Comité de sécurité de l'information

Chambre sécurité sociale et santé

CSI/CSSS/26/032

DÉLIBÉRATION N° 26/016 DU 13 JANVIER 2026 RELATIVE AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES RELATIVES À LA SANTÉ PAR LES ORGANISMES ASSUREURS, LE COLLÈGE INTERMUTUALISTE NATIONAL ET L'INAMI DANS LE CADRE DE LA LOI EXÉCUTANT UNE POLITIQUE RENFORCÉE DE RETOUR AU TRAVAIL EN CAS D'INCAPACITÉ DE TRAVAIL (BASE DE DONNÉES GAOCIT)

La chambre sécurité sociale et santé du Comité de sécurité de l'information (dénommé ci-après "le Comité") ;

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 relatif à la protection des données ou RGPD);

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 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 13 décembre 2006 *portant dispositions diverses en matière de santé*, en particulier l'article 42, § 2, 3° ;

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

Vu la loi du 19 décembre 2025 *exécutant une politique renforcée de retour au travail en cas d'incapacité de travail* ;

Vu la demande de l'INAMI ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 2 janvier 2026 ;

Vu le rapport de monsieur Michel Deneyer ;

Émet, après délibération, la décision suivante, le 13 janvier 2026 :

I. OBJET DE LA DEMANDE

1. Au cours de cette législature, le gouvernement souhaite élaborer un plan global pour la prévention et la réinsertion des malades de longue durée. Le fondement de ce vaste plan consiste à responsabiliser davantage les différents acteurs concernés.

2. Les personnes concernées sont les bénéficiaires du droit aux indemnités mentionnés à l'article 86, § 1er, de la loi *relative à l'assurance obligatoire soins de santé et indemnités*, coordonnée le 14 juillet 1994 et à l'article 3 de l'arrêté royal du 20 juillet 1971 *instituant une assurance indemnités et une assurance maternité en faveur des travailleurs indépendants et des conjoints aidants* et pour lesquels les médecins traitants établissent un certificat d'incapacité de travail par voie électronique à destination du médecin-conseil de la mutualité. Les certificats d'incapacité de travail sont transmis par voie électronique par les médecins traitants via leur logiciel à destination du médecin-conseil de la mutualité, pour les bénéficiaires susvisés, via le projet « Mult-eMediatt » itération 1.

3. Dans le cadre des articles 13 et 14 de la loi du 19 décembre 2025 *exécutant une politique renforcée de retour au travail en cas d'incapacité de travail*, il est prévu de créer, au sein de l'INAMI, une base de données pseudonymisées "GAOCIT" à partir de laquelle les analyses, suivis, rapportages et datamining pourront être réalisés[1]. La création de cette base de données nécessite l'utilisation du service SEALS de la plate-forme eHealth.

