Comité sectoriel de la Sécurité sociale et de la Santé
Section « Sécurité sociale »

CSSS/07/183

DÉLIBÉRATION N° 07/070 DU 4 DÉCEMBRE 2007 CONCERNANT LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LES ORGANISMES ASSUREURS AUX PRESTATAIRES DE SOINS INFIRMIERS À DOMICILE EN VUE DE LA PRISE EN CHARGE, PAR LES ORGANISMES ASSUREURS, DES SOINS FOURNIS PAR LES PRESTATAIRES DE SOINS INFIRMIERS À DOMICILE

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment son article 15, § 1er ;

Vu la demande du Collège Intermutualiste National du 19 septembre 2007 ;

Vu le rapport d'auditorat de la Banque Carrefour de la sécurité sociale du 26 novembre 2007 ;

Vu le rapport de monsieur Yves Roger.

A. OBJET DE LA DEMANDE

1.1. La demande a pour objet l'échange de certaines données à caractère personnel entre, d'un côté, les prestataires de soins infirmiers à domicile et, de l'autre côté, les organismes assureurs, via un réseau sécurisé. Cette échange vise la prise en charge, par les organismes assureurs, des soins fournis par les prestataires de soins infirmiers à domicile.

Actuellement, les données concernées sont échangées à l'aide de formulaires papiers. Grâce à l'utilisation des nouvelles technologies, les prestataires de soins disposeront d'un accès plus rapide à l'information, continuellement réactualisée.

L'échange de données à caractère personnel interviendra à l'intervention de la plateforme BeHealth. La plateforme BeHealth constitue une plateforme de services électronique en vue de l'échange de données à caractère personnel entre acteurs des soins de santé. Il est géré par le service d'Etat à gestion séparée de même nom, créé au sein du service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement par l'article 4 de la loi du 27 décembre 2006 *portant des dispositions diverses (I).*

Il est par ailleurs fait appel à MyCareNet, un système mis à la disposition par les organismes assureurs en vue de l'échange électronique de données à caractère personnel entre les organismes assureurs et les professionnels des soins de santé (dont notamment les infirmiers). MyCareNet constitue donc une des applications qui font appel à certains services de la plateforme BeHealth. Dans le cas présent, lors de la connexion de l'utilisateur, il est fait usage du user management de BeHealth (identification et authentification) : différents fichiers de référence authentiques validés et systèmes de contrôle surveillent les profils des utilisateurs potentiels. Sur base de ces profils, il peut être déterminé s'ils ont ou non accès à l'application en question.

1.2. La procédure peut être décrite comme suit.

Le prestataire de soins infirmiers à domicile doit, à l'entame des soins de toilettes ou d'une visite, notifier à l'organisme assureur du patient sur la base de critères déterminant l'état du patient le type de forfaits et/ou le nombre de visites toilettes qu'il compte appliquer ou effectuer. Cette notification est, d'un point de vue réglementaire, obligatoire pour la prise en charge par l'assurance obligatoire des soins donnés à des patients au stade de soins palliatifs ou non. Cette notification peut concerner une première demande, une demande de modification des forfaits notifiés antérieurement à l'organisme assureur si vu l'état du patient les types de soins donnés évoluent dans le temps ou une prolongation d'une notification préalablement acceptée par l'organisme assureur si l'état du patient le justifie.

Le prestataire de soins infirmiers à domicile communique les catégories de données suivantes: des données d'identification du patient, des données d'identification du prestataire de soins (et si nécessaire l'indication qu'il y a eu un changement de prestataire de soins), des données relatives à la demande (notamment l'indication du forfait pratiqué et la fréquence des soins), des données sur l'état du patient (notamment les éléments de la grille KATZ qui permettent de déterminer le degré de dépendance du patient), et enfin des données relatives au centre de jour si les soins sont prodigués à un patient se trouvant dans un tel centre.

1.3. L'organisme assureur, par le biais de ses services de médecin-conseil, prend acte de cette notification et envoie en réponse à celle-ci sa décision au prestataire de soins infirmiers à domicile.

