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

CSI/CSSS/20/216

**DÉLIBÉRATION N° 20/128 DU 5 MAI 2020 PORTANT SUR L'ÉCHANGE DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ ENTRE CERTAINS ORGANISMES ASSUREURS ET LES CENTRES DE SANTÉ MENTALE (CSM) VIA MYCARENET EN VUE DE DÉTERMINER LE STATUT D'ASSURABILITÉ DES PATIENTS CONCERNÉS AFIN DE FOURNIR LE FICHIER DE FACTURATION À L'ORGANISME ASSUREUR**

Le Comité de sécurité de l'information, chambre sécurité sociale et santé (dénommé ci-après, le Comité),

Vu le 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 relatif à la protection des données ou GDPR) ;

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 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 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 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 le décret du 18 mai 1999 *relatif au secteur de la santé mentale*;

Vu l'arrêté du Gouvernement flamand du 5 octobre 2012 *relatif à l'établissement de la contribution du patient dans les centres de santé mentale*, en particulier l'article 5 ;

Vu le décret du 5 avril 2019 *relatif à l'organisation et au soutien de l'offre de santé mentale*;

Vu le rapport de monsieur Bart Viaene ;

Émet, après délibération, la décision suivante, le 5 mai 2020:

## I. OBJET

### A. LES CENTRES DE SANTÉ MENTALE (CSM)

1. Les centres flamands de santé mentale (CSM) accompagnent chaque année plus de 50.000 personnes souffrant de lourds troubles psychiques et/ou psychiatriques. Tout CSM dispose d'un fonctionnement spécifique pour les enfants et adolescents, les adultes et les personnes plus âgées. Tout CSM dispose aussi d'un numéro INAMI. L'asbl CSM Vagga intervient en tant que mandataire de l'association de frais créée qui est responsable pour la gestion et le développement du dossier patient informatisé (DPI). Les CSM qui font partie de cette association de frais sont repris à l'annexe 1.

### B. LA PLATEFORME MYCARENET

2. MyCareNet est une plateforme centrale orientée service, au profit des prestataires individuels et institutions, par laquelle des informations peuvent être échangées avec les mutualités (ou « organismes assureurs ») via le Collège Intermutualiste National (CIN), d'une manière simple, fiable et sécurisée. C'est via MyCareNet qu'auront lieu les échanges de données visés dans la présente communication.

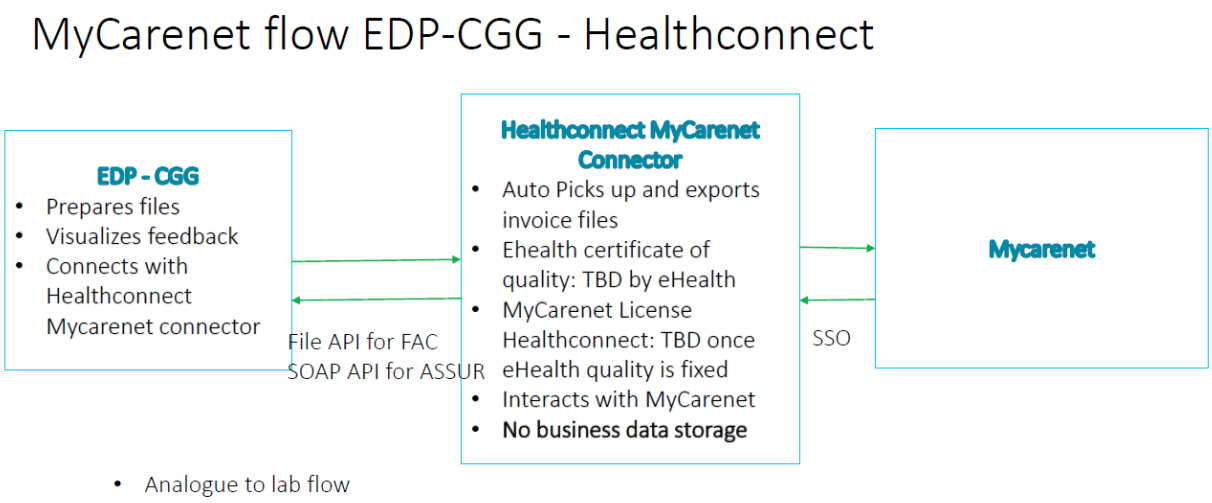
3. D'une manière générale, MyCareNet peut être utilisé par un prestataire individuel ou par une institution/groupement. Dans le cas d'une institution ou d'un groupement, MyCareNet utilise le service de base "*user management*" de eHealth pour vérifier le lien entre un utilisateur et son organisation qu'il dit représenter. MyCareNet et eHealth ont aussi prévu la possibilité pour une entité "le mandant" (prestataire individuel ou institution/groupement) de mandater une autre entité "le mandataire" (personne physique ou organisation), ce qui est le cas pour le CSM Vagga vzw dans cette délibération.