4. A terme, cette base de données GAOCIT contiendra les données pseudonymisées suivantes :

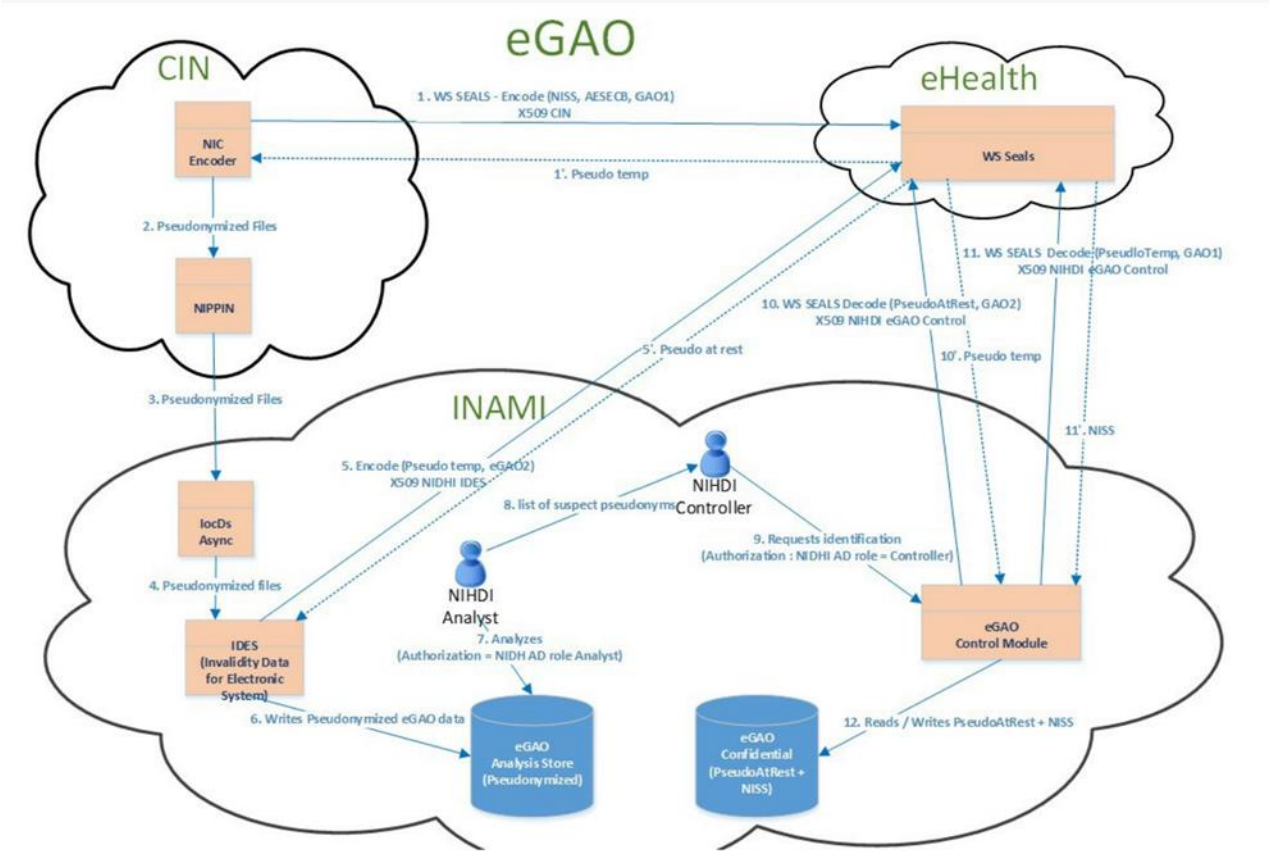
- les informations d'identification pseudonymisées du bénéficiaire du droit aux indemnités (le NISS - numéro d'identification visé à l'article 8 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale*) ;
- les informations d'identification du médecin traitant concerné (le NISS ou le numéro INAMI) ;
- la date de début et la date de fin de la période d'incapacité de travail ;
- un diagnostic ou une pathologie codés de manière uniforme ;
- si disponible, la mention qu'il s'agit de la première déclaration d'incapacité de travail ou de la prolongation de l'incapacité de travail ;
- la date de rédaction du certificat électronique.

5. Le Collège intermutualiste national (CIN) enverra ce set de données limité à l'INAMI avec le NISS du patient pseudonymisé, l'INAMI disposera ainsi d'une base de données GAOCIT à partir de laquelle les analyses, suivis, rapportages et datamining pourront être réalisés. Cette pseudonymisation pourra être levée à la demande du Service « SIDU-SECM CONTROL » (appelé NIHDI CONTROL) dans le cadre des missions légales de contrôle médical de l'INAMI pour les dossiers individuels en fonction des constatations effectuées.

[1] Art. 13 de la loi du 19 décembre 2025 *exécutant une politique renforcée de retour au travail en cas d'incapacité de travail*, M.B., 30 décembre 2025, p. 98742.

Description schématique de l'échange de données

6. Le NISS sera communiqué par le Collège intermutualiste national (CIN) à la plate-forme eHealth via la procédure suivante :



Step 1 : Pseudonymization WS SEALS at NIC side NIC Encoder contacts eHealth to encode SSIN into a temporary pseudonym Encode for project = eGAO1 Algorithm "AESECB": This algorithm realizes a no randomized encryption. This means that each time a user encrypts a same input with the same key, he receives the same output.

Steps 2–4 : File Transfert to NIHDI NIC Encoder sends the pseudonymized file to NIPPIN ⟨NIC messaging system⟩ NIPPIN forwards the file to IOCds IOCds delivers the pseudonymized data to IDES

Step 5 : Retrieve Pseudonym at rest ⟨eGAO2⟩ IDES calls eHealth to encode the temporary pseudonym WS SEALS ENCODE ⟨pseudo temp, Algorithm "AESECB"⟩ -> returns pseudo at rest authentication = cert X509 NIHDI IDES

Steps 6 : IDES stores pseudonym at rest Tip : Right click on image(s) --> open in a new tab to view them in full screen Contact Person The pseudonym returned by eHealth is persisted in eGAO Analysis datastore ⟨pseudonym at rest⟩

