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

CSSSS/13/042

**DÉLIBÉRATION N° 09/017 DU 17 MARS 2009, DERNIÈREMENT MODIFIÉE LE 22 JANVIER 2013, 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 délibération n° 09/017 du 17 mars 2009, modifiée le 19 mai 2009;

Vu la demande de modification;

Vu le rapport d'auditorat de la plate-forme eHealth du 14 janvier 2013;

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 (ci-après, le 'SPF Santé publique') 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 permettre au SPF Santé publique 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 codage 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 SPF Santé publique, qui pourrait alors procéder à leur enregistrement dans la banque de données à caractère personnel (UREG) prévue à cet effet.

Chaque hôpital a uniquement accès à ses propres données à caractère personnel. Les personnes concernées du SPF Santé publique, 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 mois de naissance, le sexe, le code postal du lieu de résidence, le code pays, l'indicateur de nationalité et le statut d'assurance.

*Données à caractère personnel relatives à l'admission au service des urgences* : la date et l'heure de l'inscription, le type d'inscription, le lieu avant l'inscription et la catégorie de l'instance qui a renvoyé l'intéressé au service des urgences.

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

*Données à caractère personnel relatives à la problématique* : le motif de l'inscription au service des urgences, les actes thérapeutiques, le type d'accident de la route et le triage.

**1.3.** Un premier codage du NILP est effectué dans le HIS de l'hôpital (*ce codage est réversible étant donné qu'il doit toujours être possible de retourner au NILP initial à partir du NILP codé une première fois*), un deuxième codage est effectué avant l'enregistrement des données à caractère personnel dans la banque de données à caractère personnel UREG. Pour ce codage, la plate-forme eHealth intervient en tant qu'organisation intermédiaire, en exécution de l'article 5, 8° de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, tel que demandé par le Comité sectoriel dans une version précédente de la présente délibération. Les utilisateurs finaux auprès du SPF Santé publique 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 codage du NILP*) et du service web UREG sécurisé du SPF Santé publique (*deuxième codage 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 SPF Santé publique, à l'aide du NICP, dans la banque de données à caractère personnel UREG, après quoi la plate-forme eHealth décoderait le NICP en NILP codé une fois, qui à son tour serait converti par l'hôpital même en NILP. Dans l'hôpital, les données à caractère personnel pourraient alors être modifiées ou complétées pour être ensuite transmises à nouveau au SPF Santé publique (selon la méthode décrite ci-dessus, le NILP étant codé deux fois).

Grâce à l'intervention de la plate-forme eHealth, le SPF Santé publique satisfait à la condition que le Comité sectoriel avait imposée dans une version précédente de cette délibération, à savoir la condition selon laquelle le deuxième codage devait 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.

## 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*.

Par ailleurs, 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.

**2.2.** 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 SPF Santé publique semble dès lors justifié.

**2.3.** La communication de données à caractère personnel codées par les hôpitaux participants au SPF Santé publique poursuit une finalité légitime. En cas de crise ou lors d'une situation potentiellement dangereuse, le SPF Santé publique 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 SPF Santé publique 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 est d'avis que les données à caractère personnel dans le chef du SPF Santé publique sont effectivement de nature codée.

D'une part, le numéro d'identification utilisé par l'hôpital pour l'identification du patient est codé une première fois à la source, c'est-à-dire par l'hôpital. Le service web employé assure ensuite un deuxième codage 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 et mois de naissance, sexe, code postal, code pays, code nationalité).

Le Comité sectoriel constate que la date et l'heure exactes sont demandées à la fois pour l'inscription 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 SPF Santé publique 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.

**2.4.** Les hôpitaux peuvent faire appel au service UREG sur l'eHealth ESB (Enterprise Service Bus), soit directement (moyennant l'authentification via un token: le eHealth Secure Token Service), soit via un hub[1]. Dans ce dernier cas, le hub se charge de l'authentification correcte de l'hôpital et de la sécurisation nécessaire de la communication entre le hub et le eHealth ESB. Le hub a une fonction purement technique (en tant que proxy pour les services UREG).

Le Comité sectoriel prend acte du fait que les données relatives à l'hôpital et les données à caractère personnel codées relatives à la santé, hormis le numéro d'identification à coder, sont chiffrées à l'aide de la clé publique avant qu'elles ne soient communiquées par l'hôpital concerné au SPF Santé publique par le biais du service UREG. Ceci garantit que seul le destinataire de l'information, à savoir le SPF Santé publique, puisse déchiffrer les données chiffrées, à l'exclusion de toute autre partie, y compris l'organisation intermédiaire à laquelle il est fait appel pour le codage des numéros d'identification.

**2.5.** Le SPF Santé publique 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 SPF Santé publique qui sont associés au projet pilote concernant l'enregistrement d'urgences) et, d'autre part, aux deux hôpitaux participants. Ces derniers se chargent de l'octroi de l'accès à l'application pour leurs collaborateurs.

[1] Un hub est un réseau de communication développé autour d'un ou plusieurs hôpitaux. À l'heure actuelle, il y a cinq hubs en Belgique.

**2.6.** Le Comité sectoriel souligne enfin que le SPF Santé publique doit prévoir 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.

La plate-forme eHealth, qui intervient comme organisation intermédiaire pour le codage des données à caractère personnel, est autorisée à conserver le lien entre le numéro d'identification réel et le numéro codé par la plate-forme eHealth et à procéder au décodage et ceci uniquement afin de permettre aux hôpitaux concernés de consulter les données à caractère personnel enregistrées par eux et de les adapter, le cas échéant.

Yves ROGER
Président