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

CSI/CSSS/26/210

DÉLIBÉRATION N° 25/126 DU 1ER JUILLET 2025, MODIFIÉE LE 6 OCTOBRE 2026, 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 l'article 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 et du 15 septembre 2026 ;

Vu le rapport de monsieur Michel Deneyer ;

Émet, après délibération, la décision suivante, le 6 octobre 2026 :

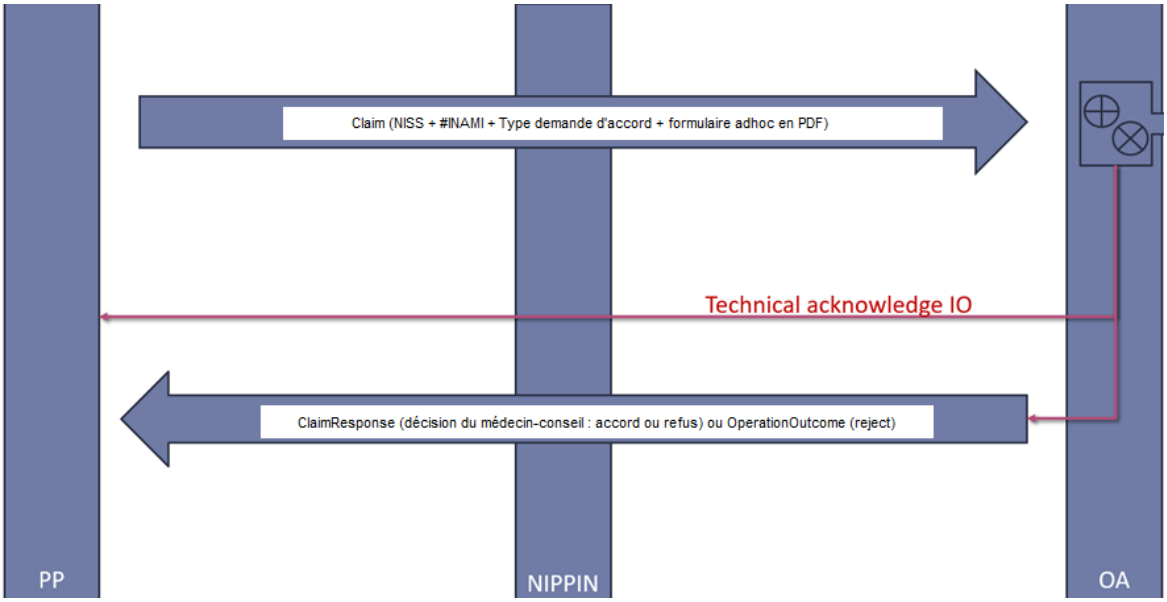
I. OBJET DE LA DEMANDE

1. Le Collège intermutualiste national a introduit en juin 2025 une demande relative à la partie fédérale de la phase 1 du projet eAgreement Light, ayant pour objectif de digitaliser les demandes d'accords de prestataires de soins adressés aux médecins-conseils des Organismes Assureurs. En mai 2026, le CIN a introduit une demande de modification de la délibération du 1er juillet 2025, en vue de définir les phase 2 et 3 du projet eAgreement.

2. Au niveau fédéral, les personnes concernées sont tous les patients parmi la population belge en ordre d'assurabilité concernés par une demande d'accord aux médecins-conseils des Organismes Assureurs.

3. Les prestataires de soins concernés par la phase 1 sont les hôpitaux, les médecins et les dentistes. Lors de la phase 2 & 3, d'autres secteurs de soins pourront utiliser le service eAgreement Light.

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 déroule en 3 phases :

A. Phase 1 (en cours) :

1. A l'aller, les données reprises dans le flux sont :
   a) des données structurées à caractère personnel relatives à l'identification du patient: nom, prénom et le numéro d'identification de la sécurité sociale (NISS) ainsi que type de document envoyé

b) des données à caractère personnel relatives à la santé de l'affilié. Ces données sont reprises dans un seul PDF. Ce PDF peut comporter plusieurs documents. Pour les documents qui nécessitent une signature d'un prestataire de soins et/ou d'un patient, il existe différentes possibilités de les signer.

