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

CSSS/11/072

DÉLIBÉRATION N° 11/047 DU 21 JUIN 2011 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 DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES AUX SERVICES D'URGENCES

La section santé du Comité sectoriel de la sécurité sociale et de la santé (dénommé ci-après « le Comité sectoriel »);

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 37;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*;

Vu la demande d'autorisation du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement du 16 mai 2011;

Vu le rapport d'auditorat du 1er juin 2011;

Vu le rapport de monsieur Yves Roger;

Émet, le 21 juin 2011, la délibération suivante:

I. OBJET DE LA DEMANDE

A. CONTEXTE

1. Dans le cadre d'un projet pilote d'enregistrement de données relatives aux services d'urgences, le Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement (dénommé ci-après « SPF Santé publique ») souhaite obtenir de la part des hôpitaux participants, la communication de certaines données à caractère personnel codées. Celles-ci lui permettront de mieux comprendre le fonctionnement des services d'urgence et de prendre les mesures adéquates en cas de crise ou lors d'une situation potentiellement dangereuse.

2. Le Comité sectoriel a déjà autorisé cette communication dans sa délibération n°09/017 du 17 mars 2009, modifiée le 19 mai 2009, 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[1].

   Cette autorisation n'a toutefois été octroyée que jusqu'au 1er mars 2010 inclus. D'où la présente demande.

B. OBJECTIFS DE L'ENREGISTREMENT

3. En cas de crise ou de situations potentiellement dangereuses, il est en effet nécessaire pour les autorités de pouvoir disposer rapidement de données relatives aux services d'urgence de manière à pouvoir prendre promptement les décisions (réactives ou préventives) qui s'imposent.

   Un tel enregistrement sera donc 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, ...).

4. L'enregistrement permettra, non seulement en situation de crise mais également 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.

[1] Délibération n°09/017 du 17 mars 2009, modifiée le 19 mai 2009, 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, disponible sur le site de la Commission de la protection de la vie privée http://www.privacycommission.be/fr/

C. ENREGISTREMENT DES DONNÉES À CARACTÈRE PERSONNEL

1° Les données à caractère personnel concernées

5. Les variables enregistrées concernent aussi bien la structure de l'hôpital que l'aspect médical, administratif et social des patients. Ainsi, outre l'identification de l'hôpital (à l'aide du numéro d'agrément de l'hôpital, du numéro de site et d'une description des moyens techniques), pour chaque patient concerné, les informations suivantes sont demandées:

- le numéro d'identification utilisé par l'hôpital pour identifier le patient (numéro d'identification local du patient, dénommé ci-après « NILP »). Celui-ci sera doublement codé (voir *infra*);

- l'année et le mois 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.

6. Exceptionnellement et plus précisément si le contrôle des données à caractère personnel fait apparaître une déviation statistique anormale, le SPF Santé publique souhaiterait disposer de données à caractère personnel *ad hoc* afin de retrouver les causes de l'écart constaté. En situation hivernale, il pourrait par exemple être demandé s'il y a une recrudescence d'admission de sans-abris. Le motif d'une augmentation de la durée de séjour au service des urgences pourrait par exemple être également demandé.

La liste de ces données à caractère personnel supplémentaires serait chaque fois établie, à la demande du Ministre de la Santé publique ou du SPF Santé publique, par deux médecins spécialistes en médecine d'urgence et faisant partie d'une commission *ad hoc*,

composée de représentants du SPF Santé publique et de quatre médecins spécialistes en médecine d'urgence.

2° Enregistrement des données à caractère personnel concernées

7. Les données à caractère personnel concernées sont introduites par les hôpitaux participants dans leur système d'information (*Hospital Information System* - HIS). Elles sont ensuite, après un double codage du NILP en numéro d'identification codé du patient (numéro d'ordre unique dénué de sens, dénommé ci-après « NICP »), mises à la disposition du SPF Santé publique à l'aide d'un service Web (UREG). Il pourra alors procéder à leur enregistrement dans la banque de données à caractère personnel prévue à cet effet.

Le service Web en question est accessible via le site Internet du SPF Santé publique. Chaque hôpital aura uniquement accès à ses propres données à caractère personnel. Les personnes concernées du SPF Santé publique auront, quant à elles, accès à toutes les données à caractère personnel codées enregistrées.

8. Comme indiqué *supra*, le numéro d'identification local du patient sera codé deux fois. Le NILP est, dans un premier temps, codé en NILCP (numéro d'identification local codé du patient) par l'hôpital lui-même. Le NILP et le NILCP ne sont donc connus que de l'hôpital.

Conformément à l'exigence posée par le Comité sectoriel dans sa délibération n°09/017 du 17 mars 2009, il est désormais fait appel aux services d'une organisation intermédiaire, à savoir la plate-forme eHealth instituée par la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*[2], pour exécuter le second codage du NILCP en NICP[3].