Steps 7 : Analysis of pseudonymized data NIHDI Analyst accesses eGAO pseudonymized datastore in order to find suspect records

Step 8 : Communication of lists of suspect records to NHIDI Controller This action occurs outside the application ⟨Excel file⟩

Steps 9–12 : Suspicious Case Identification NIHDI Controller requests identification of pseudonyms related to a suspect record via the eGAO Control web application NIDHI Controller is authorized via NIHDI Active Directory group membership Two calls to eHealth ensue: a. WS SEALS DECODE ⟨pseudo at rest, eGAO2⟩ -> returns pseudo temp authentication = X509 cert NHIDI eGAO control b. WS SEALS DECODE ⟨pseudo temp, eGAO1⟩ -> returns NISS authentication = X509 cert “eGAO control" eGAO Control writes the SSIN with the corresponding pseudonym at rest to the Confidential Store eGAO Control reads nominative data from eGAO Confidential Store ⟨contains SSIN⟩ Access is authorized via NIHDI Active Director.

7. Par ailleurs, l’utilisateur final doit avoir la possibilité de demander la levée de la pseudonymisation du NISS du bénéficiaire du droit aux indemnités dans les situations suivantes :

Dans le cadre des finalités décrites dans la loi susmentionnée, le CIN enverra un set de données limité à l'INAMI avec le NISS du patient pseudonymisé, l'INAMI disposera ainsi d'une base de données à partir de laquelle les analyses, suivis, rapportages et datamining susvisés pourront être réalisés.

Cette pseudonymisation pourra toutefois être levée à la demande du Service « SIDU-SECM CONTROL » (appelé NIHDI CONTROL) dans le cadre des missions légales de contrôle médical de l’INAMI pour les dossiers individuels en fonction des constatations effectuées. En effet, pour l’exécution de leurs missions de contrôle dans le cadre du traitement des dossiers individuels par le Service des indemnités et le Service d'évaluation et de contrôle médicaux de l'INAMI, les médecins du Service des indemnités, membres du Conseil médical de l'invalidité et les inspecteurs sociaux du Service d'évaluation et de contrôle médicaux, peuvent avoir accès aux données dépseudonymisées.

8. Dans ce cadre, ils demandent à la plateforme eHealth d'avoir accès au numéro d'identification, visé à l'article 8 de la loi du 15 janvier 1990, dépseudonymisé en fonction des constatations effectuées par :

- les médecins du Service des indemnités, membres du Conseil médical de l'invalidité, pour les missions qui leur sont attribuées en vertu de l'article 82, alinéa 2, de la loi *relative à l’assurance obligatoire soins de santé et indemnités*, coordonnée le 14 juillet 1994 (exécuter le pouvoir de décision relatif à l'état d'incapacité de travail) ;
- les médecins-inspecteurs du Service d'évaluation et de contrôle médicaux, pour les missions qui leur sont attribuées en vertu de l'article 139, alinéa 4, de la loi coordonnée précitée du 14 juillet 1994 (entre autres chargés de contrôler les prestations de l'assurance soins de santé sur le plan de la réalité et de la conformité aux dispositions de la présente loi, de ses arrêtés et règlements d'exécution et des conventions et accords conclus en vertu de

cette même loi et d'assurer le contrôle médical des prestations de l'assurance indemnités et de l'assurance maternité).

9. Le Collège Intermutualiste des mutualités (CIN) d'une part et l'INAMI d'autre part, s'engagent :
- à ce que la dépseudonymisation du NISS du patient se fasse exclusivement avec l'intervention de la plate-forme eHealth qui exerce un rôle de tiers de confiance (TTP - Trusted Third-Party);
- à interdire toute tentative de réidentification d'un patient sur base du pseudonyme temporaire; en cas de tentative, les parties intervenantes (INAMI, CIN, mutualités) prendront les mesures nécessaires pour que toute tentative de violation de leur engagement soit sanctionnée de manière suffisamment dissuasive, et en informe le Comité de Sécurité de l'Information.

10. Selon le diagramme de contexte, le CIN ne fait pas de dépseudonymisation. Il y a 2 clefs différentes. Une clé pour pseudonymiser le NISS (ce qui est fait par la plate-forme eHealth et demandé par le CIN). Une clé pour pseudonymiser la pseudonymisation envoyée par le CIN, qui est faite par la plate-forme eHealth et demandé par l'INAMI. Ainsi l'INAMI ne connait pas le NISS (pseudonymisation par le CIN) et le CIN ne sait pas sur quelles pseudonymisations sont faites les enquêtes (pseudonymisation par l'INAMI). Pour dépseudonymiser, l'INAMI est obligée de passer par la plate-forme eHealth deux fois.