L'organisme assureur peut donner son accord sur les éléments contenus dans la notification ou refuser la notification pour divers motifs (par exemple s'il existe une notification similaire existante pour le patient). Dans certains cas, suite à une visite de contrôle du médecin-conseil au domicile du patient, l'organisme assureur peut modifier de sa propre initiative un accord préalable.

La décision de l'organisme assureur reprend, en fonction de la situation concrète, tout ou parties des données envoyées préalablement par le prestataire de soins infirmiers à domicile complétées de la décision de l'organisme assureur.

Ces informations permettent également à l'organisme assureur d'accomplir une autre mission importante à savoir de contrôler au moment de la vérification de facturation l'adéquation entre, d'une part, les soins facturés par le prestataire de soins infirmiers à domicile et, d'autre part, les informations acceptées au moment de la notification.

Les données à caractère personnel que l'organisme assureur communique au prestataire de soins infirmiers à domicile en réponse à sa notification se composent, d'une part, de tous les éléments communiqués dans la notification par le prestataire de soins infirmiers (voir 1.2.) et, d'autre part, de la réponse de l'organisme assureur qui contient:

- des données d'identification du bénéficiaire, à savoir les nom et prénom du patient concerné (ceci permet au prestataire de s'assurer de l'identification correcte du patient);
- le numéro d'identification du médecin-conseil de l'organisme assureur;
- la décision de l'organisme assureur (accord ou refus);
- le numéro de référence de l'accord ou du refus communiqué par l'organisme assureur;
- s'il s'agit d'un refus, la codification du motif du refus;
- les dates de début et de fin de la période de traitement accordée;
- l'information qui précise que le patient est en soins palliatifs (cette donnée constitue en fait un rappel qui n'est communiqué que si au préalable et pour ce patient un accord pour ce type de soins a été transmis au prestataire de soins infirmiers à domicile);
- dans le cas particulier de la dispensation à domicile de soins palliatifs, la date de début de la période de facturation.

1.4. Dans le cadre de sa mission de contrôle, l'organisme assureur peut être amené, après une visite du médecin-conseil au domicile du patient, à modifier des éléments de la notification initiale. En effet, le médecin-conseil qui constaterait un changement des critères pris en considération pour déterminer le type de forfait à appliquer doit dès lors communiquer sa nouvelle décision au prestataire de soins infirmiers à domicile qui a établi la notification originale. Si, entre-temps, le patient a changé de dispensateur de soins, la modification sera notifiée au nouveau prestataire de soin désigné par le patient.

La communication de données de données dans ce cas particulier par l'organisme assureur au prestataire de soins infirmiers à domicile se compose des types de données suivantes:

- des données liées à l'identification du patient: le NISS du patient, le nom et le prénom du bénéficiaire, le sexe;
- le numéro de l'organisme assureur;
- le numéro d'inscription du patient auprès de cet organisme assureur;
- le numéro d'identification INAMI du prestataire concerné;
- de données concernant l'accord initial: date de début de la période du forfait initial, type de forfait initial et référence;
- des informations connues avant la visite du médecin-conseil: score KATZ, précision continence et notion de démence;
- des données concernant les modifications apportées à l'accord initial: date de la visite, le numéro d'identification INAMI du médecin-conseil, nature du message de modification, nouveau forfait après visite, date de fin de la période forfait initial, date de début de la période du forfait après visite, référence de la notification communiquée par l'organisme assureur;
- des données obtenues suite à la visite du médecin-conseil: score KATZ, précision continence, notion de démence, nombre de jours de soins par semaine, fréquences de toilettes, nombre de toilettes sur la fréquence, nombre de visites par jour, notion de patient palliatif.

1.5. Cette communication électronique entrerait en production le 1er janvier 2008.

B. EXAMEN DE LA DEMANDE

2.1. L'article 70 de la loi du 1er mars 2007 *portant des dispositions diverses (III)* modifie l'article 42 de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé* en ce sens qu'à partir d'une date encore à déterminer par le Roi et sauf quelques exceptions, toute communication de données à caractère personnel relatives à la santé doit faire l'objet d'une autorisation de principe de la section santé du Comité sectoriel de la sécurité sociale et de la santé.

