

<p>Comité de sécurité de l'information Chambre sécurité sociale et santé</p>
--

CSI/CSSS/22/328

DÉLIBÉRATION N° 22/178 DU 6 DÉCEMBRE 2022, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ ENTRE LES ORGANISMES ASSUREURS BRUXELLOIS ET LA CAAMI D'UNE PART ET LES MAISONS DE REPOS, MAISONS DE REPOS ET DE SOINS, CENTRES DE SOINS DE JOUR D'AUTRE PART, DANS LE CADRE DE LA FACTURATION ÉLECTRONIQUE ET D'ACCES AUX DONNÉES DE LEURS MEMBRES VIA IRISCARENET

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 3 décembre 2017 *portant création de l'Autorité de protection des données*, notamment l'article 114, modifié par la loi du 25 mai 2018 ;

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 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre 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*, notamment l'article 97 ;

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 Iriscare ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 30 septembre 2022 et du 30 novembre 2022;

Vu le rapport de monsieur Bart Viaene ;

Émet, après délibération, la décision suivante, le 6 décembre 2022:

I. OBJET DE LA DEMANDE

1. Dans le cadre de la 6ème réforme de l'Etat, la Commission Communautaire Commune de Bruxelles-Capitale ("Cocom") s'est vue transférée un certain nombre de matières notamment la politique de dispensation de soins dans les institutions pour personnes âgées¹. Ce sont les organismes assureurs bruxellois qui interviennent dans le coût des prestations de soins aux individus dans ces institutions.²
2. La Cocom a décidé d'implémenter la facturation électronique mensuelle obligatoire dans ces institutions pour personnes âgées, à savoir 137 maisons de repos et maisons de repos et de soins et 8 centres de soins de Jour. Le passage à la facturation électronique sera obligatoire à partir du 1^{er} avril 2023 pour toutes ces institutions. A partir de cette date, les factures seront envoyées aux organismes assureurs bruxellois (5 Sociétés Mutualistes Régionales Bruxelloises et la CAAMI en sa qualité de caisse auxiliaire bruxelloise) chaque mois par flux électronique via la nouvelle plate-forme régionale bruxelloise Iriscarenet.
3. Iriscarenet, la nouvelle plate-forme bruxelloise, est identique à MyCarenet fédéral³. Il s'agit de 2 plateformes similaires mais distinctes et sans interaction entre elles.
4. Le Collège Intermutualiste Bruxellois (C.I.B.) est le titulaire des différents certificats eHealth. LeC.I.N (Conseil Intermutualiste National) intervient comme opérateur technique de la plate-forme IrisCareNet.

a. Consultation des données des résidents (Member Data – MDA)

5. A cette fin, les institutions doivent pouvoir consulter certaines données concernant leurs résidents (données d'assurabilité, données relatives au dossier médical global, données relatives au pharmacien de référence, données relatives au statut palliatif). Pour ce faire, elles interrogeront l'assurabilité fédérale ainsi que les droits dérivés des organismes assureurs fédéraux via le service Member Data (MDA).
6. Les personnes concernées sont les bénéficiaires de l'assurance obligatoire soins de santé et indemnités, les résidents des maisons de repos, maisons de repos et de soins, centres de soins de jour.

¹ Art. 5, §1^{er}, I, 3^o de la Loi spéciale de réformes institutionnelles.