4. L'asbl CSM Vagga pour l'ensemble des CSM qui l'ont mandaté, souhaite avoir accès à deux services de MyCareNet : le service assurabilité et le service facturation tiers payant.

   Le service assurabilité permet à toute institution ou prestataire de soins autorisé de consulter les informations (assurabilité et droits dérivés) du bénéficiaire de soins nécessaires pour effectuer une facturation correcte dans le cadre du tiers payant.

   Le service facturation permet à toute institution ou prestataire de soins autorisé de transmettre aux organismes assureurs, de manière électronique, via réseau, le fichier de facturation créé dans le cadre du tiers payant.

5. Ci-dessous, le schéma résumant les transferts de dossiers électroniques des patients via MyCareNet :




Ce flux de données illustre le flux entre le DPI des CSM et MyCareNet. Afin de faciliter la communication entre le DPI des CSM et MyCareNet, il est fait usage de l'application Hector de la firme logicielle HealthConnect.

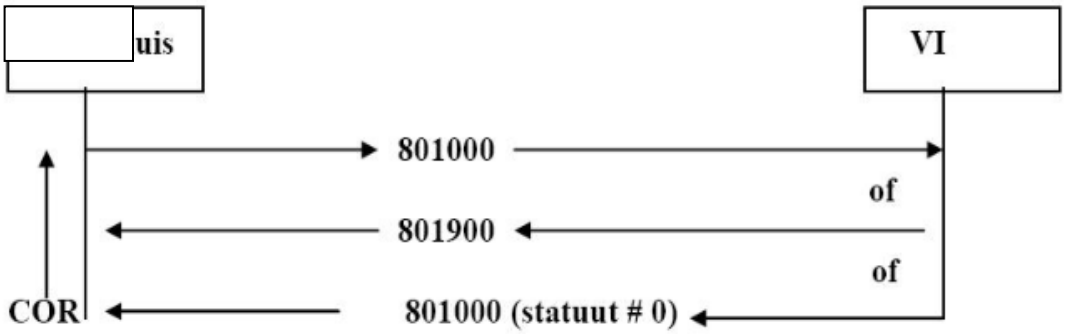
*Flux service assurabilité*

6. Afin d'utiliser le service assurabilité, le prestataire soumet une requête qui, outre l'identification du patient, précisera la période pour laquelle cette consultation d'informations est demandée. Cette requête peut comporter une ou plusieurs consultations d'assurabilité, une seule s'il a opté pour une consultation en mode synchrone, plusieurs s'il a opté pour le mode asynchrone. Cette requête est aiguillée vers les organismes assureurs concernés. Cet aiguillage se fera soit sur la base d'un répertoire national (filtre intermutualiste), soit sur la base d'informations d'appartenance mutualiste complétées dans la requête par le prestataire lui-même (aiguillage forcé). L'organisme assureur traite la consultation et selon les cas, complétera sa réponse par les informations prévues sur le patient tenant compte de la période consultée. Le message réponse est alors retourné par l'OA et est mis à la disposition du prestataire requérant directement ou en différé selon le mode de transmission.

Cette procédure donne la possibilité à chaque prestataire (principalement dans le cas de prestations étalées sur une période - soins infirmiers, kiné,...) de vérifier en début de période de soins la situation d'assurabilité du patient. S'agissant d'informations portant sur le futur, aucun engagement de paiement ne sera associé aux informations communiquées. Cette procédure permet, via la consultation, d'obtenir les informations d'assurabilité consolidées par un numéro d'engagement de paiement à reprendre dans le fichier facturation. Cet engagement de paiement relatif au statut assurabilité du bénéficiaire ne portera que sur une période échue par rapport à la date de consultation ou sur une période s'étalant dans le futur et dont la date de fin est à négocier avec la Commission des

conventions concernée. Par défaut, l'engagement de paiement porte sur le mois civil durant lequel la consultation de l'assurabilité a été faite avec l'option " F ".

7. Voici le schéma du flux assurabilité:




Door het gecodifieerde bericht onder de benaming "801000" kan een aanvraag aan de VI overgemaakt worden die naast de identificatie van de patiënt, de periode waarvoor de raadpleging van informatie wordt gevraagd, zal bepalen.

De informatie i.v.m. het antwoord op de aanvraag is meegedeeld in het bericht die gecodifieerd wordt onder de benaming "801900". In geval van fout(en), wordt het bericht 801000 terug verzonden.

Afin de pouvoir utiliser le service assurabilité, le CSM introduit une demande contenant outre l'identification du patient, la période pour laquelle cette consultation des données est demandée.

Cette demande peut contenir une ou plusieurs consultations d'assurabilité; une suffit s'il a été opté pour une consultation synchrone.

La demande est envoyée aux organismes assureurs concernés. L'envoi aura lieu soit sur la base du numéro national (filtre intermutualiste), soit sur la base d'informations relatives à l'affiliation mutualiste qui seront remplies dans la demande par le prestataire de soins même (envoi forcé).

L'organisme assureur traitera la demande et remplira, en fonction des cas, sa réponse avec les informations prévues relatives au patient. Il est tenu compte de la période consultée. Le message réponse est renvoyé par les organismes assureurs et mis à la disposition du prestataire de soins. Si la communication a eu lieu de manière synchrone, la réponse est immédiate. Si la communication a eu lieu de manière asynchrone, la réponse est envoyée au mailbox du prestataire de soins qui est consultable par lui/elle.

8. Les données à caractère personnel concernant les patients qui sont transférées dans le cadre du flux assurabilité sont donc:
- le nom et le prénom;
- le numéro d'identification de la sécurité sociale;

- s’il est impossible d’identifier le patient au moyen de son NISS, le prestataire peut effectuer une recherche sur la base du numéro d'inscription auprès de la mutualité, couplé au numéro de la mutualité. Dans ce cas, le système MyCareNet ne recherche pas l’affiliation mutualiste mais transmet la demande à l’organisme assureur qui a été indiqué par le prestataire de soins;
- le statut assurabilité;
- le numéro INAMI du prestataire (médecin) et la date, le code nomenclature et le numéro de consultation des prestations envoyées à l’organisme assureur (via MyCareNet).

9. L’échange de données a pour objectif d’obtenir des informations relatives à l’état d’assurabilité des patients afin de déterminer la contribution correcte après une consultation d’un médecin et la contribution correcte du patient après la consultation d’un prestataire de soins non médecin, conformément à l’article 5 de l’arrêté du Gouvernement flamand du 5 octobre 2012 *relatif à l'établissement de la contribution du patient dans les centres de santé mentale*. Il est important pour les CSM d’obtenir les informations relatives au statut d’assurabilité de leurs patients pour la facturation des consultations auprès des médecins à l'organisme assureur dans le cadre du régime du tiers payant ou pour savoir si une réduction de la contribution du patient est applicable à leurs patients pour les consultations auprès de prestataires de soins (non médecins), de sorte qu’ils puissent facturer le montant correct à leurs patients.

L’assurabilité du patient permet de déduire que ce dernier a ou non droit à l’intervention majorée ou entre en considération pour une réduction de sa contribution pour la consultation de prestataires non médecins.

Cet échange de données concerne environ 55 000 patients per an au sein de l’ensemble des CSM. Les CSM souhaitent contrôler le statut d’assurabilité de tous leurs patients afin de vérifier que ces derniers sont effectivement assurés, auprès de quel organisme assureur ils sont assurés, s’ils tombent sous le système de l’intervention majorée et quelle est la situation dans le cadre du maximum à facturer. De cette manière, il est clair quel montant peut être facturé au client pour une consultation d’un médecin et quelle contribution du patient peut être facturée au client pour une consultation d’un prestataire de soins non médecin.

10. Cependant, ni le décret du 18 mai 1999 *relatif au secteur de la santé mentale,* ni le décret du 5 avril 2019 *relatif à l'organisation et au soutien de l'offre de santé mentale* ne détermine de délai de conservation concret pour le traitement de données à caractère personnel par un CSM. Les deux initiatives législatives renvoient au pouvoir exécutif pour déterminer le délai de conservation maximal.

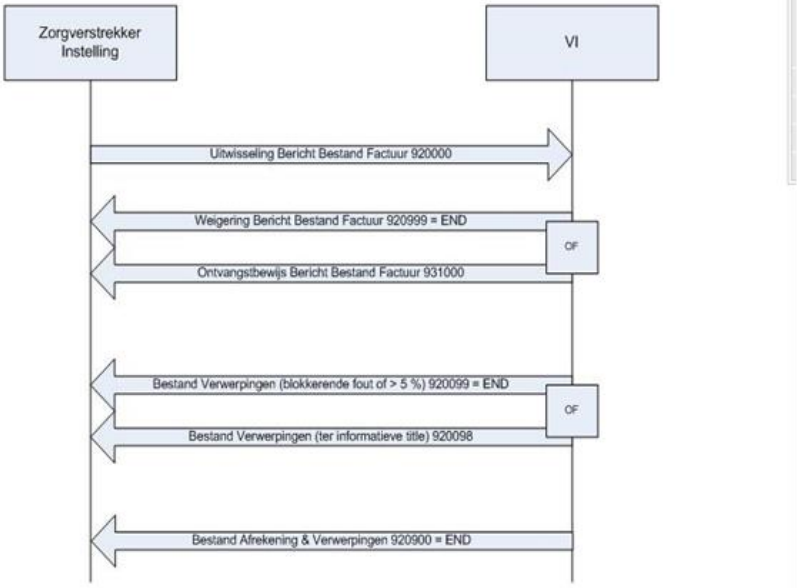
Dans l’attente, il est conseillé de toujours partir d’un délai de conservation maximal de 30 ans, à compter du dernier contact avec le patient. Ceci afin de toujours pouvoir consulter la continuité et la qualité des soins. Ce délai est aussi repris à l’article 24 du Code de déontologie médicale et à l’article 35 de la loi du 22 avril 2019 *relative à la qualité de la pratique des soins de santé.*

11. La fréquence de la consultation des données est permanente. Il est essentiel que les centres de santé mentale puissent contrôler l'assurabilité de leurs clients, sans que cette possibilité ne soit limitée en ce qui concerne la fréquence. Le fait de ne pas pouvoir contrôler l'assurabilité est néfaste pour les soins auxquels les clients ont droit.

*Flux service facturation*

12. Le service facturation permet de remplacer le support magnétique utilisé à ce jour (CD, cassette, disquette) par une transmission électronique, sécurisée, via réseau, du fichier facturation créé par le prestataire dans le cadre du tiers payant. Le fichier facturation conserve, en ce qui concerne son contenu détaillé, la même structure que celle décrite dans les directives de l'Institut national d'assurance maladie invalidité (INAMI) en la matière (instructions de facturation). Cette fonction via réseau permet aussi de supprimer le document papier qui constitue le bordereau d'accompagnement, lequel est remplacé par des informations complémentaires ajoutées au fichier facturation.

13. Voici le schéma du flux assurabilité accompagné d'explications :




920000 : bericht met facturatiebestand overgemaakt door de zorgverstrekker
931000 : ontvangstbewijs bericht 920000 door de betrokkene VI ;
920999 : vermelding van de weigering bericht 920000 door de betrokkene VI ;
920098 : informeel bestand van foutief bericht door de betrokkene VI
920099 : verwerping van het facturatiebestand wegens blokkeringsfout of percentage fouten > 5%
920900 : bestand van afrekening en verwerpingen : eindfase van behandeling van een 920000;

L'échange du dossier de facturation (message 9200000) en mode asynchrone comprend plusieurs étapes:

I. Le prestataire de soins ou l'institution envoie le fichier de facturation à l'organisme assureur (lay-out de l'INAMI) et le complète par des bordereaux d'accompagnement

(message 920000). Un message 920000 comprend un seul envoi (un seul enregistrement de type 10).

II. L'organisme assureur réalise toute une série de contrôles préalables sur les données disponibles dans les enregistrements de ce fichier, à l'exception dans les enregistrements détaillés de la facture même (RT 10 à 90).

a. Si une erreur est constatée, l'organisme assureur envoie un message spécifique (920999) contenant au moins un enregistrement du type en-tête ainsi que tous les enregistrements de type 95 et/ou 96 dans lesquels une erreur a été constatée. Il est important de signaler que l'envoi de ce type de fichier avec signalisation des erreurs signifie également que l'ensemble du fichier de facturation, en ce compris les factures, est considéré comme non valable et devra complètement être renvoyé à l'organisme assureur.

b. Si aucune erreur n'est constatée, l'organisme assureur envoie un accusé de réception (message 931000) pour le fichier de facturation qui devra encore être traité en détail.

III. L'organisme assureur effectue un contrôle des détails de la facture.

a. En cas d'erreur bloquante ou si le nombre d'erreurs est > à 5% par rapport au nombre d'enregistrements liés à la facture, l'organisme assureur envoie un fichier de rejets (message 920099), ce qui entraîne un rejet total du fichier de facturation. Dans ce cas, le prestataire ou l'institution enverra à nouveau un fichier 920000 après correction.

b. S'il n'y a pas d'erreur bloquante ou si le nombre d'erreurs est à < 5% par rapport au nombre d'enregistrements liés à la facture, l'organisme assureur envoie un fichier de rejets (message 920098) à titre d'information. Il s'agit en l'espèce d'un fichier permettant de communiquer rapidement les erreurs constatées, ce qui permet au prestataire ou à l'organisation d'apporter les améliorations pour les factures suivantes.

IV. L'organisme assureur réalise un contrôle plus approfondi. Après réalisation de ces contrôles en collaboration avec les mutualités concernées, l'organisme assureur envoie un fichier de décompte contenant les montants acceptés ainsi que les enregistrements rejetés (message 920900).

14. Les données à caractère personnel concernant les patients qui sont transférées dans le cadre du flux facturation sont:

<u>Pour les transferts de données « CSM vers organismes assureurs » :</u>

- Données d'identification du patient (le nom et le prénom; le numéro d'identification de la sécurité sociale; si le patient ne peut être identifié par son NISS, le prestataire peut effectuer une recherche sur la base du numéro d'inscription auprès de la mutualité, couplé au numéro de la mutualité. Dans ce cas, le système MyCareNet ne recherche pas l'affiliation mutualiste mais transmet la demande à l'organisme assureur indiqué par le prestataire de soins.

- Données d'identification prestataire de soins exécutant (numéro INAMI du prestataire (médecin) et la date, le code nomenclature et le numéro de consultation des prestations envoyées à l'organisme assureur (via MyCareNet));
- Numéro de registre national :
- Données relatives à la santé - codes de prestation (les données enregistrées sur les états récapitulatifs).