Les utilisateurs finaux auprès du SPF Santé Publique ne disposent dès lors que du NICP.

9. Les hôpitaux associés au projet pilote sont identifiés via la gestion des utilisateurs et des accès de la plate-forme eHealth et sont authentifiés à l'aide d'un certificat eHealth. Par sa délibération n° 09/008 du 20 janvier 2009, le Comité sectoriel a accordé une autorisation pour l'application de la gestion intégrée des utilisateurs et des accès par la plate-forme eHealth.

Les hôpitaux associés au projet pilote sont responsables de l'octroi de droits d'accès à leurs propres collaborateurs et de leur identification et authentification conformément aux méthodes applicables au sein des hôpitaux concernés.

Le SPF Santé publique se charge de l'octroi de l'accès aux données pour ses propres utilisateurs (un nombre limité de collaborateurs au sein du SPF Santé publique qui sont associés au présent projet pilote).

---

[2] Loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*, *M.B.*, 13 novembre 2008, p. 54454.

[3] Pour rappel, la délibération initiale prévoyait que provisoirement cette mission pouvait être confiée au SPF Santé publique.

2. COMPÉTENCE

10. En vertu de l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*[4], la section santé du comité sectoriel de la sécurité sociale et de la santé est en principe compétente pour l'octroi d'une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé.

11. L'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth* dispose que toute communication de données à caractère personnel par ou à la plate-forme eHealth requiert une autorisation de principe de la section santé du comité sectoriel de la sécurité sociale et de la santé, sauf dans quelques cas exceptionnels.

12. Conformément à l'article 5, 8°, de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*, l'intervention de la plate-forme eHealth en tant qu'organisation intermédiaire pour le couplage et le codage de données à caractère personnel et la conservation du lien entre le numéro d'identification réel et le numéro codé requiert l'autorisation du Comité sectoriel.

13. Le Comité sectoriel s'estime dès lors compétent pour se prononcer sur la présente demande d'autorisation.

3. EXAMEN DE LA DEMANDE

A. LÉGITIMITÉ

14. Le traitement de données à caractère personnel relatives à la santé est en principe interdit, et ce conformément au prescrit de 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 personne* (dénommée ci-après la « LVP »)[5].

15. L'interdiction posée ne s'applique toutefois pas lorsque, en autres, le traitement est nécessaire à la promotion et à la protection de la santé publique[6]. Dans le cas présent, le traitement des données à caractère personnel codées semble dès lors justifié.

B. FINALITÉ

16. L'article 4, § 1er, 2°, de la LVP n'autorise le traitement de données à caractère personnel que pour des finalités déterminées, explicites et légitimes.

17. La communication de données à caractère personnel codées par les hôpitaux participants au SPF Santé publique poursuit bel et bien une finalité légitime. En cas de crise ou lors d'une situation potentiellement dangereuse, celui-ci doit pouvoir disposer rapidement

[4] Loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, *M.B.*, 22 décembre 2006, p. 73782.
[5] Loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, *M.B.*, 18 mars 1993, p. 05801.
[6] Article 7, § 2, d).

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.

C. PROPORTIONNALITÉ

18. L'article 4, § 1er, 3°, de la LVP dispose que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

19. 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.

20. 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.

21. Comme indiqué *supra*, le NILP sera codé une première fois à la source, c'est-à-dire par l'hôpital, et le NILP codé, à savoir le NILCP, sera codé une deuxième fois par la plate-forme eHealth.

22. Par ailleurs, 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).

23. S'agissant de la date et l'heure exactes, celles-ci 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'espèce 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.

24. À la lumière de ce qui précède, le Comité sectoriel estime que les données précitées peuvent être considérées comme adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues.

25. Le Comité sectoriel est conscient du fait que la communication des données à caractère personnel mentionnées *supra* 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 LVP, 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.

26. 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.

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

D. TRANSPARENCE

28. L'article 9, § 2, de la LVP dispose que si les données à caractère personnel ne sont pas obtenues auprès de la personne concernée, le responsable du traitement doit, au plus tard au moment de la première communication de données, fournir à la personne concernée toute une série d'informations (le nom et l'adresse du responsable du traitement, les finalités du traitement,…).

29. Le responsable du traitement est toutefois dispensé de fournir ces informations lorsque « l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés »[7]. Dans le cas présent, le Comité sectoriel considère que les efforts nécessaires qui devront être fournis par le SPF Santé publique peuvent être qualifiés de disproportionnés compte tenu du nombre de patients pouvant être impliqués dans ce projet pilote (environ 120.000 patients par an) et de la finalité du projet.