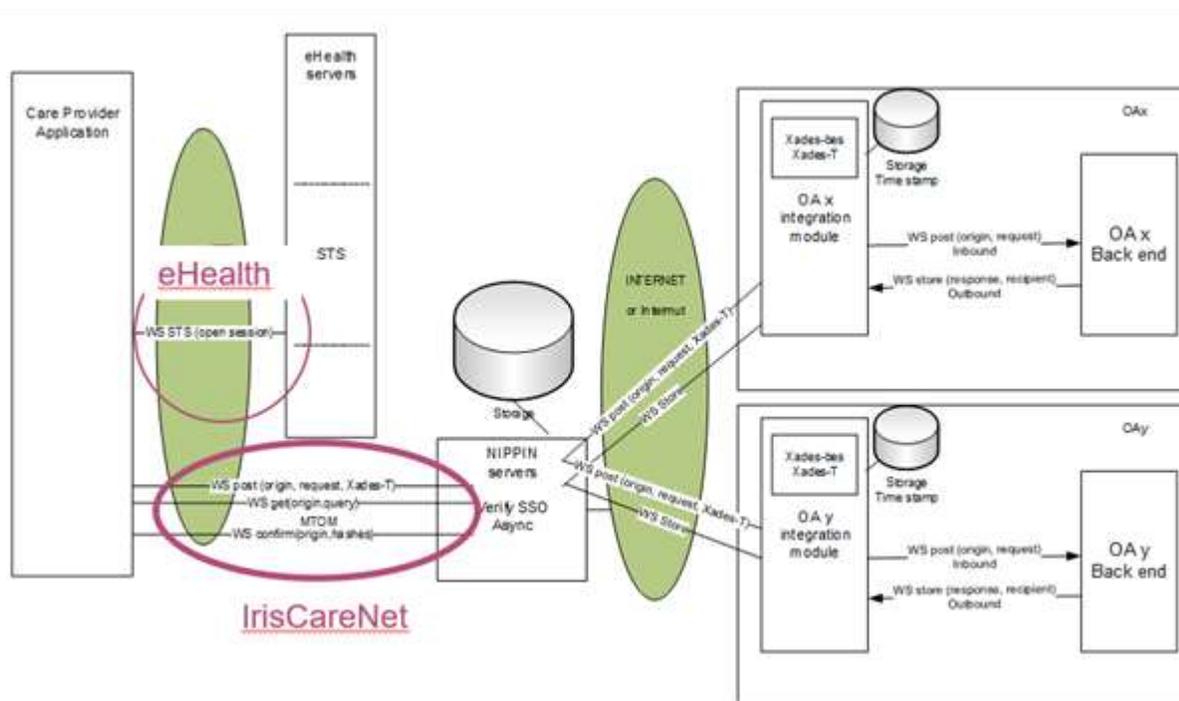
² Art. 3, §1^{er}, 2^o de l'ordonnance du 21 décembre 2018 relative aux organismes assureurs bruxellois dans le domaine des soins de santé et de l'aide aux personnes.

³ Délibération n° 11/052 du 19 juillet 2011, modifiée le 3 juillet 2018 et le 1^{er} septembre 2020 concernant la Communication de données à caractère personnel relatives à la santé entre les prestataires de soins et les offices de tarification, d'une part, et les organismes assureurs, d'autre part, en vue de la détermination du statut d'assurabilité des patients concernés et du calcul du tarif applicable dans le cadre du régime du tiers payant ou de la prise en charge de l'aide médicale par le CPAS, et en vue d'éviter une double prise en charge de certains frais d'hospitalisation.

7. La présente demande concerne :

- 1) **Les données relatives à l'identification de l'organisme assureur du patient** en ce compris les données générales d'identification du patient, les données relatives à une hospitalisation, les données relatives à la situation générale du patient (inscription, mutation, etc.)
- 2) **Les données relatives au pharmacien de référence du patient** en ce compris le numéro Inami de l'officine et la date de début de la convention.
- 3) **Les données relatives au dossier médical global du patient** si celui-ci est détenteur d'un DMG en ce compris le numéro Inami, le nom et le prénom du médecin généraliste ou de la maison médicale détenteur du DMG.
- 4) **Les données relatives au statut palliatif du patient** si celui-ci a reçu le statut palliatif sur base de la notification du médecin traitant en ce compris la date de début du statut palliatif.

8. Les données seront demandées aux organismes assureurs fédéraux via le CIN selon le schéma suivant :



- Le service données du membre (MDA) permet à toute institution autorisée de consulter les informations reprises ci-dessous nécessaires pour effectuer une facturation ou pour délivrer des prestations/des produits de manière correcte.

III. EXAMEN

A. ADMISSIBILITÉ

12. En vertu de l'article 9, 1^{er} du RGPD, le traitement de données à caractère personnel relative à la santé est interdit.
13. 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).
14. La Cocom se réfère à l'article 53, § 1^{er} de la loi coordonnée du 14 juillet 1994 relative à l'assurance obligatoire soins de santé et indemnités : « 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 ».
15. L'arrêté du Collège réuni de la Commission communautaire commune du 8 septembre 2022 modifiant l'arrêté du Collège réuni de la Commission communautaire commune du 30 septembre 2021 portant exécution de l'article 3, § 1er, deuxième alinéa de l'ordonnance du 21 décembre 2018 relative aux organismes assureurs bruxellois dans le domaine des soins de santé et de l'aide aux personnes a été publié au Moniteur belge le 5 octobre 2022.. Les modifications apportées à législation actuelle donnent force probante à l'application des nouvelles règles en matière de facturation électronique dans les instances concernées
16. Dans l'article 2 de l'arrêté du Collège réuni de la Commission communautaire commune du 30 septembre 2021 portant exécution de l'article 3, § 1er, deuxième alinéa de l'ordonnance du 21 décembre 2018 relative aux organismes assureurs bruxellois dans le domaine des soins de santé et de l'aide aux personnes, l'alinéa suivant a étéajouté :

"En outre, en ce qui concerne les interventions dans le coût des prestations de soins aux individus dans les institutions pour personnes âgées, des modalités supplémentaires de ces interventions, y compris des modalités de facturation électronique, peuvent être fixées dans une convention entre, d'une part, les maisons de repos, les maisons de repos et de soins et les centres de soins de jour et, d'autre part, les organismes assureurs bruxellois. Cette

convention peut préciser les interventions précitées et détermine les conditions dans lesquelles les données enregistrées, traitées ou communiquées au moyen de techniques photographiques et optiques, ainsi que leur reproduction sur papier ou sur tout autre support lisible, ont la même force probante que les données originales. Cette convention n'est valable qu'après son approbation par le Conseil de gestion."

17. 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

18. 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.
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).

a. Consultation des données des résidents (Member Data – MDA)

21. **Les données relatives à l'identification de l'organisme assureur du patient** en ce compris les données générales d'identification du patient, les données relatives à une hospitalisation, les données relatives à la situation générale du patient : données du patient, NISS, nom, prénoms, date de naissance, code sexe, date de décès de l'assuré, période d'assurabilité, numéro d'inscription mutualiste, numéro de mutualité, Code titulaire 1 et 2, engagement de paiement, date de communication de l'information, hospitalisation, numéro INAMI de l'hôpital où le patient est hospitalisé, service d'admission de l'hospitalisation, date d'admission de l'hospitalisation, situation générale, situation globale de l'assuré, transfert, organisme assureur du transfert, date du transfert.
22. **Les données relatives au pharmacien de référence du patient** en ce compris le numéro Inami de l'officine et la date de début de la convention.

- 23. Les données relatives au dossier médical global du patient** si celui-ci est détenteur d'un DMG en ce compris le numéro Inami, le nom et le prénom du médecin généraliste ou de la maison médicale détenteur du DMG : DMG, Nom, prénoms et numéro INAMI du médecin généraliste ou de la maison médicale détenteur du DMG,
- 24. Les données relatives au statut palliatif du patient** si celui-ci a reçu le statut palliatif sur base de la notification du médecin traitant en ce compris la date de début du statut palliatif : statut palliatif, date de début du statut palliatif.

b. Facturation

- 25. Les données d'identification** : le NISS, numéro de mutualité, numéro de registre national, nom, prénoms, adresse, numéro interne à l'organisme assureur, code titulaire 1 et 2.
- 26.** Conformément à l'article 5, §1er, e), 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.
- 27.** La consultation des données est nécessaire aussi longtemps qu'Iriscare remboursera les forfaits des personnes concernées. Les prestations sont remboursables pendant une période de 2 ans mais le prestataire peut faire une demande jusqu'à 5 ans dans le passé pour un jour précis. Les données seront donc conservées durant 5 ans.
- 28.** Le Comité de sécurité de l'information estime que ce délai de conservation est raisonnable.

3. TRANSPARENCE

- 29.** 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.
- 30.** Le Comité constate qu'Iriscare invoque l'exception que le personne concernée dispose déjà de ces informations. Iriscare n'informer pas les personnes concernées.
- 31.** Le Comité de sécurité de l'information est d'avis qu'il existe suffisamment de transparence quant au traitement envisagé.

4. MESURES DE SÉCURITÉ

- 32.** 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).

- 33.** 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
- 34.** 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.
- 35.** Le Comité rappelle également qu'Iriscare doit désigner un délégué à la protection des données et communiquer son identité à la BCSS.
- 36.** 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,

Compte tenu de la publication au Moniteur des dispositions législatives mentionnées et de leur entrée en vigueur,

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.

Bart VIAENE
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 (tél. 32-2-741 83 11).