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

CSI/CSSS/26/314

DÉLIBÉRATION N° 25/156 DU 2 SEPTEMBRE 2025, MODIFIÉE LE 6 OCTOBRE 2026, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ ENTRE LES ORGANISMES ASSUREURS WALLONS ET LES MAISONS DE REPOS, MAISONS DE REPOS ET DE SOINS, LES MAISONS DE SOINS PSYCHIATRIQUES ET LES CENTRES DE SOINS DE JOUR DANS LE CADRE DU SERVICE D'ADMISSION ELECTRONIQUE DE LEURS MEMBRES VIA WALCARENET (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 de AVIQ ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 30 juillet 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. L'Agence pour une vie de qualité, en abrégé "AVIQ", a introduit, en 2025, une demande au nom et pour le compte des institutions et des organismes assureurs wallons (OAW) en tant que régulateur dans le cadre de la phase 1 du projet eAgreement Light, ayant pour objectif de digitaliser les demandes d'accords de prestataires de soins adressées aux médecins-conseils des Organismes Assureurs Wallons (OAW).

2. Depuis la 6ème réforme de l'Etat, la Région wallonne s'est vue transférer un certain nombre de compétences dans le domaine de la santé notamment le financement des institutions de soins situées sur le territoire de la Région wallonne.

3. L'AVIQ a décidé d'implémenter le service des admissions électroniques dans les institutions (par « admissions » ou « demande d'admission », on entend l'ensemble des procédures de demandes, telles que visées aux articles 152 et suivants de l'arrêté royal du 3 juillet 1996 et introduites auprès des organismes assureurs wallons (AOW)). Ces institutions envoient à l'heure actuelle leurs formulaires de demande d'admissions sur support papier via courriel postal.

4. Suite à la constatation de plaintes récurrentes formulées par de nombreuses institutions relatives à des courriers perdus par la poste contenant les demandes d'obtention d'allocation de base et des pénalités financières engendrées par la perte de ces courriers mais aussi du décalage qui en découle entre le processus de facturation électronique plus rapide et le processus d'admission papier plus long, la mise en place de ce service permettra également de répondre à problèmes rencontrés par les institutions et les OAW sur le terrain.

5. Ce service permettra aux institutions d'envoyer leurs demandes d'admissions aux OAW de manière électronique via Walcarenet et que les OAW renvoient leur décisions aux institutions également de manière électronique via Walcarenet.

6. AVIQ a prévu trois phases dans la mise en place du service **'admissions électroniques'**:

Phase 1 (eAgreement light en cours) : envoi des documents sur support digital avec accusé de réception mais traitement des demandes et envoi des formulaires de retour (décisions) sur support papier.

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, NISS et le type de document envoyé ;

b) des données à caractère personnel relatives à la santé de l'affilié (dans l'échelle de Katz). Ces données sont reprises dans un seul document PDF. Ce document nécessite une signature d'un prestataire de soins. Il existe une seule possibilité de signer ce document.

Scan du document : le document est imprimé et complété par le prestataire de soins (médecin ou infirmière) qui le signe manuscritement. Il mentionne son nom, prénom, et son numéro INAMI si c'est un médecin. Ensuite, ce document est scanné, converti en PDF et encapsulé dans un message FHIR eAgreement light qui est transmis, via le

certificat eHealth de l'institution, à la plate-forme WalCareNet. L'organisme assureur doit vérifier la présence d'une signature manuscrite du prestataire de soins comme cela se fait aujourd'hui par courrier postal.

Au retour, l'organisme assureur répond uniquement par voie postale.

Phase 2 (prévue pour la fin du 1er trimestre 2027) :

a. A l'aller :

a.1. Le principe d'envoi du message reste identique à la phase 1.

a.2. Ajout de la possibilité de signer le document médical (échelle de Katz) avec une Signature Digitale Qualifiée (SDQ). L'OA doit vérifier qu'il existe effectivement une SDQ sur la partie du document qui concerne le prestataire de soin.

a.3. Ajout de la possibilité d'envoyer le message au moyen du login et du mot de passe de l'émetteur, sous réserve du respect des exigences de sécurité annexées**,** soit l'obtention d'un score de 100 % dans les six domaines. Le questionnaire est également disponible au format Excel ;

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 :

- des données à caractère personnel relatives à l'identification des patients : nom, prénom et n° NISS.
- - Des données à caractère médical 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 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 WalCareNet.

