Comité sectoriel de la sécurité sociale et de la santé
Section « Sécurité sociale »

CSSS/10/101

AVIS N° 10/21 DU 7 SEPTEMBRE 2010 CONCERNANT LA DEMANDE DU MINISTRE DES AFFAIRES SOCIALES RELATIVE AU PROTOCOLE, ÉTABLI LE 17 MARS 2010 PAR LA COMMISSION DE CONVENTIONS PRATICIENS DE L'ART INFIRMIER – ORGANISMES ASSUREURS, PORTANT LES CONDITIONS ET LES MODALITÉS SELON LESQUELLES FORCE PROBANTE PEUT ÊTRE ACCORDÉE JUSQU'À PREUVE DU CONTRAIRE AUX DONNÉES QUI SONT ENREGISTRÉES OU CONSERVÉES AU MOYEN D'UN PROCÉDÉ ÉLECTRONIQUE OU COMMUNIQUÉES D'UNE AUTRE MANIÈRE QUE SUR UN SUPPORT PAPIER, AINSI QUE LES CONDITIONS ET LES MODALITÉS SELON LESQUELLES CES DONNÉES SONT REPRODUITES SUR PAPIER OU SUR TOUT AUTRE SUPPORT LISIBLE

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*;

Vu l'arrêté royal du 27 avril 1999 *relatif à la force probante des données enregistrées, traitées, reproduites ou communiquées par les dispensateurs de soins, les organismes assureurs, l'Institut national d'assurance maladie-invalidité et toute autre personne physique ou morale en application de la loi coordonnée le 14 juillet 1994 (relative à l'assurance obligatoire soins de santé et indemnités) et de ses arrêtés d'application*;

Vu la demande de l'Institut national d'assurance maladie-invalidité;

Vu le rapport d'auditorat de la Banque-carrefour de la sécurité sociale du 23 août 2010;

Vu le rapport de monsieur Yves Roger.

A. OBJET DE LA DEMANDE

1. L’article 2 de l’arrêté royal du 27 avril 1999 *relatif à la force probante des données enregistrées, traitées, reproduites ou communiquées par les dispensateurs de soins, les organismes assureurs, l'Institut national d'assurance maladie-invalidité et toute autre personne physique ou morale en application de la loi coordonnée le 14 juillet 1994 (relative à l’assurance obligatoire soins de santé et indemnités) et de ses arrêtés d'application* dispose que, pour l'application de l'assurance obligatoire soins de santé et indemnités, les données dont les dispensateurs de soins, les organismes assureurs, l'Institut national d'assurance maladie-invalidité ou toute autre personne physique ou morale disposent et qui sont enregistrées ou conservées au moyen d'un procédé électronique, photographique, optique ou de toute autre technique, ou qui sont transmises sur un support autre qu'un support papier, ainsi que leur reproduction sur papier ou sur tout autre support lisible, ont force probante jusqu'à preuve du contraire, si la procédure adoptée pour leur enregistrement, leur conservation ou leur communication est conforme à la procédure décrite dans un protocole rédigé conformément aux dispositions de l'article 3 et approuvé par le Ministre en vertu de l'article 9.

2. En vertu de l’article 9 de l’arrêté royal précité, le Ministre examinera, entre autres, si la procédure décrite répond aux conditions suivantes :

1) la procédure proposée garantit une reproduction fidèle, durable et complète des informations;
2) la procédure prévoit un enregistrement systématique et complet des données;
3) la procédure prévoit que les données sont soigneusement conservées, systématiquement classées et protégées contre toute altération et elle prévoit des mesures de sécurité afin de protéger le caractère confidentiel des données;
4) la procédure prévoit que les données suivantes relatives au traitement des données sont conservées :
    a) l'identité du responsable du traitement ainsi que de celui qui a exécuté celui-ci;
    b) la nature et l'objet des informations auxquelles le traitement se rapporte;
    c) le lieu et la date de l’opération;
    d) les perturbations éventuelles qui ont été constatées pendant le traitement.