I. *Scan du document* : le document est imprimé et complété par le prestataire de soins et/ou le patient qui le signe manuscritement. Chacune des parties mentionne son nom, prénom et n°INAMI (si c'est un prestataire de soins). Ensuite, il est scanné, transformé en PDF et encapsulé dans un message FHIR eAgreement light qui est transmis via le certificat eHealth de l'institution à la plate-forme MyCareNet. L'OA doit vérifier la présence d'une signature manuscrite du prestataire de soins et/Lu du patient, comme cela se fait déjà aujourd'hui par courrier postal. Dans le cas où le document doit être signé manuscritement par le patient, le prestataire de soins est tenu de garder l'original en cas de contrôle ou de demande d'une autorité.

II. *L'utilisation de la SDQ (Signature Digitale Qualifiée)*: l'OA doit vérifier qu'il existe effectivement une SDQ valable sur la partie du document qui concerne le prestataire de soin et/ou le patient.

2. Au retour : L'OA répond uniquement par voie postale à l'émetteur de la demande.

B. Phase 2 (prévue pour fin Q1 2027) :

a. A l'aller : le principe d'envoi du message reste identique à la phase 1.

b. Le retour se fait de manière électronique :

i. L'enveloppe du message est structurée : l'OA envoie sa réponse (décision du médecin-conseil) via la plateforme NIPPIN vers le prestataire à l'origine de la demande.

ii. Les données reprises dans le flux sont :

1. des données à caractère personnel relatives à l'identification des patients : nom, prénom et n° NISS.

2. Des données à caractère personnel relatives à la santé de l'affilié :

- La décision (accord ou refus) du médecin-conseil
- Tout le reste : inséré dans des documents en format PDF où figurera la signature manuscrite scannée du médecin-conseil ainsi que son nom, prénom et n° INAMI. Ce PDF est encapsulé dans un message FHIR eAgreement light qui est transmis avec le certificat eHealth de l'OA à l'émetteur de la demande via la plate-forme MyCareNet.

Les prestataires de soins concernés par cette deuxième phase sont essentiellement les hôpitaux, les médecins et les dentistes.

C. Phase 3 (prévue pour 2028) – « eAgreement generic » :

1. A l'aller : le principe du message reste identique aux précédentes phases mais le dataset sera enrichi avec des informations permettant plus d'automatisation (ex : référence OA d'un accord, date de début souhaitée pour un traitement,…).
2. Au retour : le principe du message retour reste identique à la phase 2 mais là aussi, le dataset sera enrichi avec de nouveaux codes décision (demande d'information complémentaire du médecin-conseil,…) et des dates de début et fin autorisées par exemple.
3. Par ailleurs, l'orchestration des échanges ne se limitera plus à un aller/retour puisque d'autres cas seront prévus :
    - Permettre à un prestataire d'annuler sa demande en cas d'erreur,
    - Permettre au médecin-conseil, afin de traiter la demande d'accord, de demander des informations complémentaires au prestataire de soins et permettre au prestataire de soins de lui répondre directement,
    - Permettre au prestataire de transmettre proactivement des compléments d'information opportuns pour une demande,
    - Permettre au prestataire de demander la prolongation d'un accord existant,
    - Permettre au prestataire ou au médecin-conseil de clôturer anticipativement un accord pour des situations spécifiques,
    - …

6. Liste des documents qui sont échangés : L'INAMI détermine pour chaque secteur les documents standards à échanger entre le prestataire de soins et les Organismes Assureurs. Chaque secteur peut avoir plusieurs type de documents à échanger. Vu la volonté des autorités de simplifier ces documents, ils sont susceptibles d'évoluer dans le temps. Voici une liste non-exhaustive de documents qui sont échangés :