Pour l'instant cependant, conformément à l'article 15 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, une autorisation de principe est seulement requise pour la communication de données à caractère personnel relatives à la santé par les institutions de sécurité sociale, dont les organismes assureurs.

L'article 72, alinéa 1er, de la loi précitée du 1er mars 2007 dispose par ailleurs que "*dans l'attente de l'institution du Comité sectoriel de la sécurité sociale et de la santé et de la nomination de ses membres, les missions attribuées au Comité sectoriel de la sécurité sociale existant précédemment, tel qu'institué avant l'entrée*

en vigueur de la présente loi, continuent à être exercées par ce même comité sectoriel de la sécurité sociale".

2.2. Il ressort donc de cette analyse que la communication par l'organisme assureur au prestataire de soins infirmiers à domicile, qui reprend tout ou partie des données envoyées par le prestataire de soins infirmiers à domicile complétées de la décision de l'organisme assureur, est donc bien une communication de données à caractère personnel qui, en vertu de l'article 15 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 autorisation de principe de la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé.

2.3. La communication poursuit une finalité légitime, à savoir l'exécution de l'article 8 de l'arrêté royal du 14 septembre 1984 *établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités* et l'article 6 du règlement du 28 juillet 2003 *portant exécution de l'article 22, 11°, de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994*.

L'article 6 du règlement du 28 juillet 2003 précité prévoit en effet que les remboursements de l'assurance soins de santé sont accordés à la condition que soit remise à l'organisme assureur une attestation de soins, lorsqu'il s'agit de prestations effectuées par les praticiens de l'art infirmier.

2.4. Les données à caractère personnel précitées sont pertinentes et non excessives par rapport à cette finalité.

Dans le cadre de communication de données relatives à la santé, il est évident qu'il est essentiel d'identifier correctement le patient et le prestataire de soins infirmiers à domicile.

La communication par l'organisme assureur des données transmises initialement par le prestataire de soins répond expressément à une demande des prestataires de soins infirmiers à domicile qui peuvent dès lors plus facilement reconstituer le dossier du patient.

Les autres données communiquées par l'organisme assureur se composent soit de la décision d'accord ou de refus de prise en charge du forfait proposé soit, en cas de modification d'un accord préalable, des éléments concrets qui justifient la modification de cet accord initial.

2.5. Conformément à l'article 14, alinéa 2, de la loi du 15 janvier 1990, la communication se fait sans l'intervention de la Banque Carrefour de la sécurité sociale.

C. MESURES DE SÉCURITÉ

3.1. Pour l'application précitée, il y a lieu de prévoir un solide système d'identification et d'authentification des utilisateurs.

Pour rappel, l'échange de données à caractère personnel interviendra à l'intervention de MyCareNet qui utilise le user management élaboré dans le cadre de la plateforme BeHealth en vue de la gestion des utilisateurs et des accès.

3.2. Les loggings relatifs à l'échange de 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 dispensateur de soins a obtenu quels types de données à caractère personnel relatives à quel patient, à quel moment et pour quelles finalités. Ces loggings doivent permettre au Comité sectoriel de la sécurité sociale et de la santé 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 conseillers en sécurité des institutions de sécurité sociale concernées par l'application, à la demande du Comité sectoriel de la sécurité sociale et de la santé 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.

3.3. 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 2, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.

3.4. La communication des données à caractère personnel proprement dite, à l'aide de l'application précitée, doit également faire l'objet de mesures de protection spécifiques.

Il y a lieu d'utiliser un système d'autorisation d'accès à l'application afin de permettre au 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, 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.

3.5. 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 autorisation du Comité sectoriel de la sécurité sociale et de la santé.

Par ces motifs,

le Comité sectoriel de la sécurité sociale et de la santé, section sécurité sociale,

autorise les organismes assureurs à communiquer, via la plate-forme BeHealth, les données à caractère personnel précitées aux prestataires de soins infirmiers à domicile en exécution de l'article 8 de l'arrêté royal du 14 septembre 1984 *établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités* et de l'article 6 du règlement du 28 juillet 2003 *portant exécution de l'article 22, 11°, de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994*.

Yves ROGER
Président