3. En vertu de l’article 3 de ce même arrêté royal, le protocole précité est rédigé par la commission de conventions ou d'accords de l’Institut national d’assurance maladie-invalidité relative à la catégorie des dispensateurs de soins pour laquelle elle est compétente pour conclure un accord ou une convention. Ce protocole comprend une description précise des conditions et modalités selon lesquelles les données nécessaires pour l'application de l'assurance obligatoire soins de santé et dont disposent lesdits dispensateurs de soins ou les organismes assureurs, peuvent être enregistrées ou conservées au moyen d'un procédé électronique, photographique, optique ou de toute autre technique ou communiquées d'une autre manière que sur

un support papier, ainsi que les conditions et modalités selon lesquelles ces données sont reproduites sur papier ou sur tout autre support lisible.

La commission de conventions ou d'accords concernée soumet le protocole à l'approbation du Ministre des Affaires sociales. Avant de prendre une décision, le Ministre soumet le protocole au Comité sectoriel de la sécurité sociale et de la santé, qui lui transmet ses remarques éventuelles dans un délai de deux mois.

4. Par un courrier du 6 avril 2010, l'Institut national d'assurance maladie-invalidité a soumis au Ministre des Affaires sociale le protocole *MyCareNet* relatif à la force probante des données électroniques dans le cadre des soins infirmiers à domicile, en exécution de l'arrêté royal du 27 avril 1999.

Conformément à l'article 9 de l'arrêté royal précité, le protocole a entre-temps été soumis pour avis au Comité sectoriel de la sécurité sociale et de la santé.

Le Comité sectoriel de la sécurité sociale et de la santé a informé le Ministre du fait que des informations complémentaires de la part de l'Institut national d'assurance maladie-invalidité et du Collège intermutualiste national étaient nécessaires afin de pouvoir formuler un avis motivé quant au protocole soumis. Le Ministre a transmis ces informations[1] au Comité sectoriel en date du 8 juillet 2010.

B. EXAMEN DE LA DEMANDE

5. Le protocole doit être confronté aux conditions techniques prévues à l'article 9 de l'arrêté royal précité du 27 avril 1999.

Le protocole soumis fixe les conditions et les modalités auxquelles doit répondre la procédure de transmission de données entre infirmiers et organismes assureurs afin de pouvoir accorder force probante jusqu'à preuve du contraire aux données énumérées ci-après qui sont enregistrées ou conservées au moyen d'un procédé électronique, photographique, optique ou de toute autre technique ou qui sont communiquées d'une autre manière que sur un support papier : d'une part, des données en matière de facturation, d'autre part, des documents médico-administratifs, à savoir les demandes de toilettes et forfaits, les notifications de soins palliatifs et les demandes de prestations techniques spécifiques de soins infirmiers.

[1] Suite aux remarques formulées par le service Sécurité de l'information de la Banque Carrefour de la sécurité sociale, la Commission de conventions infirmiers-organismes assureurs a rédigé une nouvelle version de l'annexe II "*Solution MyCareNet: Principes techniques de l'échange et de la reproduction des données"* du protocole. Cette annexe II adaptée a été approuvée par ladite commission le 29 juin 2010.

Le Comité sectoriel et le service de Sécurité de l'information de la Banque Carrefour de la sécurité sociale ont examiné le protocole notamment sur la base des critères mentionnés à l'article 9, 1° à 5°, de l'arrêté royal du 27 avril 1999. La procédure en question semble répondre aux critères précités. Néanmoins, le Comité sectoriel souhaite formuler quelques recommandations et suggestions susceptibles d'améliorer la sécurité de l'information.

6. Principes techniques

L'échange de données se déroule via la plateforme MyCareNet. Il s'agit d'un réseau sécurisé entre les dispensateurs de soins et les organismes assureurs, qui utilise certains services de la plate-forme eHealth et le réseau CareNet existant. Les échanges d'informations à travers cette plateforme peuvent s'effectuer de manière *synchrone* (transactionnelle) ou *asynchrone* (transfert en mode batch : la réponse à la question parvient en mode différé). Les données pour lesquelles force probante est demandée par le biais du protocole en question (fichiers de facturation et documents médico-administratifs) seront, pour l'instant, uniquement traitées de manière asynchrone. Le service de base eBox de la plate-forme eHealth est utilisé pour fournir des informations concernant le déroulement du traitement (situation des différentes informations et leur historique et disponibilité des fichiers à consulter). Le dispensateur de soins doit régulièrement consulter les messages dans ce mailbox électronique sécurisé de sorte à être au courant des communications effectuées à partir des organismes assureurs.

Pour la gestion intégrée des utilisateurs et des accès (identification / authentification / autorisation), en ce compris les mandats, il est fait appel à des services de base élaborés par la plate-forme eHealth. Plusieurs fichiers de référence authentiques validés et systèmes de contrôle veillent aux profils des utilisateurs potentiels. Ces profils permettent de déterminer si la personne concernée peut avoir accès ou non à l'application en question.

La plateforme MyCareNet prévoit à la fois des interactions de *système à système* (services web) et une *application portail* (via www.mycarenet.be) pour la transmission de données. Dans les deux cas, l'utilisateur doit s'authentifier de manière univoque au moyen du certificat d'authentification présent sur sa carte d'identité électronique (eID). Comme mentionné ci-avant, il est fait appel à des services de base spécialisés de la plate-forme eHealth pour ce contrôle de l'identité du dispensateur de soins ou de son mandataire et pour la vérification de ses autorisations.

En cas d'authentification positive, une session sécurisée est ouverte. Conformément aux autorisations n° 07/003 du 9 janvier 2007 et n° 07/070 du 4 décembre 2007, le

canal de communication[2] entre le dispensateur de soins et MyCareNet est chiffré: la protection de cette connexion est basée sur SSL/TLS.

La protection au niveau du transport s'effectue donc au moyen de HTTPS via *1-way SSL*. Ceci garantit un canal de communication sécurisé. La section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé attire l'attention sur le fait que l'utilisation de HTTPS via *2-way SSL* (authentification du client et du serveur) est fortement recommandée. La documentation de MyCareNet mentionne que tous les *SSL cipher suites* sont soutenus. Il est par ailleurs fortement recommandé de rendre cette liste plus restrictive avec des paramètres cryptographiques de sorte à éviter des attaques au protocole SSL.

Les fichiers de facturation et les documents médico-administratifs échangés au sein de MyCareNet (regroupés par transmission dans un CPD (Care Provider Document)) sont signés électroniquement au moyen de l'eID à des fins d'intégrité, à la fois dans le mode "système à système" et dans le mode portail. Cette signature est appliquée globalement sur l'ensemble des documents transmis dans un CPD. La personne qui signe peut être le dispensateur de soins individuel ou le responsable du regroupement de dispensateurs de soins, ou tout utilisateur MyCareNet autorisé désigné par l'un d'eux au moyen du *user management* de eHealth ou au moyen d'un *mandat* eHealth.

Pour la communication avec les organismes assureurs, MyCareNet échange des messages avec une passerelle « Client » via le réseau CareNet. Les organismes assureurs disposent d'une passerelle « Serveur ». Ces passerelles (*client* et *serveur*) assurent la signature numérique et le chiffrement des informations transmises via le réseau et ce à l'aide de certificats spécifiques. Le chiffrement de cette connexion entre MyCareNet et les organismes assureurs s'effectue sur base de TDES (128 bit).

L'échange de messages entre ces passerelles s'effectue conformément aux principes techniques décrits dans les annexes du protocole CareNet, établi le 19 avril 2001 entre les organisations représentatives des établissements de soins et les organismes assureurs.

Le Comité sectoriel tient à rappeler que CareNet est déjà utilisé pour l'échange de données entre les hôpitaux et les organismes assureurs conformément à l'autorisation accordée par la délibération n° 97/48 du 3 juillet 1997 et que ces données[3] bénéficient dans ce contexte de force probante (voir l'avis n° 01/011 du 11 décembre 2001). Ce même réseau CareNet est maintenant également utilisé pour l'échange de données entre les infirmiers et les organismes assureurs, à partir de la passerelle client MyCareNet jusqu'à la passerelle serveur des organismes assureurs.

---

[2] En cas d'un S2S (relation "système à système"): la connexion entre l'application du producteur de logiciels et MyCareNet. Dans le cas de l'application portail: la connexion entre le navigateur sur l'ordinateur de l'utilisateur et MyCareNet.

[3] Certaines données nécessaires à l'exécution des obligations des organismes assureurs en ce qui concerne le régime du tiers payant et à l'exécution correcte des hospitalisations.

Il est souhaitable de suivre l'évolution des algorithmes cryptographiques et de choisir des algorithmes standard. A cet égard, l'utilisation d'algorithmes tels que AES (avec une force de clé minimale de 128 bits) est fortement recommandée (plutôt que TDES). Par contre, l'utilisation de l'algorithme de hachage SHA1 à moyen terme est fortement déconseillée.

Dans le souci de cohérence entre les mesures techniques prévues, il y a lieu de préciser les mesures de sécurité physiques et logiques applicables aux ordinateurs et aux passerelles clients / serveurs qui assureront, d'une part, le traitement des messages et, d'autre part, la conservation des clés publiques et privées (*key management*). Une technique d'authentification stricte en combinaison avec des mesures de sécurité physiques et un accès limité sont recommandés.

7. Non-répudiation d'envoi et de réception

Dans le cadre de MyCareNet, les services de sécurité "intégrité des données" et "non-répudiation d'origine" sont réalisés conformément aux dispositions des autorisations n° 07/003 du 9 janvier 2007 et n° 07/070 du 4 décembre 2007. L'expéditeur (infirmier ou mandataire) signe les documents (ou l'ensemble des documents dans le cas de plusieurs documents et non chaque document individuel) au moyen de sa carte d'identité électronique: ceci garantit l'origine du message et sa non-falsification. A la réception du message, MyCareNet enverra un numéro d'audit à l'expéditeur. Etant donné qu'il n'existe pas de relation univoque entre le numéro d'audit et le message envoyé, le service *non-répudiation d'envoi et de réception* n'est pas implémenté. MyCareNet transmet le message ainsi que le numéro d'audit précité aux organismes assureurs via le réseau CareNet existant. Le lien entre le message et le numéro d'audit créé doit être conservé de manière sécurisée, à la fois par l'expéditeur, par la plateforme MyCareNet et par les organismes assureurs.

A cet égard, il y a lieu de remarquer que dans le cas de CareNet (le protocole établi le 19 avril 2001), les services de sécurité *intégrité des données* et *non-répudiation d'envoi et de réception* sont effectivement réalisés au moyen d'une combinaison de la signature numérique et de l'accusé de réception (*return receipt*). La présomption irréfutable que le message a été reçu / envoyé est garantie par un accusé de réception obligatoire, qui est transmis par l'organisme assureur et également pourvu d'une signature électronique: cet accusé de réception contient la signature du message envoyé et un numéro de ticket, l'ensemble étant signé par le destinataire (à savoir la passerelle serveur de l'organisme assureur). Cet accusé de réception permet à l'expéditeur du message de vérifier si le destinataire du message a bien reçu le message avec la garantie de l'intégrité du message.

8. Procédure Back Office et sécurité

Etant donné l'hétérogénéité des différents "back offices", il est difficile de décrire une procédure commune d'archivage. Il est également difficile de spécifier les mesures de sécurité spécifiques pour tous les points finaux (ordinateurs des

dispensateurs de soins, passerelles serveurs des organismes assureurs, …). Néanmoins, des mesures de sécurité adéquates doivent être prévues. Dans le cadre de CareNet, un contrôle est prévu sur base d'une check-list. Cette check-list permet de vérifier si les procédures « back offices » répondent aux exigences (en matière de sécurité). Dans le cadre de MyCareNet, un tel contrôle (sur base d'une check-list) n'est pas prévu.