II. COMPETENCE

11. En vertu de l'article 42, § 2, 2°, 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 rendre une délibération concernant toute communication de données à caractère personnel relatives à la santé.

12. En vertu de l'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth,* toute communication de données à caractère personnel par ou à la plate-forme eHealth requiert une autorisation de principe de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

III. EXAMEN

A. ADMISSIBILITÉ

13. Selon l'article 6 du Règlement (UE) 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 (RGPD), le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions mentionnées est remplie[2].

14. Selon l'article 5 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*, la plate-forme eHealth a, notamment, pour mission de développer un système de pseudonymisation et d'anonymisation des informations. Selon l'article 7 de la loi précitée, la plate-forme eHealth a, pour l'exécution de ses missions, le droit d'utiliser le numéro d'identification du Registre national.

15. L'INAMI a été autorisé, par l'arrêté royal du 5 décembre 1986, à accéder au registre national des personnes physiques, en vue de l'accomplissement de ses missions. Les organismes assureurs déclarent être autorisés à utiliser le numéro de Registre national et à avoir accès au Registre national par l'article 1er de l'arrêté royal du 5 décembre 1986 *organisant l'accès aux informations et l'usage du numéro d'identification du Registre national des personnes physiques dans le chef d'organismes qui remplissent des missions d'intérêt général dans le cadre de la législation relative à l'assurance maladie-invalidité*.

16. Le traitement de données à caractère personnel relatives à la santé est en principe interdit, et ce conformément au prescrit de l'article 9, §1er, du Règlement (UE) 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), dénommé ci-après le RGPD.

17. 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).

18. Le Comité constate que la loi du 19 décembre 2025 *exécutant une politique renforcée de retour au travail en cas d'incapacité de travail* a été publiée au Moniteur belge le 30 décembre 2025. Les dispositions concernées entrent en vigueur le 1er janvier 2026.

B. FINALITÉ

19. Conformément à l'art. 5, b) du RGPD, le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes.

[2] Article 6, §1er, c, du RGPD, le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.

20. Telle que décrite à l'article 13, §3, de la loi du 19 décembre 2025 *exécutant une politique renforcée de retour au travail en cas d'incapacité de travail*, la finalité de la base de données pseudonymisées GAOCIT est de :

1) Disposer de suffisamment de connaissances
   - sur le nombre de cas dans lesquels une incapacité de travail est constatée par un médecin généraliste tenant compte de la taille et de la population de patients de son cabinet médical de la durée précise de l'incapacité de travail, liée au diagnostic ou à la pathologie constatée chez le patient, prescrite par ce médecin ;
   - sur le nombre de médecins généralistes qu'un assuré social consulte dans le cadre de la relation thérapeutique qu'il entretient avec ces médecins en raison de son incapacité de travail si elle donne lieu à prescription d'une période d'incapacité de travail.

2) Ces connaissances acquises doivent permettre de développer des outils d'autogestion pour les médecins, en leur permettant de comparer et d'adapter leur propre comportement de prescription avec des « normes » scientifiquement fondées et le comportement de prescription de leurs collègues dans une même région.

3) Responsabilisation financière des médecins prescripteurs quant à l'acte médical de prescription d'incapacité de travail dans le cadre de la relation thérapeutique. L'INAMI prendra appui sur la nouvelle base de données GAOCIT qui entrera en vigueur à partir du 1er janvier 2026. Cette procédure permettra ainsi de pouvoir identifier, contacter, et suivre et, le cas échéant, de sanctionner financièrement les médecins concernés. De plus, l'INAMI les incitera à ajuster leur comportement de prescription de l'incapacité de travail au travers de campagnes d'actions de sensibilisation visant à leur permettre d'adapter leur propre comportement de prescription de l'incapacité de travail. Ces médecins pourront également être tenus financièrement responsables de leur comportement de prescription, selon des modalités qui seront définies dans la réglementation INAMI.

C. PROPORTIONNALITÉ

21. Conformément à l'art. 5, b) et c) du RGPD, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

22. Toute personne concernée est identifiée par son numéro d'identification de la sécurité sociale, soit le numéro de Registre national (selon l'article 1er de l'arrêté royal du 5 décembre 1986 *organisant l'accès aux informations et l'usage du numéro d'identification du Registre national des personnes physiques*, l'INAMI est autorisée à utiliser le numéro de Registre national), soit le numéro Banque Carrefour (l'usage du numéro Banque Carrefour est libre, conformément à l'article 8, § 2, de la loi du 15 janvier *1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.