30. Compte tenu de ce qui précède, le Comité sectoriel estime que l'exception prévue à l'article 9, § 2, al. 2, est dès lors rencontrée.

E. MESURES DE SÉCURITÉ

31. Conformément à l'article 7, § 4, de la LVP, le traitement de données à caractère personnel relatives à la santé peut uniquement être effectué sous la surveillance et la responsabilité d'un professionnel des soins de santé.

32. Même si cela n'est pas strictement requis par la LVP, le Comité sectoriel estime qu'il est préférable de traiter de telles données sous la responsabilité d'un médecin[8]. Ce qui est le cas en l'espèce.

33. Le Comité sectoriel rappelle que lors du traitement de données à caractère personnel, le professionnel des soins de santé ainsi que ses préposés ou mandataires sont soumis au secret[9].

34. Conformément à l'article 16, § 4, de la LVP, le SPF Santé publique doit prendre toutes les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel. Ces mesures devront assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraînent

[7] Art. 9, § 2, de la LVP.
[8] Le Comité sectoriel a formulé cette préférence dans sa délibération n°07/034 du 4 septembre 2007 relative à la communication de données à caractère personnel au Centre fédéral d'expertise des soins de santé en vue de l'étude 2007-16-HSR « étude des mécanismes de financement possibles pour l'hôpital de jour gériatrique ».
[9] Art. 7, § 4, de la LVP.

l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

35. Afin d'assurer la confidentialité et la sécurité du traitement des données, tout organisme qui conserve, traite ou communique des données à caractère personnel est tenu de prendre des mesures dans les dix domaines d'action liés à la sécurité de l'information suivants: politique de sécurité; désignation d'un conseiller en sécurité de l'information; organisation et aspects humains de la sécurité (engagement de confidentialité du personnel, informations et formations régulières du personnel sur le thème de la protection de la vie privée et sur les règles de sécurité); sécurité physique et de l'environnement; sécurisation des réseaux; sécurisation logique des accès et des réseaux; journalisation, traçage et analyse des accès; surveillance, revue et maintenance; système de gestion des incidents de sécurité et de la continuité (systèmes de tolérances de panne, de back up, …); documentation[10].

36. À condition qu'elles soient appliquées de manière correcte et intégrale, le Comité sectoriel estime que les mesures de sécurité précitées sont suffisantes et permettent de garantir la confidentialité et la sécurité du traitement de données à la lumière des dispositions de la LVP.

37. Le Comité sectoriel rappelle qu'il est interdit, conformément à l'article 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*[11], d'entreprendre toute action visant à convertir les données à caractère personnel codées qui ont été communiquées en données à caractère personnel non codées. Le non-respect de cette interdiction est assorti d'une amende variant de cent à cent mille euros en vertu de l'article 39, 1°, de la LVP. Le Comité sectoriel rappelle également qu'en cas de condamnation du chef d'infraction à l'article 39, le juge peut prononcer la confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction (fichiers manuels, disques et bandes magnétiques, …) ou ordonner l'effacement de ces données. Le juge peut également interdire de gérer, personnellement ou par personne interposée, et pour deux ans au maximum, tout traitement de données à caractère personnel[12].

F. INTERVENTION DE LA PLATE-FORME eHEALTH

38. La plate-forme eHealth est chargée du codage du NILCP.

39. En vertu 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*, la plate-forme eHealth peut, en tant qu'organisme intermédiaire, recueillir, agréger, coder ou anonymiser et mettre à disposition des données utiles à la connaissance, à la conception, à la gestion et à la prestation de soins de santé.

---

[10] Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel, document établi par la Commission de la protection de la vie privée disponibles à l'adresse: http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf

[11] 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*, *M.B.*, 13 mars 2001, p. 07839.

[12] Article 41 de la LVP.

40. La plate-forme eHealth peut uniquement réaliser cette mission à la demande de certaines instances, et par exemple à la demande d'un service public fédéral.

41. En outre, elle pourra conserver « les données à caractère personnel traitées dans le cadre de cette mission que pour la durée nécessaire à leur codification »[13]. La plate-forme eHealth ne pourra cependant « conserver le lien entre le numéro d'identification réel d'une personne concernée et le numéro d'identification codé qui lui a été attribué que si le destinataire des données à caractère personnel codées en fait la demande d'une façon motivée, et ce moyennant une autorisation du Comité sectoriel »[14]. A cet égard, le Comité sectoriel constate qu'il n'est pas nécessaire de conserver le lien dans le cadre du projet pilote.

Par ces motifs,

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

42. 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 de données à caractère personnel relatives aux services d'urgence.

Yves ROGER
Président

[13] Art. 5, 8°, de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth, M.B.*, 13 octobre 2008, p. 54454.
[14] *Ibidem*.