Pour les transferts de données « organismes assureurs vers CSM » :
- Corrections des informations transmises par les CSM

15. L'échange de données a pour but de transmettre les fichiers de facturation de manière sécurisée aux organismes assureurs et de recevoir l'input des organismes assureurs concernant le fichier de facturation de manière sécurisée. Le CSM est ainsi en mesure de maintenir à jour son administration et sa facturation. Sur la base des informations que les CSM reçoivent via MyCareNet, les CSM savent comment le patient est assuré (uniquement les gros risques ou aussi les petits), s'il est assuré et auprès de quel organisme assureur il est assuré. Les CSM doivent dès lors aussi facturer en partie directement à l'organisme assureur. Ils souhaitent à cet effet avoir recours à la connexion sécurisée offerte par MyCareNet pour fournir le fichier de facturation à l'organisme assureur. Ils souhaitent pouvoir le faire pour l'ensemble de leurs patients.

Il est primordial que les CSM puissent fournir leurs fichiers de facturation de manière sécurisée aux organismes assureurs sans que cela ne soit limité dans le temps. Le lay-out du fichier de facturation et les données à fournir aux organismes assureurs ont été fixés par l'INAMI.

Cet échange de données concerne quelque 55 000 patients par année au sein de l'ensemble des CSM. Les CSM souhaitent appliquer pour l'ensemble de leurs patients assurés contre les petits risques le régime du tiers payant, de sorte qu'ils puissent facturer directement aux mutualités, de manière sécurisée, pour l'ensemble de ces clients.

16. Cependant, ni le décret du 18 mai 1999 *relatif au secteur de la santé mentale*, ni le décret du 5 avril 2019 *relatif à l'organisation et au soutien de l'offre de santé mentale* ne détermine de délai de conservation concret pour le traitement de données à caractère personnel par un CSM. Les deux initiatives législatives renvoient au pouvoir exécutif pour déterminer le délai de conservation maximal.

Dans l'attente, il est conseillé de toujours partir d'un délai de conservation maximal de 30 ans, à compter du dernier contact avec le patient. Ceci afin de toujours pouvoir consulter la continuité et la qualité des soins. Ce délai est aussi repris à l'article 24 du Code de déontologie médicale et à l'article 35 de la loi du 22 avril 2019 *relative à la qualité de la pratique des soins de santé*.

17. La fréquence de la consultation des données est permanente. Il est essentiel que les centres de santé mentale puissent contrôler l'assurabilité de leurs clients, sans que cette possibilité ne soit limitée en ce qui concerne la fréquence. Le fait de ne pas pouvoir contrôler l'assurabilité est néfaste pour les soins auxquels les clients ont droit.

## II. EXAMEN DE LA DEMANDE

### A. COMPÉTENCE

18. 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.

19. Sur la base de l'identité du demandeur et/ou du code nomenclature de la prestation effectuée, des données à caractère personnel relatives à la santé de la personne concernée dont l'assurabilité est consultée ou pour laquelle le tarif applicable est demandé pourraient en principe être déduites. Le traitement des données à caractère personnel précitées doit dès lors être qualifié de communication de données à caractère personnel relatives à la santé.

20. Certaines données transférées dans le cadre de la présente communication sont quant à elles relatives à la sécurité sociale. Sur le fondement de l'article 15 de la la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale,* la chambre sécurité sociale et santé du Comité de sécurité de l'information est également compétente en ce qui concerne la communication de ces données.

21. 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.

### B. ADMISSIBILITÉ

22. Le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions mentionnées à l'article 6, §1er, du RGPD est remplie. Ceci est notamment le cas lorsque le traitement est nécessaire à l'accomplissement d'une mission d'intérêt public tel qu'établit à l'article 5 de l'arrêté du Gouvernement flamand du 5 octobre 2012 *relatif à l'établissement de la contribution du patient dans les centres de santé mentale*.

23. Le Comité estime par conséquent qu'il existe un fondement pour le traitement des données à caractère personnel envisagé.

### C. FINALITÉ

24. 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.