23. Le CIN enverra un set de données limité à l'INAMI avec le NISS du patient pseudonymisé, l'INAMI disposera ainsi d'une base de données à partir de laquelle les analyses, suivis, rapportages et datamining repris dans les finalités pourront être réalisés :

- les informations d'identification du bénéficiaire du droit aux indemnités (numéro d'identification visé à l'article 8 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale) et du médecin traitant concerné (numéro d'identification visé à l'article 8 de la loi précitée du 15 janvier 1990 ou le numéro INAMI) ;
- la date de début et la date de fin de la période d'incapacité de travail ;
- un diagnostic ou une pathologie codés de manière uniforme ;
- si disponible, la mention qu'il s'agit de la première déclaration d'incapacité de travail ou de la prolongation de l'incapacité de travail ;
- la date de rédaction du certificat électronique.

24. L'INAMI est le responsable du traitement des données pseudonymisées[3]. Ces données seront traitées, selon les modalités décrites à l'article 13, §4, de la loi précitée, par le Service des indemnités de l'INAMI (Médecins SIDU et data analystes), le Service d'évaluation et de contrôle médicaux de l'INAMI (Médecins inspecteurs) et le Service DataOffice de l'INAMI pour la gestion des données.

25. Conformément à l'article 5, 8°, de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la Plate-forme eHealth*, la plate-forme eHealth intervient en tant qu'organisme intermédiaire via l'utilisation du service SEALS (*voyez points 6 à 10*). La plate-forme eHealth est autorisée à conserver la clé de codage pour la durée nécessaire à l'exécution de cette mission ainsi que pour toute la durée durant laquelle la dépseudonymisation peut être demandée tel que prévu par l'article 13, §3, dernier alinéa, de la loi du 19 décembre 2025 *exécutant une politique renforcée de retour au travail en cas d'incapacité de travail*.

D. LIMITATION DE LA CONSERVATION

26. Conformément à l'article 5, §1er, 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).

27. L'article 13, §6, de la loi du 19 décembre 2025 précitée prévoit que « *les données dans la base de données GAOCIT ne sont pas conservées plus longtemps que nécessaire pour*

[3] Art. 13, §5, loi du 19 décembre 2025 *exécutant une politique renforcée de retour au travail en cas d'incapacité de travail*.

atteindre la finalité poursuivie dans le cadre de leur traitement, avec une durée maximale de conservation de cinq ans à compter du 1er janvier de l'année qui suit l'année au cours de laquelle le certificat électronique concerné a été rédigé ».

E. TRANSPARENCE

28. 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.

29. En vertu de l'article 14, §5, du RGPD, l'INAMI déclare qu'il n'est pas nécessaire d'informer la personne concernée car celle-ci dispose déjà de ces informations (il s'agit des certificats d'incapacité complétés par les médecins généralistes). De plus, 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.

F. MESURES DE SÉCURITÉ

30. Conformément à l'article 5, f) du RGPD, le demandeur doit prendre toutes les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel. Ces mesures doivent garantir un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

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 constate que l'INAMI, le CIN et la plate-forme eHealth ont désigné un délégué à la protection des données et disposent d'une politique de sécurité de l'information.

33. Le Comité rappelle que les dispositions de l'article 35 du RGPD relatives à l'analyse d'impact relative à la protection des données doivent être respectées.

34. L'INAMI, le CIN et la plate-forme eHealth déclarent que tous leurs collaborateurs sont soumis à un devoir de confidentialité. Il en va de même pour les médecins traitants qui sont tenus par le secret médical conformément à l'article 458 du Code pénal.

35. Le Comité 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 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 soustraitant;
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.

36. Le Comité attire explicitement l'attention sur les dispositions du Titre 6 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, qui prévoit des sanctions administratives et pénales sévères dans le chef du responsable du traitement et des sous-traitants pour la violation des conditions prévues dans le RGPD et la loi du 30 juillet 2018 précitée.

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 fictives 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;

autorise l'utilisation du service de base SEALS de la plate-forme eHealth selon la procédure prévue par l'article 13 de la loi du 19 décembre 2025 e*xécutant une politique renforcée de retour au travail en cas d'incapacité de travail*.

La présente délibération entre en vigueur le 14 janvier 2026.

Michel DENEYER
Président

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles.