

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

CSI/CSSS/20/398

DÉLIBÉRATION N° 07/003 DU 9 JANVIER 2007, MODIFIÉE LE 2 FÉVRIER 2010, LE 5 JUILLET 2011, LE 7 OCTOBRE 2014, LE 2 FÉVRIER 2016, LE 6 JUIN 2017, LE 5 SEPTEMBRE 2017 ET LE 1^{ER} SEPTEMBRE 2020, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LES ORGANISMES ASSUREURS AUX PRESTATAIRES DE SOINS ET AUX OFFICES DE TARIFICATION 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 UN CENTRE PUBLIC D'ACTION SOCIALE ET EN VUE D'ÉVITER UNE DOUBLE PRISE EN CHARGE DE CERTAINS FRAIS D'HOSPITALISATION

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, § 1^{er};

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 114;

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 les rapports de la Banque Carrefour de la sécurité sociale du 21 décembre 2006, du 21 janvier 2010, du 28 juin 2011, du 1^{er} septembre 2014, du 8 janvier 2016, du 17 mai 2017 et du 24 août 2020;

Vu le rapport de monsieur Bart Viaene.

A. OBJET DE LA DEMANDE

1. Dans le régime du tiers payant, l'organisme assureur rembourse directement au prestataire de soins concerné – il s'agit à la fois de personnes physiques (médecins, infirmiers, pharmaciens, ...) et d'entités (hôpitaux généraux, hôpitaux psychiatriques, maisons de repos et de soins, laboratoires, groupements de médecins, groupements d'infirmiers, pharmacies, ...) - le montant de l'intervention de l'assurance dans ses frais d'honoraires. Par conséquent, l'assuré social ne doit plus avancer ce montant mais doit uniquement payer la part personnelle, appelée aussi ticket modérateur, au prestataire de soins.

L'application du régime du tiers payant suppose cependant que les prestataires de soins concernés soient au courant du statut d'assurabilité de leurs patients. Une application a, à cet effet, été développée, également au profit des offices de tarification, à l'aide de laquelle ils peuvent contrôler, d'une manière sécurisée, ce statut d'assurabilité et donc calculer correctement le montant restant à payer par le patient.

Une autre application permet aux prestataires de soins de consulter le tarif qu'ils peuvent facturer compte tenu du statut d'assurabilité du patient concerné.

- 2.1. Lorsque l'intervention des organismes assureurs dans le coût des fournitures délivrées par les pharmaciens n'est pas directement versée par ces organismes aux titulaires, l'article 165 de la loi *relative à l'assurance obligatoire soins de santé et indemnités*, coordonnée le 14 juillet 1994, dispose que toutes les opérations de tarification et tous les paiements des organismes assureurs pour fournitures délivrées par les pharmaciens sont obligatoirement effectués par l'intermédiaire d'offices de tarification agréés.

Les pharmaciens doivent donc obligatoirement être affiliés auprès d'un office de tarification. Les offices de tarification interviennent, au profit des pharmaciens, dans le traitement administratif des fournitures pharmaceutiques par les organismes assureurs. Ils peuvent être considérés comme les intermédiaires obligatoires dans les relations entre les pharmaciens et les organismes assureurs et ils doivent, en cette qualité, pouvoir faire appel à certaines données à caractère personnel lorsque la facturation est rejetée par l'organisme assureur en question (ce qui n'arrive qu'exceptionnellement). Il est à noter que les données à caractère personnel obtenues peuvent uniquement être utilisées à cette fin par les offices de tarification, à l'exclusion de toute autre finalité. En d'autres termes, ils peuvent uniquement traiter les données à caractère personnel dans la mesure où cela est nécessaire au règlement administratif des fournitures pharmaceutiques entre les pharmaciens et les organismes assureurs.

Les offices de tarification sont considérés, dans le cadre de la réglementation relative à la protection de la vie privée, comme des sous-traitants des pharmaciens, ces derniers étant les responsables du traitement. Leur relation mutuelle est régie dans le contrat de sous-traitance, visé à l'article 28 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*. Les données à caractère personnel sont traitées par les offices de tarification exclusivement sur la base des instructions fournies par les pharmaciens. En tant que sous-traitant, l'office de tarification ne dispose donc pas d'un droit d'accès aux données à caractère personnel.

- 2.2. En ce qui concerne les psychologues et orthopédagogues cliniciens, le comité de l'assurance de l'INAMI a approuvé une convention qui règle le remboursement des séances de première ligne réalisées par eux. Ces séances sont réalisées dans leur pratique dans la zone d'activité du réseau. Pour pouvoir réaliser les séances, les psychologues et orthopédagogues cliniciens doivent avoir conclu une convention avec le réseau de la région où se trouve leur pratique.

Il y a un hôpital par réseau qui facture les séances. Les psychologues et orthopédagogues cliniciens communiquent les détails des séances qu'ils ont réalisées à l'hôpital chargé de facturer au sein de leur réseau. L'hôpital paie aux psychologues et

orthopédagogues cliniciens l'intervention de l'assurance dans les séances qu'ils ont réalisées.

Cependant, l'intervention personnelle du psychologue et de l'orthopédagogue clinicien est facturée au patient. Seuls ceux ayant conclu une convention avec le réseau de leur région verront leurs prestations remboursées par l'assurance obligatoire et devrait avoir, dans ce cadre limité, accès aux données d'assurabilité de leurs patients.

Le message électronique qui est transmis par un organisme assureur à un psychologue clinicien ou un orthopédagogue clinicien contient, outre quelques données administratives relatives au message électronique, des données à caractère personnel d'identification de la personne concernée (le numéro d'identification de la sécurité sociale, le nom, le prénom, le sexe, la date de naissance et, le cas échéant, la date de décès) et certaines données à caractère personnel relatives à l'assurabilité (le numéro d'identification de l'organisme assureur, le code CT1/CT2, la date de la communication et la mutualité).

3. Sur base du numéro d'identification de la sécurité sociale (le numéro d'identification du registre national des personnes physiques ou le numéro d'identification de la Banque Carrefour de la sécurité sociale) du patient, le prestataire de soins concerné est en mesure de prendre connaissance de certaines données à caractère personnel.

Conformément à l'article 4 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*, le numéro d'identification de la sécurité sociale peut être utilisé dans les relations entre les organismes assureurs et les personnes qui sont tenues de recevoir ou de fournir des renseignements au sujet du titulaire de ce numéro d'identification, dans le cadre des obligations qui leur sont imposées par une disposition légale ou réglementaire relative à la sécurité sociale.

Par ailleurs, différentes catégories de prestataires de soins ont, dans l'intervalle, été autorisées par les comités sectoriels (jadis) compétents à accéder, à des fins de facturation, au registre national des personnes physiques et aux registres Banque Carrefour et à utiliser son numéro d'identification (voir par exemple la délibération n° 21/2009 du 25 mars 2009 du Comité sectoriel du registre national et la délibération n° 09/39 du 7 juillet 2009 du Comité sectoriel de la sécurité sociale et de la santé).

Les deux applications précitées vérifieront, sur base du numéro d'identification de la sécurité sociale communiqué, dans une banque de données à caractère personnel gérée par le Collège intermutualiste national, auprès de quel organisme assureur le patient concerné est affilié. Il est néanmoins possible que le prestataire de soins concerné indique lui-même l'organisme assureur concerné, lors de la vérification de l'assurabilité.

- 4.1. Grâce à l'application de consultation du statut d'assurabilité du patient, le prestataire de soins (et le cas échéant, l'office de tarification qui est confronté au rejet de la facturation d'un pharmacien par un organisme assureur) reçoit un message électronique qui, en plus de quelques données administratives relatives au message électronique même, contient les données à caractère personnel suivantes relatives à son patient (et - en ce qui

concerne les offices de tarification - relatives au client du pharmacien au profit duquel ils assurent le traitement administratif des fournitures pharmaceutiques).

Données d'identification. Il s'agit du numéro d'identification de la sécurité sociale du patient concerné, de ses nom et prénom, de sa date de naissance, de son sexe, et, le cas échéant, de sa date de décès. Le prestataire de soins concerné est en principe déjà au courant du numéro d'identification de la sécurité sociale du patient, étant donné qu'il doit utiliser ce numéro lorsqu'il effectue sa demande.

Reprise de certaines données à caractère personnel mentionnées dans la demande. Lors de la réalisation de la demande, l'application sécurisée applique plusieurs critères de consultation. Ceux-ci sont repris dans le message réponse au prestataire de soins concerné. Il s'agit du numéro de référence qu'il a éventuellement indiqué dans sa demande, du type de consultation, du type de contact, des dates de début et fin de la période consultée (pour les pharmaciens, la date de la demande/de la délivrance), de la situation globale du patient (cette zone permet de mentionner une situation exceptionnelle du patient se rapportant à la période consultée, par exemple la mutation vers un autre organisme assureur), de la date de la mutation éventuelle vers un autre organisme assureur, de l'indication de l'organisme assureur initial et du nouvel organisme assureur, de la date d'affiliation au cours de la période consultée, de l'indication selon laquelle le régime du tiers payant peut être appliqué ou non, de l'identification de l'hôpital où le patient est hospitalisé, de la date d'admission pour l'hospitalisation en cours et du service d'admission pour l'hospitalisation en cours. En ce qui concerne la communication initiale de données à caractère personnel par les prestataires de soins aux organismes assureurs, veuillez-vous référer à la délibération n° 11/52 du 19 juillet 2011, modifiée en dernier lieu le 1^{er} septembre 2020.

Données à caractère personnel relatives au maximum à facturer. Ces données à caractère personnel permettent au prestataire de soins de vérifier si le patient a droit à l'application du maximum à facturer pendant la période consultée. Il s'agit notamment de l'année la plus récente située dans la période consultée au cours de laquelle le patient a droit au maximum à facturer, complétée des autres années situées dans la période consultée au cours desquelles le patient a droit au maximum à facturer.

Données à caractère personnel relatives à l'assurabilité du patient. Il s'agit, par cas concerné, du code statut, des dates de début et de fin de la période d'assurabilité, de l'identification de l'organisme assureur, du code titulaire 1, du code titulaire 2, du numéro de l'accord concerné en matière d'obligation de paiement et de la date de la communication.

Données à caractère personnel supplémentaires. Il est possible que le patient bénéficie pour la période consultée d'une convention avec une maison médicale. Les maisons médicales reçoivent, pour chaque patient inscrit auprès d'elles sur base d'un abonnement, un montant forfaitaire qui couvre les prestations réalisées par les médecins, infirmiers et kinésithérapeutes de la maison médicale. Les prestations de ces catégories de prestataires de soins ne sont donc plus remboursables individuellement pour les abonnés d'une maison médicale. Le prestataire de soins qui, dans le cadre du régime du tiers payant, facture ses prestations à l'organisme assureur d'un abonné d'une maison médicale se verra donc confronté à un refus de remboursement. Les médecins, infirmiers et kinésithérapeutes doivent donc être informés de l'existence d'une convention conclue

avec une maison médicale. Le cas échéant, les dates de début et de fin de la convention sont mentionnées dans le message réponse. En ce qui concerne certaines catégories d'assurés sociaux – par exemple celles qui entrent en considération pour un forfait de soins aux malades chroniques –, il est interdit de leur facturer des honoraires supplémentaires lorsqu'en cas d'hospitalisation ces assurés partagent une chambre de deux personnes ou une chambre commune. C'est la raison pour laquelle l'organisme assureur doit transmettre cette donnée à caractère personnel à l'hôpital en cas d'hospitalisation.

Données à caractère personnel relatives au séjour de l'intéressé dans une maison de repos pour personnes âgées, dans une maison de repos et de soins ou dans un hôpital : les officines publiques (en tant que responsables du traitement) et les offices de tarification (en tant que sous-traitants) ont besoin de ces données à caractère personnel dans le cadre de la tarification à l'unité de médicaments délivrés dans une officine publique à des personnes qui séjournent dans une maison de repos pour personnes âgées ou dans une maison de repos et de soins. Dans le cadre d'une mesure d'économie du gouvernement visant à maîtriser le volume de médicaments facturés, les pharmaciens sont tenus de facturer à l'unité (p.ex. au comprimé) certains médicaments (spécialités pharmaceutiques remboursables ayant une forme d'administration orale-solide pour les traitements aigus et chroniques) délivrés dans les officines publiques aux résidents de maisons de repos pour personnes âgées et de maisons de repos et de soins. Dès lors, ils doivent avoir connaissance de ce type de séjour. Le séjour des intéressés dans un hôpital doit également être connu puisque cela met un terme à l'obligation précitée.

- 4.2.** Pour déterminer le tarif à facturer, le prestataire de soins envoie au moyen de l'application développée un message électronique contenant les données à caractère personnel suivantes : le numéro d'identification de la sécurité sociale du patient, le numéro d'identification de la sécurité sociale du prestataire de soins, la date de la prestation, les codes nomenclature pour lesquels le prestataire de soins souhaite connaître le tarif et – si d'application – le numéro INAMI du détenteur du dossier médical global et le motif spécifique permettant d'appliquer le régime du tiers payant.

Le message électronique que l'organisme assureur envoie à titre de réponse, contient les données à caractère personnel suivantes : l'identification du patient (numéro d'identification de la sécurité sociale, nom, prénom, date de naissance, sexe, code titulaire 1/2) et, par code nomenclature demandé, le montant à payer par l'organisme assureur, le montant à payer par le patient (le ticket modérateur), le numéro de l'accord applicable en matière d'engagement de paiement et le motif permettant d'appliquer le régime du tiers payant.

- 4.3.** Par sa délibération n° 12/21 du 6 mars 2012, la section sécurité sociale du Comité de sécurité sociale et de la santé a accordé une autorisation pour l'échange de données à caractère personnel dans le cadre du projet « eCarmed » (actuellement « Mediprima »), qui porte sur la décision électronique de prise en charge de l'aide médicale pour les personnes en difficultés financières. Cette décision est prise par un centre public d'action sociale et permet à la personne concernée de bénéficier, sous certaines conditions, d'aide médicale dont le coût est pris en charge par la Caisse auxiliaire d'assurance maladie-invalidité.

- 4.4.** Afin de permettre aux prestataires de soins de facturer correctement le ticket modérateur aux patients couverts par une décision de prise en charge de l'aide médicale par le CPAS, un service web a été développé par le Collège intermutualiste national. Sur la base de l'information fournie par le prestataire de soins, de l'information dont la Caisse auxiliaire d'assurance maladie-invalidité dispose elle-même et de la décision de prise en charge de l'aide médicale (telle qu'enregistrée au niveau de Mediprima), le tarif applicable pourra être calculé. Le prestataire de soins communique les informations suivantes via le service web : la date de la prestation, le numéro d'identification de la sécurité sociale, le(s) code(s) de nomenclature pour le(s)quel(s) le prestataire de soins souhaite connaître le tarif et la version du message électronique. Il reçoit ensuite de la Caisse auxiliaire d'assurance maladie-invalidité l'identité du patient (le numéro d'identification de la sécurité sociale, le nom, le prénom, la date de naissance et le sexe) et, par code de nomenclature mentionné, le tarif applicable (la date de la prestation, l'honoraire, le ticket modérateur, le numéro d'agrément de l'engagement de paiement, le montant du remboursement à l'égard du Service public de programmation Intégration sociale et du centre public d'action sociale, l'identité du centre public d'action sociale, la référence et la version du message électronique et l'indication du besoin d'une attestation « aide médicale urgente »).

Le traitement des données à caractère personnel s'effectue comme suit. Une demande de consultation du tarif à facturer pour une personne déterminée est envoyée à la Caisse auxiliaire d'assurance maladie-invalidité à partir du logiciel du prestataire de soins via le webservice 'Consultation Mediprima' et à l'intervention de la Plate-forme eHealth et du Collège intermutualiste national. La Caisse auxiliaire d'assurance maladie-invalidité consulte, à l'intervention du Collège intermutualiste national et de la Banque Carrefour de la sécurité sociale, la banque de données des décisions de prise en charge de l'aide médicale, calcule le tarif et confirme ou non l'engagement de couvrir les frais. Le résultat du calcul et l'information relative à l'engagement sont finalement transmises au prestataire de soins concerné à l'intervention du Collège intermutualiste national et de la Plate-forme eHealth.

B. EXAMEN DE LA DEMANDE

- 5.** Il s'agit d'une communication de données à caractère personnel qui, en vertu de l'article 15, § 1^{er}, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, doit faire l'objet d'une délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

En vertu du règlement (UE) 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, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de limitation des finalités), elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données), elles 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 (principe de limitation de la conservation) et elles 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 (principe d'intégrité et confidentialité).

6. La demande poursuit des finalités légitimes, à savoir l'application efficace du régime du tiers payant, ce qui permet aux patients de ne pas devoir d'abord payer eux-mêmes le montant de l'intervention de l'assurance dans le coût des honoraires des prestataires de soins pour ensuite récupérer ce montant auprès de l'organisme assureur, ainsi que l'application efficace de la décision de prise en charge de l'aide médicale par un centre public d'action sociale.
7. Les données à caractère personnel à communiquer sont pertinentes et non excessives par rapport à cette finalité.
Les données d'identification du patient concerné sont nécessaires en vue d'une identification univoque de ce dernier.

Le numéro de référence que le prestataire de soins a éventuellement mentionné dans sa demande, le type de consultation, le type de contact et les dates de début et de fin de la période consultée constituent des critères de recherche dont il a au préalable connaissance. Il ne constitue pas pour lui de nouvelles données à caractère personnel.

Le prestataire de soins doit être au courant de l'identité de l'organisme (des organismes) assureur(s) concerné(s) auprès duquel (desquels) l'intéressé est affilié durant la période consultée, étant donné qu'en cas d'application du régime du tiers payant, il doit directement s'adresser à l'organisme assureur de l'intéressé, en vue d'obtenir le remboursement des soins fournis.

L'identification de l'hôpital où le patient est hospitalisé, la date d'admission de l'hospitalisation en cours et le service d'admission de l'hospitalisation en cours sont uniquement mentionnés si les soins sont fournis dans un hôpital de soins ambulatoires ou techniques autre que l'hôpital où le patient est hospitalisé. Pendant un séjour dans l'hôpital A, il se peut qu'un patient doive subir un examen ou un traitement dans l'hôpital B, après quoi il retourne le jour même à l'hôpital A. C'est l'hôpital B qui facturera ce montant ; toutefois, sur la facture, il devra aussi mentionner l'hôpital A ainsi que le jour d'hospitalisation et le type de service hospitalier dans lequel l'intéressé séjourne.

Les données à caractère personnel relatives au maximum à facturer sont nécessaires dans les cas où le prestataire de soins doit aussi transmettre cette information au patient assuré de sorte que ce dernier puisse disposer d'un aperçu complet des données de facturation le concernant, notamment en cas d'hospitalisation, et dans les cas où la réglementation prévoirait que le prestataire de soins doive adapter la facturation de ses prestations, conformément à cette information. Voir cependant aussi le point 8.

Le prestataire de soins a besoin des données à caractère personnel proprement dites relatives à l'assurabilité du patient – les dates de début et de fin de la période d'assurabilité, le code titulaire (CT1) et le code titulaire 2 (CT2) – en vue de vérifier si la facturation peut effectivement avoir lieu (sur base de la constatation que l'assuré a effectivement droit aux interventions pour les prestations de soins de santé concernées) et en vue de déterminer la part des frais de santé qui tombent à charge de l'organisme

assureur de l'assuré. Les codes CT1 et CT2 permettent de faire une distinction entre l'assurabilité *gros risques* et l'assurabilité *petits risques*. Les CT1 et es CT2 contiennent des informations relatives au droit à l'assurabilité (respectivement pour les grands et petits risques), la qualité de l'assuré et le montant de l'intervention (intervention majorée ou intervention ordinaire).

Les données à caractère personnel complémentaires relatives aux conventions conclues avec une maison médicale doivent être transmises pour la raison suivante. Les maisons médicales reçoivent, pour chaque patient inscrit auprès d'elles sur base d'un abonnement, un montant forfaitaire qui couvre les prestations réalisées par les médecins, infirmiers et kinésithérapeutes de la maison médicale. Les prestations de ces catégories de prestataires de soins ne sont donc plus remboursables individuellement pour les abonnés d'une maison médicale. Le prestataire de soins qui, dans le cadre du régime du tiers payant, facture ses prestations à l'organisme assureur d'un abonné d'une maison médicale se verra donc confronté à un refus de remboursement. Les médecins, infirmiers et kinésithérapeutes doivent donc être informés de l'existence d'une convention conclue avec une maison médicale.

Enfin, en ce qui concerne certaines catégories d'assurés, il est interdit de leur facturer des honoraires supplémentaires lorsqu'en cas d'hospitalisation, ces assurés partagent une chambre de deux personnes ou une chambre commune. C'est la raison pour laquelle l'organisme assureur doit transmettre cette donnée à caractère personnel à l'hôpital en cas d'hospitalisation.

Les données à caractère personnel mentionnées au point 4.2., avec en particulier (par code nomenclature pour lequel le prestataire de soins pose une question) le montant que le patient doit personnellement payer et le montant pris en charge par l'organisme assureur, sont nécessaires pour déterminer le tarif que le prestataire de soins doit facturer. L'organisme assureur déterminera ce tarif sur la base des renseignements fournis par le prestataire et des renseignements qu'il possède concernant le patient.

Les données à caractère personnel relatives au séjour dans une maison de repos pour personnes âgées, dans une maison de repos et de soins ou dans un hôpital sont nécessaires dans le cadre de la tarification obligatoire à l'unité de certains médicaments délivrés dans une officine publique à des personnes qui séjournent dans une maison de repos pour personnes âgées ou dans une maison de repos et de soins.

- 8.1.** L'Institut national d'assurance maladie et invalidité prie également le Comité de sécurité de l'information de lui accorder une autorisation pour l'utilisation des données à caractère personnel précitées relatives au maximum à facturer pour une autre finalité, à savoir éviter une double prise en charge de certains frais d'hospitalisation.

Le système du maximum à facturer offre à chaque ménage la garantie qu'il ne devra pas dépenser plus qu'un certain plafond pour les frais de santé. En effet, les frais d'hôpitaux ne sont pas exclusivement couverts par l'assurance obligatoire soins de santé, mais peuvent également faire l'objet d'un remboursement par une assurance hospitalisation.

Afin d'éviter une double prise en charge de certains frais d'hôpitaux, il est proposé d'informer les hôpitaux sur l'applicabilité du système du maximum à facturer, afin qu'ils puissent mentionner cette applicabilité sur la note d'hospitalisation qui est remise

au patient. Ce dernier doit utiliser cette note d'hospitalisation vis-à-vis de l'assureur hospitalisation afin de prouver ses frais. L'assureur hospitalisation est ainsi informé du fait que l'ayant droit bénéficie du maximum à facturer et que ce dernier se voit donc déjà rembourser ses frais par l'assurance obligatoire soins de santé. L'assureur hospitalisation ne doit donc plus rembourser ces frais.

Ainsi, il faudrait permettre aux organismes assureurs de communiquer aux hôpitaux le fait qu'un bénéficiaire donné a droit au maximum à facturer pour l'année civile concernée. Cette communication doit pouvoir avoir lieu par la voie électronique et sur support papier.

La communication des données à caractère personnel relatives au maximum à facturer poursuit par conséquent aussi une deuxième finalité légitime, à savoir éviter une double prise en charge de certains frais d'hôpitaux (par, d'une part, l'assurance obligatoire soins de santé et, d'autre part, l'assurance hospitalisation). Les données à caractère personnel communiquées sont pertinentes et non excessives par rapport à cette finalité.

Le système du maximum à facturer a pour conséquence que, lorsque le montant des quotes-parts personnelles qui ont été prises en charge pendant une année civile déterminée par les membres d'un ménage, atteint le montant plafond en vigueur, les quotes-parts personnelles dépassant ce montant plafond sont entièrement prises en charge par l'assurance obligatoire soins de santé et indemnités.

En vertu de l'article 3, alinéa 3, de la loi du 5 juin 2002 *relative au maximum à facturer dans l'assurance soins de santé*, les prestataires de soins peuvent être informés de l'octroi du maximum à facturer à des patients. L'arrêté royal du 13 janvier 2014 *portant exécution de l'article 3, alinéa 3, de la loi du 5 juin 2002 relative au maximum à facturer dans l'assurance soins de santé, en ce qui concerne les pharmaciens*, qui entre en vigueur au 1^{er} janvier 2015, dispose à cet égard que lorsqu'un pharmacien délivre une prestation de santé à un bénéficiaire dans une officine ouverte au public et que ce bénéficiaire bénéficie de l'octroi du maximum à facturer pour l'année dans laquelle la prestation est délivrée, l'organisme assureur auprès duquel ce bénéficiaire est affilié ou inscrit en informe le pharmacien lors de la consultation des données d'assurabilité du bénéficiaire.

Lors de la délivrance de produits remboursables, le pharmacien est donc en mesure de vérifier à l'aide d'une application si un droit au maximum à facturer existe pour la période concernée dans le chef du patient. Il pourra ainsi garantir une facturation correcte vis-à-vis du patient.

9. Par sa délibération n° 97/48 du 3 juillet 1997, le Comité de surveillance près la Banque Carrefour de la sécurité sociale (le prédécesseur de la chambre sécurité sociale et santé du Comité de sécurité de l'information) a déjà autorisé la communication de certaines données à caractère personnel par les organismes assureurs aux prestataires de soins, dans le cadre du régime du tiers payant. Toutefois, cette communication était limitée à la communication de données à caractère personnel en vue de la rectification ou de la mise à jour des données à caractère personnel initialement communiquées par le prestataire de soins même.

- 10.1.** Les offices de tarification ne consulteraient les données à caractère personnel qu'en cas de rejet de la facturation d'un pharmacien par un organisme assureur. De plus, en tant que sous-traitant, l'office de tarification ne dispose pas d'un droit d'accès aux données à caractère personnel, mais uniquement d'un droit en tant que sous-traitant du pharmacien pour lequel il intervient.
- 10.2.** Pour permettre aux acteurs concernés de consulter les informations relatives au tarif de la prise en charge de l'aide médicale par un centre public d'action sociale, le Comité de sécurité de l'information consent par ailleurs au traitement des données à caractère personnel mentionnées au point 4.4.

C. MESURES DE SÉCURITÉ

- 11.** Pour les applications précitées, il y a lieu de prévoir un solide système d'identification et d'authentification des utilisateurs.

La mise à la disposition des applications doit se limiter aux prestataires de soins visés à l'article 2, n), de la loi *relative à l'assurance obligatoire soins de santé et indemnités*, coordonnée le 14 juillet 1994, et à leurs mandataires respectifs, en vue de l'application du régime du tiers payant et (en ce qui concerne les données à caractère personnel relatives au maximum à facturer) en vue d'éviter une double prise en charge de certains frais d'hôpitaux.

Les offices de tarification doivent également avoir accès aux données à caractère personnel au profit des pharmaciens.

En ce qui concerne les psychologues cliniciens ou orthopédagogues cliniciens qui ont conclu une convention avec le réseau de leur région, ils peuvent, pour les interventions personnelles, avoir (dans un cadre limité) accès aux données d'assurabilité de leurs patients.

- 12.** Par ailleurs, les loggings relatifs à la consultation des données à caractère personnel concernées doivent être gérées et tenues à la disposition du Comité sectoriel de la sécurité sociale et de la santé. Ces loggings doivent notamment mentionner quel prestataire de soins a obtenu quels types de données à caractère personnel relatives à quel patient, à quel moment et pour quelles finalités.

Les loggings doivent permettre à l'organe de surveillance compétent de réaliser sa mission de contrôle. Ils doivent être conservés pendant une période de dix ans minimum.

L'accès aux loggings doit se limiter aux délégués à la protection des données des institutions de sécurité sociale concernées par l'application, à la demande de l'organe de surveillance compétent ou des fonctionnaires dirigeants des institutions de sécurité sociale concernées. Lors de l'accès aux loggings, il y a également lieu de prévoir un solide système d'identification et d'authentification, par exemple au moyen de la carte d'identité électronique.

13. La Banque Carrefour de la sécurité sociale ne doit pas intervenir dans la présente communication de données à caractère personnel, en vertu de l'article 14, alinéa 1^{er}, 2^o, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.
14. Les délégués à la protection des données des parties concernées par les applications (« consultation de l'assurabilité » et « consultation des tarifs ») – tant les délégués désignés auprès des institutions de sécurité sociale, conformément à la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* que (le cas échéant) les délégués désignés auprès des hôpitaux (conformément à l'arrêté royal du 23 octobre 1964 *portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre*) et des offices de tarification (conformément à l'arrêté royal du 15 juin 2001 *déterminant les critères d'agrément des offices de tarification*) – doivent, dans le cadre de leurs missions légales et réglementaires, surveiller l'usage de l'application.
15. La communication des données à caractère personnel proprement dite, à l'aide des applications précitées, doit également faire l'objet de mesures de protection spécifiques.

Il y a lieu d'utiliser un système d'autorisation d'accès aux deux applications afin de permettre à leur gestionnaire de l'application de vérifier, d'une part, la légitimité de l'accès de l'utilisateur et, d'autre part, de disposer d'un système qui assure en permanence l'adéquation entre les missions de l'utilisateur et les autorisations accordées.

Par ailleurs, il y a lieu de mettre en œuvre les mesures techniques et organisationnelles nécessaires afin de pouvoir constater avec certitude quel utilisateur utilise ou a utilisé les services, à quel moment et pour quelles finalités.

Selon la technologie utilisée (particulièrement lors de l'utilisation des services web), il est nécessaire de mettre en place un système qui garantit l'origine du message et sa non-altération durant l'échange. À cette fin, l'utilisation de la signature numérique est demandée.

Dans le cadre d'échanges de données en dehors de l'Extranet de la sécurité sociale ou en dehors de réseaux privés sécurisés reconnus par la Banque Carrefour de la sécurité sociale ou dans le cadre de l'échange de données qui n'ont pas lieu à l'intervention de la Plate-forme eHealth, il y a lieu d'utiliser une procédure de cryptage end-to-end.

Au niveau applicatif, c'est l'usage d'un protocole HTTPS qui est obligatoire.

Dans le cadre de l'utilisation du réseau Internet et afin de protéger le réseau contre d'éventuelles attaques externes, il y a lieu de prévoir la mise en place d'un serveur "mandaté". Ainsi, les utilisateurs d'Internet ont seulement indirectement accès à certains serveurs internes à l'infrastructure.

16. Les données à caractère personnel concernées doivent, le cas échéant, être mises à la disposition de la Banque Carrefour de la sécurité sociale, conformément à l'article 10 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.

Ainsi, elles pourraient être communiquées à d'autres personnes qui en besoin en vue de l'application de leurs missions légales et réglementaires.

Toutefois, cette communication ultérieure doit, en toute hypothèse, faire l'objet d'une délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

- 17.** Les différents hôpitaux et offices de tarification ne pourront obtenir communication des données à caractère personnel précitées que pour autant qu'ils disposent d'un délégué à la protection des données et d'un plan de sécurité de sécurité de l'information.
- 18.** Lors du traitement des données à caractère personnel, les parties tiennent compte de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* et de toute autre réglementation relative à la protection de la vie privée, en particulier 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* et de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

conclut que la communication de données à caractère personnel par les organismes assureurs aux prestataires de soins concernés (et/ou à leurs mandataires) et aux offices de tarification, en vue d'une application efficace du régime du tiers payant, du maximum à facturer et du système Mediprima, de la simplification de la facturation des prestations de santé et, en ce qui concerne les données à caractère personnel relatives au maximum à facturer, en vue d'éviter une double prise en charge de certains frais d'hôpitaux, telle que décrite dans la présente délibération, est autorisée moyennant le respect des mesures de protection de la vie privée qui ont été définies.

Les différents hôpitaux et offices de tarification ne pourront obtenir communication des données à caractère personnel précitées que pour autant qu'ils disposent d'un délégué à la protection des données et d'un plan 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).