25. Le demandeur déclare que l'objectif de la demande est de permettre à l'ensemble des CSM reprises dans « l'annexe 1 » de cette délibération d'avoir accès à deux services de MyCareNet : le service assurabilité et le service facturation tiers payant.

Le service assurabilité permet à toute institution ou prestataire de soins autorisé de consulter les informations (assurabilité et droits dérivés) du bénéficiaire de soins nécessaires pour effectuer une facturation correcte dans le cadre du tiers payant.

Le service facturation permet à toute institution ou prestataire de soins autorisé de transmettre aux organismes assureurs, de manière électronique, via réseau, le fichier de facturation créé dans le cadre du tiers payant.

26. 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.

## D. MINIMISATION DES DONNEES

27. 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).

28. Le Comité constate que les données d'identification du patient concerné sont nécessaires en vue d'une identification univoque de ce dernier.

29. Afin de permettre aux CSM de consulter les informations relatives à l'état d'assurabilité pour remettre le dossier de facture à l'organisme assureur, le Comité estime qu'il est en effet nécessaire que les données reprises ci-dessus (numéro d'identification de la sécurité sociale (NISS) et le numéro de registre national du patient ; le nom et le prénom du patient; le statut assurabilité ; le numéro INAMI du prestataire (médecin) et la date, le code nomenclature et le numéro de consultation des prestations envoyées à l'organisme assureur (via MyCarenet) ; le code de prestation) soient échangées.

30. Le principe de proportionnalité implique que le traitement doit en principe être réalisé au moyen de données anonymes. Cependant, si la finalité ne peut être réalisée au moyen de données anonymes, des données à caractère personnel pseudonymisées peuvent être traitées. Le demandeur a besoin d'avoir accès à des données pseudonymisées et non-pseudonymisées afin d'être en mesure de réaliser des analyses très détaillées qu'il ne serait pas possible de réaliser à l'aide de données anonymes. Cette finalité justifie donc le traitement de données à caractère personnel pseudonymisées et non-pseudonymisées.

31. Le Comité estime que les données à caractère personnel sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues.

## E. DELAI DE CONSERVATION

32. 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 pseudonymisées et non-pseudonymisées seront conservées maximum 30 ans à compter du dernier contact avec le patient. Elles seront ensuite détruites.

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

## F. MESURES DE SÉCURITÉ

34. 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).

35. Le Comité de sécurité de l'information constate que les données seront traitées sous la responsabilité de professionnels des soins de santé au sein de chaque CSM qui en outre disposent ou disposeront à courte échéance d'un délégué à la protection des données (DPO).

36. 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 délégué à la protection des données; 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.

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.

38. Le Comité rappelle explicitement les dispositions du Titre 6 relatives aux sanctions 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 prévoient 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 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

Annexe 1 :

| Naam CGG | ondernemingsnr | RIZIV-nr |
|---|---|---|
| Waas en Dender | 471528480 | 72202840 |
| CGG LITP | 472466907 | 72202345 |
| CGG Mandel en Leie | 470808603 | 72201553 |
| CGG Prisma | 472448101 | 72201355 |
| RCGG Deinze-Eeklo-Gent | 467845846 | 72203236 |
| VAGGA | 473488474 | 72203137 |
| cgg Andante | 470375071 | 72203038 |
| CGG Brussel | 471365461 | 72202939 |
| VGGZ | 469813065 | 72202444 |
| CGG Zuid-Oost-Vlaanderen | 470515425 | 72200068 |
| CGG Noord-West-Vlaanderen | 470532647 | 72201949 |
| CGG Largo | 471370411 | 72202741 |
| CGG PassAnt | 446599876 | 72201652 |
| DAGG VZW | 419215489 | 72202246 |
| CGG Kempen | 416724470 | 72201751 |
| CGG Vlaams-Brabant Oost | 471366154 | 72202543 |
| CGG Ahasverus | 471364174 | 72201850 |
| De Pont | 472106225 | 72202642 |
| CGG De Drie Stromen | 471516604 | 72202048 |
| CGG Eclips | 470717046 | 72202147 |