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

CSSS/10/026

DÉLIBÉRATION N° 09/017 DU 17 MARS 2009, MODIFIÉE LE 19 MAI 2009 ET LE 16 FÉVRIER 2010, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL CODÉES PAR DES HÔPITAUX AU SERVICE PUBLIC FÉDÉRAL SANTÉ PUBLIQUE, SÉCURITÉ DE LA CHAÎNE ALIMENTAIRE ET ENVIRONNEMENT DANS LE CADRE D'UN PROJET PILOTE CONCERNANT L'ENREGISTREMENT D'URGENCES

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

Vu la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*;

Vu la demande du Ministre des Affaires sociales et de la Santé publique du 14 janvier 2009;

Vu le rapport d'auditorat de la plate-forme eHealth du 20 janvier 2009;

Vu le rapport de monsieur Yves Roger.

1. OBJET DE LA DEMANDE

1.1. Le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement souhaite, dans le cadre d'un projet pilote concernant l'enregistrement d'urgences, obtenir de la part des deux hôpitaux participants la communication de certaines données à caractère personnel codées. Ces données à caractère personnel codées devraient lui permettre de mieux comprendre le fonctionnement des services d'urgence afin de pouvoir prendre les mesures adéquates en cas de crise ou lors d'une situation potentiellement dangereuse.

L'enregistrement serait utile en cas de situation de crise nationale (une pandémie de grippe aviaire, une catastrophe nucléaire, un cas de bioterrorisme,...), de crise régionale (un tremblement de terre, de graves inondations, une pollution atmosphérique,…) ou de crise ponctuelle (une intoxication alimentaire liée à certains aliments industriels, une catastrophe aérienne,...), afin de limiter au maximum les effets de cette crise et même dans certains cas de prévenir certains de ces effets (par exemple: perte de temps dans le traitement des patients suite à une mauvaise orientation vers les hôpitaux, alerte des réseaux de soins à propos d'une menace potentielle,...). L'enregistrement permettrait non seulement en situation de crise mais aussi dans la pratique régulière, via une évaluation permanente de l'utilisation des ressources disponibles, de prendre les mesures de correction nécessaires de façon appropriée, tant au niveau de l'hôpital qu'au niveau régional et national, et de pouvoir rapidement évaluer l'effet de ces mesures.

Les données à caractère personnel en question seraient recueillies par les hôpitaux participants au moyen de leur « *Hospital Information System* » (HIS) et ensuite - après un double chiffrement réversible (voir infra) du « numéro d'identification local du patient » (NILP) en « numéro d'identification codé du patient » (NICP) - à l'aide d'un service web spécifique sécurisé (UREG) et sous la surveillance d'un médecin, ces données seraient mises à la disposition du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement, qui pourrait alors procéder à leur enregistrement dans la banque de données à caractère personnel (UREG) prévue à cet effet.

Le service web en question serait accessible à partir du site web du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement. Chaque hôpital aurait uniquement accès à ses propres données à caractère personnel. Les personnes concernées du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement, par contre, auraient accès à toutes les données à caractère personnel codées.

1.2. Outre l'identification de l'hôpital (à l'aide du numéro d'agréation attribué par l'Institut national d'assurance maladie-invalidité, du numéro d'identification du site et d'une description des ressources techniques), il s'agit des données à caractère personnel codées suivantes relatives aux patients concernés, identifiés quant à eux à l'aide du NICP (un numéro d'ordre unique dénué de sens).

Caractéristiques personnelles: l'année de naissance, le sexe, le code postal du lieu de résidence, le code pays du lieu de résidence, le code nationalité et le code assurabilité.

Données à caractère personnel relatives à l'admission au service des urgences : la date et l'heure de l'admission, le type d'admission, la localisation avant l'admission, le canal via lequel l'intéressé est arrivé au service des urgences, le type de moyen de transport et l'identification du moyen de transport.

Données à caractère personnel relatives à la sortie du service des urgences : la date et l'heure de la sortie, le type de sortie, la destination après la sortie et le type de suivi.

Données à caractère personnel relatives à la problématique : le motif du contact avec le service des urgences, la nature du problème (indication du groupe de pathologie dominant) (un problème traumatologique, médical, chirurgical, gynécologique, psychiatrique ou social, un cas d'intoxication, un contact en vue d'un contrôle ou un contact en vue de l'obtention d'un certificat ou d'une prescription), le diagnostic principal et le diagnostic secondaire (groupes globaux : cardiologie, dermatologie, neurologie,…), les actes diagnostiques et thérapeutiques (prise de sang, radiographie, ECG, …), données à caractère personnel relatives aux cas d'intoxication au monoxyde de carbone (type d'intoxication, durée estimée de l'exposition, première dose de monoxyde de carbone, oxygénation, présence d'un détecteur de monoxyde de carbone, lieu de l'intoxication et cause probable), le type d'accident et le type de fracture.

1.3. Exceptionnellement, plus précisément lorsque le contrôle des données à caractère personnel fait apparaître un écart statistique anormal, le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement aurait cependant besoin de données à caractère personnel supplémentaires afin de retrouver les causes de l'écart statistique anormal constaté.

Exemples: en cas d'augmentation de la durée de séjour au service des urgences, le motif peut être demandé ; en cas d'augmentation du nombre de transferts entre hôpitaux, la distance entre les hôpitaux en question peut être vérifiée ; en hiver, le nombre de sans-abri admis peut être demandé, …

La liste des données à caractère personnel supplémentaires serait chaque fois établie, à la demande du Ministre de la Santé publique ou du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement, par deux médecins spécialisés en médecine d'urgence et faisant partie d'une commission *ad hoc,* composée de représentants du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement et de quatre médecins spécialisés en médecine d'urgence.

1.4. Un premier chiffrement du NILP est effectué dans le HIS de l'hôpital (*ce chiffrement est réversible étant donné qu'il doit toujours être possible de retourner au NILP initial à partir du NILP chiffré une première fois*), un deuxième chiffrement est effectué par le service web UREG du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement avant l'enregistrement des données à caractère personnel dans la banque de données à caractère personnel UREG (*ce chiffrement est réversible étant donné qu'il doit toujours être possible de retourner au NILP chiffré une première fois à partir du NICP*). Les utilisateurs finaux auprès du Service public fédéral Santé publique,

Sécurité de la chaîne alimentaire et Environnement ne disposent donc pas du NILP mais du NICP.

Les données à caractère personnel communiquées sont en partie de nature dynamique et doivent donc pouvoir être modifiées. Dans ce cas, l'utilisateur au sein de l'hôpital demandera, au moyen du HIS (*premier chiffrement du NILP*) et du service web UREG sécurisé du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement (*deuxième chiffrement du NILP en NICP*), la dernière version des données à caractère personnel (c'est-à-dire les données à caractère personnel initialement communiquées par l'hôpital).

Les données à caractère personnel seraient recherchées par le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement, à l'aide du NICP, dans la banque de données à caractère personnel UREG, après quoi le service web UREG convertirait à nouveau le NICP en NILP chiffré une fois, qui à son tour serait converti par l'hôpital en NILP. Dans l'hôpital, les données à caractère personnel pourraient alors être modifiées ou complétées pour être ensuite transmises à nouveau au Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement (selon la méthode décrite ci-dessus, le NILP étant chiffré deux fois).

Le NILP est dès lors uniquement connu par l'hôpital. Avant la communication des données à caractère personnel, le NILP est chiffré une première fois par l'hôpital. Le service web UREG assure ensuite un deuxième chiffrement.

Le Comité sectoriel de la sécurité sociale et de la santé est d'avis que le deuxième chiffrement doit en principe être réalisé par une organisation intermédiaire au sens de l'article 1er, 6° de l'arrêté royal du 13 février 2001 *portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, telle que la plate-forme eHealth instituée par la loi du 21 août 2008. Provisoirement, cette mission peut être confiée au Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement. Le Comité sectoriel de la sécurité sociale et de la santé demande cependant au SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement de prendre les mesures nécessaires de sorte que le deuxième chiffrement puisse être effectué par une organisation intermédiaire à partir du 1er septembre 2010.

Ainsi, pendant la phase de test du projet et au plus tard jusqu'au 28 février 2010, le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement pourra exécuter lui-même le deuxième chiffrement des données à caractère personnel. Pour la deuxième phase du projet et en tout cas à partir du 1er septembre 2010, il faudra obligatoirement faire appel aux services d'une organisation intermédiaire.

2. EXAMEN DE LA DEMANDE

2.1. En vertu de l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, la section santé du Comité sectoriel de la sécurité sociale et de la santé visée à l'article 37 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale* est en principe compétente pour l'octroi d'une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé au sens de la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.*

Le point 3° précité a été inséré à l'article 42, § 2, de la loi du 13 décembre 2006 par l'article 70 de la loi du 1er mars 2007 *portant des dispositions diverses (III)*. L'article 71 de la même loi du 1er mars 2007 dispose cependant que le Roi détermine la date et les modalités d'entrée en vigueur du point 3°, ce qui n'a pour le moment pas encore eu lieu.

Ceci signifie que l'échange précité de données à caractère personnel entre les hôpitaux concernés et le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement ne requiert, pour l'instant, pas d'autorisation de la section santé, sauf si l'échange est opéré à l'intervention de la plate-forme eHealth.

2.2. La section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé ne doit pas non plus accorder d'autorisation en la matière. En effet, dans le cas présent, il ne s'agit pas, comme requis à l'article 15, § 1er, de la loi du 15 janvier 1990, de la communication de données à caractère personnel par une institution de sécurité sociale.

Ni les hôpitaux en question, ni le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement ne peuvent être considérés comme des institutions de sécurité sociale au sens de l'article 2, alinéa 1er, 2°, de la loi du 15 janvier 1990.

2.3. Nonobstant ce qui précède, la section santé du Comité sectoriel de la sécurité sociale et de la santé estime néanmoins qu'il peut se prononcer sur la communication précitée de données à caractère personnel.

En effet, l'article 46, § 2, de la loi du 15 janvier 1990 dispose que la section santé du Comité sectoriel de la sécurité sociale et de la santé est chargée de veiller au respect des dispositions fixées par ou en vertu de la loi visant à la protection de la vie privée à l'égard des traitements de données à caractère personnel relatives à la santé. A cet effet, elle peut formuler toutes recommandations qu'elle juge utiles et aider à la solution de tout problème de principe ou de tout litige.

2.4. Le traitement de données à caractère personnel relatives à la santé est en principe interdit, conformément à l'article 7, § 1er, de la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.*

En vertu de l'article 7, § 2, d), de la même loi cette interdiction ne s'applique toutefois pas lorsque le traitement est nécessaire à la promotion et à la protection de la santé publique. Le traitement des données à caractère personnel codées précitées par le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement semble dès lors justifié.

2.5. La communication de données à caractère personnel codées par les hôpitaux participants au Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement poursuit une finalité légitime. En cas de crise ou lors d'une situation potentiellement dangereuse, le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement doit pouvoir disposer rapidement d'informations relatives aux services d'urgence. Ce n'est qu'ainsi qu'il sera en mesure de prendre rapidement des mesures réactives ou préventives.

Pour l'accomplissement de sa mission, le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement doit pouvoir disposer de données à caractère personnel codées relatives aux patients des services d'urgence des hôpitaux participants.

La communication de données purement anonymes ne pourrait suffire étant donné que des analyses doivent pouvoir être réalisées concernant les diverses urgences qui se sont produites dans l'hôpital concerné.

Le Comité sectoriel de la sécurité sociale et de la santé est d'avis que les données à caractère personnel dans le chef du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement sont effectivement de nature codée.

D'une part, le numéro d'identification utilisé par l'hôpital pour l'identification du patient est chiffré une première fois à la source, c'est-à-dire par l'hôpital. Le service web employé assure ensuite un deuxième chiffrement du numéro d'identification.

D'autre part, le nombre de caractéristiques personnelles, c'est-à-dire les données à caractère personnel qui comportent le plus grand risque de réidentification du patient, est limité (année de naissance, sexe, code postal, code pays, code nationalité).

Le Comité sectoriel de la sécurité sociale et de la santé constate que la date et l'heure exactes sont demandées à la fois pour l'admission aux urgences et pour la sortie du service des urgences. Bien que le Comité sectoriel recommande généralement de communiquer les dates par un renvoi à la période dans laquelle elles tombent, il reconnaît en l'occurrence l'utilité d'une communication précise.

Le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement doit en effet connaître la capacité exacte et la charge réelle des divers services d'urgence.