- **Phase 3 (prévue pour 2028) – « eAgreement generic »**.

a. 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, …).

b. 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.

c. Par ailleurs, l'orchestration des échanges ne se limitera plus à un aller/retour puisque d'autres cas seront prévus :

- Permettre à un prestataire qui s'est trompé d'annuler sa demande,
- Permettre au médecin-conseil de demander des informations complémentaires et permettre au prestataire 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.

7. La précédente demande visait également à valider la procédure selon laquelle les données relatives à la santé contenues dans les analyses médicales réalisées par un professionnel de santé (médecin ou praticien de l'art infirmier), dans le cadre de ces demandes d'admissions, seront traitées et conservées par les institutions, en application de l'article 36/1, § 1er, 1° de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*. Compte-tenu du fait que les institutions de santé n'offrent pas toutes la garantie que le professionnel de santé puisse signer de façon qualifiée les analyses médicales transmises par voie électronique aux OAW, l'AVIQ a établi la procédure suivante, qui offre les même garanties qu'une signature électronique qualifiée :
- le professionnel de santé réalise l'analyse médicale et la signe de façon manuscrite ;
- le document est ainsi scanné et joint au dossier de demande d'admission qui recevra le certificat eHealth de l'institution ;
- l'original du document est conservé par l'établissement pour le tenir à disposition des OAW et de l'AVIQ en cas de contrôle sur la validité de la signature figurant sur l'analyse médicale.

8. Cette procédure sera formalisée dans les conventions bicommunautaires conclues entre les organismes assureurs wallons et les institutions.

9. Les personnes concernées sont :

• les assurés wallons au sens de l'art. 43/2, 8° du livre IIIter du Code Wallon de l'Action Sociale et de la Santé qui sollicitent une intervention des OAW dans les matières visées à l'art.437 alinéa 1, 4° et 6° du livre IIIter du Code Wallon de l'Action Sociale et de la Santé, car c'est la demande d'admission de cette catégorie de personne qui sont traitées par les institutions ;
• les institutions ou prestataires de soins visées sont les MSP, MR, MRS et CSJ. Ce sont ces institutions qui préparent et envoient les demandes d'admission qui sont soumises aux OAW pour décision.

Les **Maisons de Repos (MR)** et les **Maisons de Repos et de soins (MR.S)** sont désormais soumises à l'obligation d'hébergement de personnes âgées de 70 ans et plus. Les établissements peuvent faire rentrer toutes les personnes âgées de moins de 70 ans sans distinction ni sans demande de dérogation. Il leur appartiendra le 01/01/2029, de comptabiliser le pourcentage de résidents âgées de moins de 70 ans au sein de leur établissement. S'ils sont en dessous de 10%, ils pourront continuer à accueillir des personnes âgées de moins de 70 ans sans demande de dérogation. S'ils sont au-dessus de 10% ou quand ils arriveront à 10%, pour le suivant, ils pourront continuer à accueillir des personnes âgées de moins de 70 ans avec demande de dérogation. Donc, les 10% ne seront plus, à partir du 01/01/2029, un plafond de refus mais un plancher d'obligation de demande de dérogation. Certaines maisons de repos possèdent un agrément spécial en tant que **Maisons de Repos et de Soins (MR.S)** pour la prise en charge de personnes âgées fortement dépendantes et nécessitant des soins adaptés. Il y a 526 MR.S wallonnes.

Les **Centres de Soins de Jour (CSJ)** s'adressent aux personnes qui sont dépendantes physiquement (pour se laver, s'habiller, se déplacer, etc.) ou psychiquement (désorientation dans le temps et l'espace), et ne peuvent assurer seules leur vie quotidienne. Chaque CSJ accueille un public spécifique : personnes atteintes de démence, souffrant de problèmes moteurs, âgées de plus de 60 ans, etc. Il y a 56 CSJ wallons.