Formulaires de demandes de revalidation :

a. 7.81.5 - Affections respiratoires chroniques graves
b. 7.81.x - Oxygénothérapie de longue durée à domicile
c. 7.82.1 - Rééducation cardiaque
d. 7.82.5 - Accompagnement en cas de grossesse non-désirée
e. 7.83.1 - Décès inopiné et inexpliqué d'un enfant de moins de 18 mois
f. 7.83.5 - Monitoring mort subite

g. 7.83.6 - Enfants nés prématurément

h. 7.84.5 - Rééducation neuropsy pédiatrique

i. 7.85.2 - Assistance ventilatoire à domicile

j. 7.85.3 - Assistance ventilatoire à domicile - syndrome d'obésité-hypoventilation

Rapport médical de Consultation Oncologique Multidisciplinaire

Formulaires pour pose d'implants

Formulaire de notification vêtements compressifs

Rapport de motivation orthèse d'assise sur mesure

….

Cette troisième phase a également pour but de permettre à toutes les autres institutions/prestataires de soins qui sont sous l'autorité de l'INAMI d'utiliser ce service digital leur permettant de transmettre leurs demandes d'accords aux médecins-conseils des Organismes Assureurs Fédéraux afin de se conformer à la loi-cadre sur la digitalisation des secteurs des soins de santé (Loi-cadre II (cf. DOC 56 1335/007) approuvée au Parlement en en séance plénière du **13 mai 2026** et celui de la Loi-cadre I (cf. DOC 56 1334/010) en séance plénière du **21 mai 2026**).

7. Le Comité constate que le but de cette demande est de proposer un processus digital sécurisé pour les documents signés manuscritement lorsque la signature électronique qualifiée ne peut pas être utilisée. La demande ne vise pas la création d'une nouvelle signature électronique qualifiée. Il s'agit entre autres des documents que le dispensateur de soins doit envoyer au médecin-conseil de l'organisme assureur pour demander un accord de remboursement par l'assurance maladie obligatoire d'une prestation de soins/d'un traitement.

8. Le Comité constate qu'un avant-projet de loi portant des dispositions diverses en matière de santé, qui établit une base légale du présent processus, est en cours d'élaboration. Par conséquent, le Comité se prononce, à ce stade, sous réserve de la publication au Moniteur belge et de l'entrée en vigueur de ce projet de loi. Le cas échéant, le processus sera à nouveau soumis au Comité de sécurité de l'information pour prendre en compte les dispositions législatives définitives.

II. COMPÉTENCE

9. 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.

10. 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

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

12. 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).

13. 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.

14. 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.

15. Le Comité constate qu'un avant-projet de loi portant des dispositions diverses en matière de santé qui prévoit la base réglementaire et les effets juridiques de ce processus est en cours d'élaboration. Par conséquent, le Comité se prononce sous réserve de la publication de ce projet de loi au Moniteur belge et de son entrée en vigueur.

B. PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

1. FINALITÉ

16. 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.

17. 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.

18. 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…)

19. 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

20. 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).

21. 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.

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

3. LIMITATION DE LA CONSERVATION

23. 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).

24. 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."

25. 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.

26. 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

27. 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.

28. 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.*

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

5. MESURES DE SÉCURITÉ

30. 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).

31. 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

32. 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.

33. 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.

34. 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.

35. Le Comité constate qu'un avant-projet de loi portant des dispositions diverses en matière de santé est en cours d'élaboration. Par conséquent, le Comité se prononce sous réserve de la publication de ce projet de loi au Moniteur belge et de son entrée en vigueur. Le cas échéant, le processus sera à nouveau soumis au Comité de sécurité de l'information pour prendre en compte les dispositions législatives définitives.

36. Afin de garantir un processus digitalisé efficient et de qualité, le Comité insiste sur le respect du délai d'implémentation des phases 2 et 3. Le Comité incite les institutions concernées à mettre en œuvre la phase 2 pour le 31 mars 2027 et la phase 3 pour le 31 décembre 2028. Le Comité prend note que le projet de loi-cadre prévoit que la digitalisation devra être généralisée au 1er janvier 2030.

37. 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.

Les modifications de cette délibération, approuvées par le comité de sécurité de l'information le 6 octobre 2026, entrent en vigueur 21 octobre 2026.

Michel DENEYER
Président