Sans préjudice des constatations précitées, le Comité sectoriel rappelle cependant que les destinataires des données à caractère personnel codées ne peuvent en aucun cas essayer de retrouver l'identité des personnes concernées.

2.6. Pour l'identification des utilisateurs de l'application et l'authentification de leur identité, il est fait appel aux services du Service public fédéral Technologie de l'information et de la communication.

Le Service public fédéral Technologie de l'information et de la communication a été autorisé, par la délibération n° 26/2005 du 6 juillet 2005 de la Commission de la protection de la vie privée *loco* le Comité sectoriel du Registre national, à obtenir accès au registre national et à utiliser le numéro d'identification du registre national en vue de la gestion des utilisateurs.

A cette occasion, il avait déjà été prévu que le Service public fédéral Technologie de l'information et de la communication mettrait son système de gestion des utilisateurs également à la disposition notamment d'autres institutions belges publiques ou privées ayant besoin d'une gestion des utilisateurs sûre en vue de l'accomplissement de leurs tâches d'intérêt général.

L'accès à l'application interviendrait dans une première phase sur base d'une combinaison d'un user-id, mot de passe et token. Plus tard, la carte d'identité électronique serait employée.

Pour le volet enregistrement, il est fait usage du système « *Hospital Information System* » (HIS) qui est pourvu de sa propre gestion spécifique des utilisateurs et des accès pour régler les droits d'enregistrement au sein de l'hôpital. Pour la connexion entre le HIS et le service web, il est fait appel à une technologie S2S basée sur un certificat de protection (services web à sécurité « faible »). La plate-forme eHealth se chargerait de la gestion des certificats. Le Comité sectoriel de la sécurité sociale et de la santé prend acte du fait que le but est de faire appel à terme à la gestion intégrée des accès et des utilisateurs proposée par la plate-forme eHealth.

2.7. Le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement se charge par ailleurs de l'octroi de l'accès à l'application, d'une part, à ses propres utilisateurs (un nombre limité de collaborateurs au sein du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement qui sont associés au projet pilote concernant l'enregistrement d'urgences) et, d'autre part, aux hôpitaux participants (une vingtaine). Ces derniers se chargent de l'octroi de l'accès à l'application pour leurs collaborateurs.

2.8. Le Comité sectoriel de la sécurité sociale et de la santé est conscient du fait que la communication des données à caractère personnel mentionnées sous 1.2. donnera parfois lieu à une communication supplémentaire de données à caractère personnel qui ne peuvent pas être définies au préalable.

Il tient à souligner à cet égard que lors d'une éventuelle communication supplémentaire de données à caractère personnel, il convient de toujours tenir compte des principes prévus dans la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, en particulier du principe de proportionnalité, en vertu duquel des données à caractère personnel doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont communiquées.

La communication supplémentaire doit dès lors être limitée, d'une part, en ce qui concerne le nombre de personnes sur lesquelles portent les données à caractère personnel et, d'autre part, en ce qui concerne le nombre de données à caractère personnel. Lors de l'établissement de la liste des données à caractère personnel supplémentaires à communiquer, il convient également de ne jamais perdre de vue qu'elles ne peuvent pas avoir pour effet d'augmenter le risque de réidentification des personnes concernées.

Le Comité sectoriel de la sécurité sociale et de la santé souhaite, le cas échéant, être informé d'une telle communication supplémentaire.

2.9. La section santé du Comité sectoriel de la sécurité sociale et de la santé estime qu'à partir du 1er septembre 2010 le deuxième chiffrement du NILP doit être effectué par une organisation intermédiaire, telle que la plate-forme eHealth, et plus par le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement.

En tout état de cause, il y a lieu de prévoir déjà au sein du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement une séparation des fonctions entre, d'une part, les personnes chargées de la gestion du service web UREG et, d'autre part, les personnes chargées de la gestion de la banque de données à caractère personnel UREG.

Par ces motifs,

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

autorise les hôpitaux concernés à communiquer des données à caractère personnel codées, selon les modalités précitées, au Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement, en vue de la réalisation d'un projet pilote concernant l'enregistrement d'urgences.

Cette autorisation est octroyée jusqu'au 1er septembre 2010 inclus.

Yves ROGER
Président