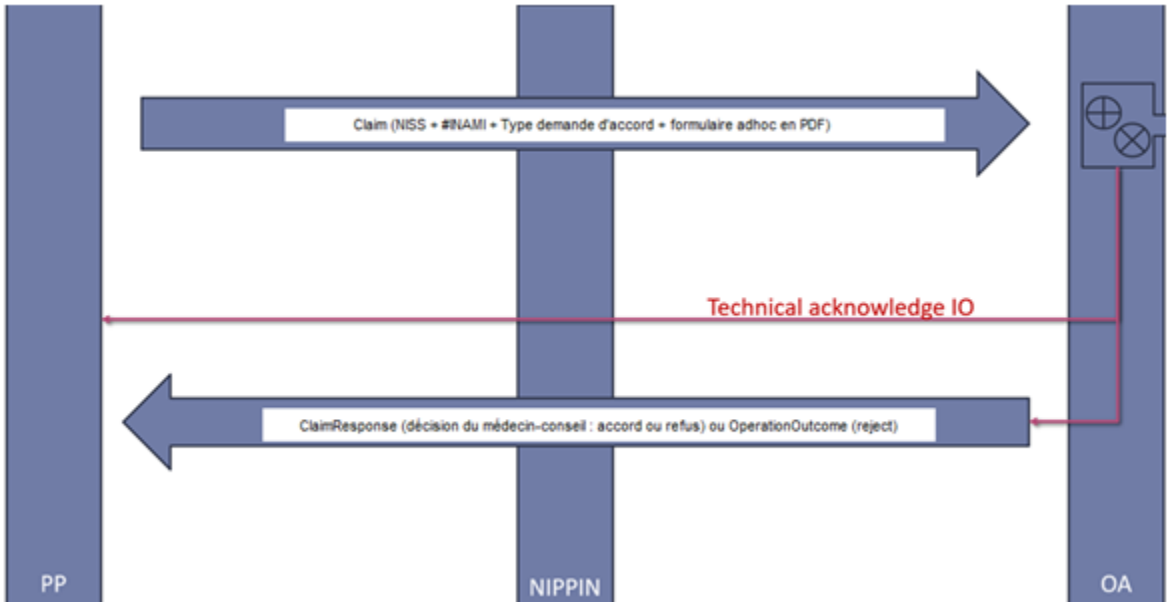
Une **Maison de Soins Psychiatriques (MSP)** est une habitation collective destinée aux personnes souffrant d'un trouble psychique chronique stabilisé ou aux personnes présentant un handicap mental. Les résidents d'une MSP y bénéficient d'un séjour à durée variable en fonction du développement des compétences indispensables pour leur autonomie. Les résidents accueillis dans ces structures n'ont plus besoin de traitement aigu à l'hôpital. Ils ne peuvent toutefois pas vivre de façon autonome ni séjourner dans une autre collectivité (maison de repos et de soins, initiative d'habitations protégées ou institution médico-pédagogique). Ils requièrent en outre un accompagnement continu. Il y a 13 MSP wallonnes.

10. Les instances qui communiqueront des données sont :
- Les institutions (MSP, MR, MRS, CSJ) et en leur sein, les prestataires de soins qui sont amenés à réaliser les analyses médicales dans le cadre de la demande d'admission (médecin/praticien de l'art infirmier);
- Les Organismes Assureurs wallons (OAW) : 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.

Flux de données

11. Le service **'admissions électroniques'** permettra aux institutions autorisées à envoyer les formulaires et documents relatifs à l'admission de leurs résidents aux organismes assureurs wallons via la plate-forme Walcarenet (phase 1 eAgreement light). Dans la phase 2 (eAgreement complet), les OAW enverront leur décision également via la plateforme Walcarenet.

12. Les données reprises dans le flux sont, d'une part, des données à caractère personnel relatives à l'identification des résidents. Ces données figurent aussi sur les carnets de membres ou sur les vignettes d'identification et dans la carte d'identité sociale. D'autre part, le flux comprend des données de santé.



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

13. Liste des documents qui sont échangés : l'AVIQ détermine pour chaque secteur les documents standards à échanger entre le prestataire de soins et les Organismes Assureur Wallons. 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 seront envoyés via Walcarenet des institutions vers les OAW:

- Pour les résidents de < 70 ans en MR et MR.S (au-dessus des 10% à partir du 01/01/2029) il est complété par le personnel administratif de l'institution.
- Demande d'octroi de l'allocation de base.
- Echelle de Katz: formulaire qui évalue l'état de dépendance du patient et fixe la catégorie à laquelle il appartient. Le formulaire sera cadenassé.
- Certificat médical justifiant la demande d'intervention: dans le cadre de l'admission en MSP. Il est complété par un professionnel de santé (médecin). Le formulaire sera cadenassé.
- Déclaration sur l'honneur: pour les résidents de < 70 ans en MR/MR.S, l'institution doit certifier qu'elle respecte le plafond autorisé relatif au nombre de résidents de < 70 ans.
- Plan d'accompagnement des résidents de < 70 ans: pour les résidents de < 70 ans en MR/MR.S.
- Spécificité Ccoma: rapport médical qui certifie que le résident en MR/MR.S appartient à la catégorie spécifique Ccoma. Le formulaire sera cadenassé.
- Exception changement de catégorie: rapport médical qui certifie que le résident en MR/MR.S doit changer de catégorie de dépendance en cas d'aggravation du degré de dépendance. Le formulaire sera cadenassé.
- Notification de fin d'hébergement: Il est complété par le personnel administratif de l'institution.
- Attestation du médecin traitant: dans le cadre de l'admission en CSJ, formulaire qui certifie que le résident est un patient palliatif souffrant d'une maladie grave. Le formulaire sera cadenassé.

14. 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.

15. 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 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

16. 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.

17. 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

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

19. 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).

20. Les institutions fournissent les prestations visées à l'article 34, 11° 12° de la loi du 14 juillet 1994 *relative à l'assurance obligatoire soins de santé et indemnités*. Les organismes assureurs wallons interviennent (Art. 37, § 12) dans le coût de ces prestations aux conditions visées dans l'arrêté royal du 3 juillet 1996. Les données à caractère personnel susceptibles d'être traitées par les institutions et les organismes assureurs wallons (dans le cadre de cette obligation légale), pour la finalité de l'octroi de l'intervention dans le coût des prestations

visées à l'article 34, 11° 12° de la loi du 14 juillet 1994 sont expressément mentionnées et/ou peuvent être logiquement déduites des articles 152, 153 et 153bis de l'arrêté royal susmentionné.

21. Par ailleurs, en vertu du point 3 de l'Annexe 120 du Code Wallon de l'Action Sociale et de la Santé, les MR, MR.S, CSJ sont habilités à traiter une liste limitative de données pour les missions qui leur sont confiées en vertu du ladite Annexe.

22. En outre, depuis la 6ème Réforme de l'État, l'AVIQ intervient pour les prestations visées à l'article 34, 11° 12° de la loi du 14 juillet 1994 et réalisées auprès des assurés wallons, via le circuit de paiement des organismes assureurs wallons. Ces derniers remplissent les missions visées à l'article 43/7 alinéa 1, 4° et 6° du livre IIIter du Code Wallon de l'Action Sociale et de la Santé. L'article 10/12 de l'arrêté du gouvernement wallon du 21 décembre 2018 précise que « les conditions de facturation des prestations et interventions sont déterminées par une convention (au sens de l'article 43/2, 10° et 11° du CWASS) ».

23. En conclusion, les institutions et les organismes assureurs sont (dans le cadre légal prédéterminé) autorisés à traiter les données et les catégories de données à caractère personnelles reprises dans l'arrêté royal de 1996 et dans le CWASS, livre IIIter et son AGW exécutif. Les modalités du traitement de ces demandes, ainsi que des précisions relatives aux catégories de données énumérées dans les dispositions légales et réglementaires peuvent être définies par voie conventionnelle.

