conservés par les organismes assureurs conformément aux délais ou conditions prescrits par la loi coordonnée du 14 juillet 1994 relative à l'assurance obligatoire soins de santé et indemnités et ses arrêtés d'exécution, en application de l'article 329bis de l'arrêté royal du 3 juillet 1996."

21. Conformément à l'article 329bis de l'arrêté royal du 3 juillet 1996, et après avis de la Commission technique, c'est le Service du contrôle administratif qui établit cette liste des pièces, documents ou données à conserver par les OA, en fonction des délais et conditions fixés par la législation précitée. La durée de conservation applicable est actuellement fixée à 3 ans.

22. Le CIN, via la plateforme NIPPIN, n'a pas accès au contenu des transactions. Le CIN ne conserve que les données de routage.

4. TRANSPARENCE

23. Conformément à l'article 12 du RGPD, le responsable du traitement doit prendre des mesures appropriées pour fournir toute information en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique.

24. Conformément à l'article 14, 5°, c) du RGPD, le responsable du traitement ne doit pas informer la personne concernée lorsque l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée. In casu, cette collecte est prévue par l'article 53, § 1er de la loi *relative à l'assurance obligatoire soins de santé et indemnités coordonnée le 14 juillet 1994.*

25. Le Comité de sécurité de l'information est d'avis qu'il existe suffisamment de transparence quant au traitement envisagé.

5. MESURES DE SÉCURITÉ

26. Selon l'article 5, §1er, f) du RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

27. Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est tenu de prendre des mesures dans les onze domaines d'action suivants liés à la sécurité de l'information: politique de sécurité; désignation d'un conseiller en sécurité de l'information; organisation et aspects humains de la sécurité (engagement de confidentialité du personnel, information et formations régulières du personnel sur le thème de la protection de la vie privée et sur les règles de sécurité); sécurité physique et de l'environnement; sécurisation des réseaux; sécurisation logique des accès et des réseaux; journalisation, traçage et analyse des accès; surveillance, revue et maintenance; système de gestion des incidents de sécurité et de la continuité (systèmes de tolérance de panne, de sauvegarde, …); documentation

28. Le Comité rappelle que les données à caractère personnel doivent être traitées sous la responsabilité d'un professionnel des soins de santé, de préférence un médecin.

29. Le Comité rappelle que selon la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, les instances connectées au réseau doivent s'assurer que les données pertinentes soient échangées directement entre elles. Les instances doivent également s'entendre afin que les assurés sociaux disposent de services intégrés connectés à des sources authentiques.

30. Le Comité rappelle qu'une analyse d'impact relative à la protection des données doit être réalisée selon les dispositions de l'article 35 du RGPD.

31. Le Comité estime, pour des raisons de sécurité, que l'ensemble du processus devra être digitalisé pour le 31 décembre 2026. Les instances concernées devront soumettre un processus informatisé complet pour cette date. Par conséquent, le Comité limite la validité de cette délibération au 31 décembre 2026.

32. La chambre sécurité sociale et santé rappelle qu'en vertu de l'article 9 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, le responsable du traitement prend les mesures supplémentaires suivantes lors du traitement de données génétiques, biométriques ou des données concernant)la santé :

1° les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information,

conclut que

la communication des données à caractère personnel telle que décrite dans la présente délibération est autorisée moyennant le respect des mesures de protection de la vie privée qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

La présente délibération entre en vigueur le 16 juillet 2025.

Le présente délibération est valable jusqu'au 31 décembre 2026.

Michel DENEYER
Président