Il est souhaitable que les recommandations suivantes soient respectées au niveau des points finaux de MyCareNet:

- Conformité avec les diverses exigences au moyen d'une check-list, par analogie avec CareNet (exigences de sécurité, description de la procédure d'archivage, ...).
- Les ordinateurs du dispensateur de soins (ou de son mandataire) doivent répondre aux exigences minimales en matière de sécurité (anti-virus, firewall, patch management, …). Par exemple, les mesures de sécurité figurant dans les directives (*policy*) rédigées par le groupe de travail Sécurité de l'information (voir infra).
- Il est proposé d'organiser, à intervalles réguliers et selon des modalités à déterminer par l'Institut national d'assurance maladie-invalidité, un audit relatif à la procédure d'archivage. Un tel audit - à exécuter par une instance neutre - peut en effet constituer un outil pour le conseiller en sécurité.

Le Comité sectoriel attire l'attention sur la nécessité pour les institutions et entités concernées d'appliquer les règles formulées par le groupe de travail Sécurité de l'information dans la *policy* "Politique de protection des postes de travail" lors de l'utilisation d'un ordinateur (fixe ou portable).

Le Comité sectoriel attire en outre l'attention sur la nécessité pour les institutions et entités concernées d'appliquer les règles formulées par le groupe de travail Sécurité de l'information dans la *policy* "Politique de sécurité PC portable" lors de l'utilisation d'un ordinateur portable.

L'attention est également attirée sur la nécessité pour l'Institut national d'assurance maladie-invalidité d'informer la Banque Carrefour de la sécurité sociale et le Comité sectoriel de la sécurité sociale et de la santé en cas d'évolution vers de nouvelles techniques ou procédures et de leur fournir une documentation à ce propos. Il serait indiqué que le Comité sectoriel puisse (à long terme) soumettre ce protocole à un nouvel examen en fonction des modifications apportées.

Par rapport à l'article 6 du protocole soumis, il y a lieu de préciser les données à archiver, à la fois auprès des organismes assureurs, auprès de la plateforme MyCareNet et dans les systèmes informatiques des dispensateurs de soins.

9. Loggings

En cas d'interactions de système à système, l'infirmier utilise une application d'un producteur de logiciels. Outre les loggings réalisés par MyCareNet et les organismes assureurs, il est également demandé au fournisseur de l'application de fournir un système de loggings. L'accès aux loggings doit être limité 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. En ce qui concerne l'accès aux loggings, il y a lieu de prévoir également un système solide d'identification et d'authentification, par exemple au moyen de la carte d'identité électronique. Des conseillers en sécurité ont été désignés pour les organismes assureurs et MyCareNet. Les loggings des applications des producteurs de logiciels doivent par ailleurs être mis à la disposition du Comité sectoriel.

Les conseillers en sécurité des institutions ou entités concernées veillent à l'existence de fichiers de loggings et à la consultation correcte de ceux-ci, conformément aux autorisations du Comité sectoriel de la sécurité sociale et de la santé (délibérations n° 07/003 du 9 janvier 2007 et n° 07/070 du 4 décembre 2007).

Ces loggings doivent permettre au Comité sectoriel de la sécurité sociale et de la santé de remplir sa mission de contrôle. Ils devront être conservés pendant au moins dix ans.

Par ces motifs,

la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé

émet un avis favorable à la condition que les recommandations mentionnées au point 8 soient mises en œuvre dans un délai de six mois. L'Institut national d'assurance maladie-invalidité est tenu d'informer le Comité sectoriel de la sécurité sociale et de la santé à ce sujet.

Les recommandations suivantes doivent donc être respectées au niveau des points finaux de MyCareNet:

- Conformité avec les diverses exigences au moyen d'une check-list, par analogie avec CareNet (exigences de sécurité, description de la procédure d'archivage, ...).

- Les ordinateurs du dispensateur de soins (ou de son mandataire) doivent répondre aux exigences minimales en matière de sécurité (anti-virus, firewall, patch management, …). Par exemple, les mesures de sécurité figurant dans les directives (*policy*) rédigées par le groupe de travail Sécurité de l'information.

- Il est proposé d'organiser, à intervalles réguliers et selon des modalités à déterminer par l'Institut national d'assurance maladie-invalidité, un audit relatif à la procédure d'archivage, à exécuter par une instance neutre.

Yves ROGER
Président