24. Ainsi, le principe du traitement des demandes d'admission au format électronique sera contenu dans trois conventions, en cours de modification :
- la convention de plateforme Walcarenet (AVIQ, OAW, CIW, CIN), permettant le recours à l'utilisation de cette plateforme d'échange de données pour des services déterminés ;
- la convention bicommunautaire entre les maisons de repos pour personnes âgées, les maisons de repos et de soins, les centres de soins de jour et les organismes assureurs wallons ;
- la convention bicommunautaires entre les maisons de soins psychiatriques et les organismes assureurs wallons ;

25. L'échange électronique de données personnelles dans le cadre des services Facturation, MDA, et Admissions électroniques s'effectue via Walcarenet qui fonctionne conformément aux dispositions de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*.

26. 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.

27. Le Comité se prononce sous réserve de la modification des conventions susmentionnées à condition que ces nouvelles conventions soient conformes aux conditions de réalisation de l'échange de données faisant l'objet de cette délibération.

28. 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 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.

B. PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

1. FINALITÉ

29. 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.

30. Les données à caractère personnel sont traitées en vue de l'envoi par les institutions aux OAW des demandes d'admission au format digitalisé. Les données traitées par les OAW qui envoient la décision relative à la demande d'admission aux institutions, au format digitalisé.

31. 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

32. 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).

33. Les **données d'identification** de la personne concernée sont le numéro d'identification de la sécurité sociale (NISS), le numéro de registre national, le numéro de mutualité, le nom, le prénom, l'adresse, le numéro interne à l'organisme assureur, CT1, CT2, date de naissance, dénomination de l'institution et le numéro INAMI.

34. Les **données relatives au suivi médical** de la personne concernée : échelle d'évaluation complétée par le praticien de l'art infirmier qui a eu la possibilité d'observer le bénéficiaire dans l'exécution des actes de la vie journalière, ou par le médecin traitant (MR/MR.S); rapport médical pour patient catégorie Cc ou dans le cadre d'une demande de révision de catégorie de dépendance (MR/MRS); certificat médical (établi par le médecin traitant) (MSP) et l'attestation du médecin traitant dans le cadre d'une admission en CSJ.

35. Le Comité de sécurité de l'information estime que ce délai de conservation est raisonnable.

3. LIMITATION DE LA CONSERVATION

36. 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).

37. L'utilisation du service **'Admissions électroniques'** est nécessaire tant que l'AVIQ financera par l'intermédiaire des OAW les interventions dans le coût des prestations de soins aux individus fournies par les institutions et prestataires de soins agréées par la Région wallonne.

38. Pour les institutions, les données médicales contenues les dossiers individualisés de soins sont conservées pendant un minimum de 30 ans à partir du dernier contact de soins (et un maximum de 50 ans).[1]

Pour les OAW, les données sont conservées pendant la durée strictement nécessaire à la correcte mise en œuvre de l'assurance protection sociale wallonne, soit minimum 5 ans et cela conformément à l'article 10/7 de l'AGW du 21 décembre 2018.

4. TRANSPARENCE

39. 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.

40. Le Comité constate que l'AVIQ invoque l'exception que la personne concernée dispose déjà de ces informations. L'AVIQ n'informera pas les personnes concernées.

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

5. MESURES DE SÉCURITÉ

42. 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).

---

[1] Article 20 alinéa 1 de la loi coordonnée sur les hôpitaux du 10 juillet 2008 et l'article 5 de la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé.

43. 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

44. 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.

45. 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.

46. 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.

47. 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 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.

48. 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.

49. Le Comité rappelle que les dispositions de l'article 36/1, § 1er, 1° de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions* doivent être respectées.

50. 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 le 21 octobre 2026.

Michel DENEYER
Président

Annexe
AVIQ Exigences de sécurité – application tierces

1. Contexte & Objectifs

Dans le cadre du recours à des prestataires externes pour le développement et l'hébergement d'applications métier tierces (SaaS / Cloud), la maîtrise des risques cybersécurité constitue un enjeu critique. Afin de garantir l'intégrité des données, la continuité de services et le respect des réglementations en vigueur (RGPD, NIS 2), l'AVIQ formalise un socle d'exigences de sécurité non négociables.

Ce document présente la démarche de cadrage technique ainsi que l'outil d'évaluation mis à disposition pour auditer les prestataires retenus.

2. Principes & Piliers de Sécurité

Les exigences imposées aux prestataires reposent sur 6 piliers fondamentaux :

- **Authentification & Gestion des Accès :** Généralisation du MFA pour les accès privilégiés, gestion stricte des sessions et hachage fort des mots de passe.
- **Traçabilité & Imputabilité :** Journalisation détaillée des événements sensibles, horodatage, protection contre l'altération des logs et interdiction d'y inscrire des données confidentielles.
- **Chiffrement & Confidentialité :** Chiffrement systématique des flux et des données au repos, renforcé par une gestion centralisée des clés.
- **Développement Sécurisé (DevSecOps) :** Application des principes *Security by Design*, audits du code source (OWASP Top 10) et gestion de la chaîne d'approvisionnement logicielle (SCA/SBOM).
- **Sécurité Cloud & SaaS :** Vérification de la souveraineté des données (hébergement UE), certifications tierces (ex. ISO 27001, SOC 2, SecNumCloud), isolation des clients et hardening des conteneurs.
- **Audit & Gouvernance :** Conditionnement de la mise en production à la réalisation d'un test d'intrusion indépendant (Pentest) et souscription d'un engagement de Maintien en Condition de Sécurité (MCS) avec SLA.

3. Questionnaire d'Évaluation

Afin d'industrialiser et d'objectiver le contrôle de ces exigences, un **outil d'évaluation interactif au format Excel** (Questionnaire_Conformite_Securite.xlsx) a été développé.

Fonctionnement du dispositif :

1. **Renseignements par le Prestataire :** Pour chaque exigence, le prestataire sélectionne son niveau de conformité (*Oui*, *Partiel*, *Non*, *Non Applicable*) et **fournit obligatoirement une preuve vérifiable** (extrait de configuration, certificat, rapport d'audit).
2. **Pondération & Scoring :** Les exigences sont associées à un coefficient de criticité de 1 à 3. Le fichier calcule automatiquement la note attribuée par domaine et globale.
3. **Tableau de Bord :** Un onglet de synthèse restitue instantanément :
    - Le **Taux Global de Conformité (%)** de l'application.
    - L'**Avis Sécurité** (*Favorable* si score ≥ 85 %, *Acceptable avec réserves* entre 70 % et 84 %, *Réserve Critique* si < 70 %).
    - Un **histogramme de performance** comparant le niveau de maturité sur chaque pilier.

4. Liste d'exigences

ID	Domaine / Catégorie	Exigence de Sécurité & Technique
AUTH-01	1. Authentification & Accès	MFA obligatoire pour les accès surtout les comptes administrateurs et privilégiés (TOTP, FIDO2/Passkeys).
AUTH-02	1. Authentification & Accès	Utilisation de protocoles d'authentification standards et éprouvés (OAuth 2.0, OIDC, SAML 2.0).
AUTH-03	1. Authentification & Accès	Utilisation de services d'authentification éprouvés en Belgique (FAS, Itsme, MyGov)
AUTH-04	1. Authentification & Accès	Gestion stricte du cycle de vie des sessions (expiration access token <= 15 min, révocation à la déconnexion, anti-session fixation).
AUTH-05	1. Authentification & Accès	Hachage fort des mots de passe avec sel individuel (Argon2id, bcrypt ou PBKDF2) sans stockage en clair.
AUTH-06	1. Authentification & Accès	Politique de complexité des mots de passe paramétrable (>= 12 car., vérification des mots de passe compromis).
AUTH-07	1. Authentification & Accès	Protection contre le brute-force (rate-limiting, verrouillage temporaire, CAPTCHA).
AUTH-08	1. Authentification & Accès	Contrôle d'accès basé sur les rôles (RBAC) respectant le principe du moindre privilège.
LOG-01	2. Traçabilité & Logs	Journalisation exhaustive des événements critiques (authentification, accès données sensibles, administration, erreurs).
LOG-02	2. Traçabilité & Logs	Format de log structuré (JSON) horodaté en UTC (ISO 8601) avec synchronisation NTP.
LOG-03	2. Traçabilité & Logs	Absence totale de données sensibles ou d'identifiants secrets dans les fichiers de logs (mots de passe, tokens, CB, PII non anonymisées).
LOG-04	2. Traçabilité & Logs	Centralisation et protection des logs contre l'altération et la suppression (export SIEM / Syslog distant, WORM).
LOG-05	2. Traçabilité & Logs	Rétention des logs paramétrable et conforme à la réglementation (ex: 1 an).
CRYP-01	3. Chiffrement & Données	Chiffrement des flux en transit avec TLS 1.3 et désactivation des protocoles/ciphers obsolètes.
CRYP-02	3. Chiffrement & Données	Configuration obligatoire des en-têtes de sécurité HTTP (HSTS, CSP, X-Content-Type-Options, X-Frame-Options).
CRYP-03	3. Chiffrement & Données	Chiffrement des données au repos (bases de données, fichiers) via AES-256.
CRYP-04	3. Chiffrement & Données	Chiffrement applicatif renforcé pour les données hautement sensibles (santé, bancaire, clés API).

CRYP-05	3. Chiffrement & Données	Gestion centralisée et sécurisée des clés de chiffrement via un KMS (rotation, séparation des accès).
DEV-01	4. Développement Sécurisé	Respect du guide de développement sécurisé OWASP Top 10 et absence de secrets en dur dans le code.
DEV-02	4. Développement Sécurisé	Analyse continue des dépendances open-source (SCA) pour détecter et corriger les vulnérabilités.
DEV-03	4. Développement Sécurisé	Validation et nettoyage strict côté serveur de toutes les entrées utilisateur (anti-SQLi, XSS, XXE, IDOR).
DEV-04	4. Développement Sécurisé	Architecture 'Security & Privacy by Design' avec isolation hermétique des environnements (Dev / Test / Prod) et anonymisation des données de test.
CLOUD-01	5. Cloud & SaaS	Certifications de sécurité et de conformité de l'hébergeur / SaaS (ISO/IEC 27001, SOC 2 Type II, SecNumCloud, ISO 27017/27018).
CLOUD-02	5. Cloud & SaaS	Souveraineté et localisation des données : Stockage et traitements exclusivement situés au sein de l'UE/EEE sans transfert extracommunautaire non encadré.
CLOUD-03	5. Cloud & SaaS	Gestion IAM Cloud & Moindre Privilège : Utilisation d'identités de service (IAM Roles/Service Accounts), pas de clés d'accès permanentes en dur, MFA sur la console de management.
CLOUD-04	5. Cloud & SaaS	Sécurité des Conteneurs & Orchestration : Images minimales/durcies, scan de vulnérabilités avant déploiement, conteneurs s'exécutant en 'non-root', isolation Kubernetes.
CLOUD-05	5. Cloud & SaaS	Cloisonnement des clients en SaaS (Multi-Tenancy) : Isolation logique ou physique stricte garantissant qu'aucun client ne peut accéder aux données d'un autre (anti-tenant leakage).
CLOUD-06	5. Cloud & SaaS	Infrastructure as Code (IaC) & Hardening : Provisionnement automatisé (Terraform/Ansible) avec scan de sécurité IaC et conformité aux benchmarks CIS.
QUAL-01	6. Audit & Gouvernance	Réalisation d'un audit de code / test d'intrusion (Pentest) indépendant avant MEP et correction obligatoire des vulnérabilités Critiques/Hautes.
QUAL-02	6. Audit & Gouvernance	Fourniture de la documentation de sécurité (DAT/DAS, matrice de flux réseau, SBOM complet).
QUAL-03	6. Audit & Gouvernance	Engagement contractuel de Maintien en Condition de Sécurité (MCS) avec SLA de correction des vulnérabilités.