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

CSSS/11/

DÉLIBÉRATION N° 11/66 DU 20 SEPTEMBRE 2011 RELATIVE AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ PAR LE SERVICE PUBLIC FÉDÉRAL SANTÉ PUBLIQUE, SÉCURITÉ DE LA CHAÎNE ALIMENTAIRE ET ENVIRONNEMENT DANS LE CADRE DE L'APPLICATION SMUREG

le Comité sectoriel de la sécurité sociale et de la santé (dénommé ci-après : "le Comité sectoriel"),

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

Vu la demande visant à obtenir une autorisation du 10 août 2011;

Vu le rapport d'auditorat du 9 septembre 2011;

Vu le rapport de monsieur Yves Roger;

Émet, après délibération, la décision suivante, le 20 septembre 2011:

I. OBJET DE LA DEMANDE

1. L'application SMUREG permet aux fonctions SMUR (services médicaux d'urgence) et aux fonctions PIT (Paramedical Intervention Team) de remplir, pour chaque intervention réalisée, une fiche reprenant les détails de celle-ci ainsi que l'état médical du patient. Cette

fiche est ensuite mise à la disposition de l'hôpital qui a accueilli le patient. Il est également prévu que le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement (SPF Santé publique) reçoit quotidiennement une sélection de données à des fins statistiques, dans laquelle les données d'identification ont été supprimées.

2. La banque de données dans laquelle les fiches sont enregistrées, est gérée par le SPF Santé publique, plus précisément par la direction générale des Etablissements de soins.

3. Les données SMUR sont enregistrées pour tous les appels pour lesquels une intervention d'une fonction SMUR/PIT a eu lieu et cela à partir de la réception de l'appel jusqu'à l'arrivée éventuelle d'un patient accompagné par une fonction SMUR/PIT à l'hôpital et le retour de la fonction SMUR/PIT à sa base de fonctionnement ou l'appel pour une autre intervention. L'enregistrement des données des interventions SMUR a aussi trait au transport de patients entre les différents hôpitaux.

4. Chaque fiche comprend trois types de données:

   - caractéristiques: nom, prénom, adresse, date de naissance, sexe, médecin traitant, médecin référent;

   - données médicales constatées au cours de l'intervention: anamnèse, pupilles, Glasgow Coma Scale, antécédents, traitement usuel, fréquence respiratoire, évaluation clinique initiale, cause externe, rythme cardiaque, paramètres vitaux, examen clinique (ECG), diagnostic, pathologie, stabilisation, perfusion, thérapie, défibrillateur externe automatique avant l'arrivée du SMUR, monitoring, médicaments et doses, oxygénothérapie, actes de réanimation, évolution du patient et défibrillation, codes ICD-9-CM,

   - données relatives à l'intervention: coordonnées (nom et prénom) du médecin SMUR, des infirmiers SMUR, éventuellement des tiers ajoutés à l'équipe SMUR, et du médecin qui a pris en charge le patient aux urgences; numéro de l'intervention, numéro de la radio du SMUR ou du PIT, type d'appel, type de lieu d'intervention, adresse de l'intervention, date et heure de l'appel à la centrale 100, de l'appel du SMUR ou du PIT, de départ du SMUR ou du PIT, de l'arrivée sur place, du départ sur place, de l'arrivée à l'hôpital, de la libération du SMUR ou du PIT, type de transport, code de l'hôpital où le patient est admis, provenance de l'appel, type d'accompagnement.

5. Le traitement de données se déroule comme suit. Le SMUR/PIT introduit à l'aide de l'application SMUREG (service web ou application web) toutes les données relatives à l'intervention qui sont disponibles pour lui. Il peut également consulter les fiches déjà introduites par une des équipes de la fonction SMUR/PIT en question. La fonction SMUR/PIT a accès à trois types de données figurant sur les fiches en question (cf. supra).

6. Au moment où l'intervention est clôturée, la centrale 100 qui a reçu l'appel introduit les données de l'intervention dont elle dispose, dans le système à l'aide d'un service web. Ces données sont ensuite disponibles pour la fonction SMUR/PIT qui a réalisé l'intervention, ce qui permet de simplifier le remplissage de la fiche d'intervention.

7. L'hôpital consulte les fiches d'intervention au moyen de l'application web ou du service web. Seules les fiches des patients qui ont été admis sur un de ses sites, sont accessibles à l'hôpital. L'hôpital a également accès à trois types de données figurant sur les fiches en question (cf. supra).

8. Le SPF Santé publique reçoit quotidiennement, via un server FTP sécurisé, en exécution de l'arrêté royal du 27 avril 2007[1], une sélection de données d'intervention, plus précisément par intervention : le numéro de la fiche SMUR, le numéro de la radio du SMUR ou du PIT, le sexe du patient, l'année de naissance du patient, la commune du domicile principal du patient et, pour les étrangers, le pays du domicile principal ; le motif du transport du patient, la nature de la personne ou de l'organisation qui a demandé le transport, l'hôpital ou le site vers lequel le patient a été transporté, la justification du choix de l'hôpital où le patient a été transporté, l'accompagnement éventuel du patient jusqu'à l'hôpital par le SMUR, le cas échéant, la date de décès du patient.

   Si la nature du lieu où le patient se trouvait au moment de la nécessité de l'intervention est qualifiée de "privée" et que l'indicateur 'adresse du patient' est identique à l'indicateur 'adresse de l'intervention', seul le code postal du lieu d'intervention est communiqué au SPF Santé publique.

9. Dans le cadre de cette application et de ce service web, les services de base de la plate-forme eHealth sont utilisés: la gestion des utilisateurs et des accès permettant d'organiser les droits des différents types d'utilisateurs, le cryptage end-to-end pour toute communication de données d'identification et de données médicales et enfin, les hôpitaux sont authentifiés à l'aide de certificats eHealth.

II. COMPÉTENCE

10. Conformément à la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé,* 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* doit faire l'objet d'une autorisation du Comité sectoriel. Cependant, cette autorisation n'est pas requise, entre autres, lorsque la communication intervient entre professionnels des soins de santé qui sont soumis au secret professionnel et qui sont personnellement concernés par l'exécution d'actes de diagnostic, de prévention et de prestations de soins à l'égard d'un patient ; elle n'est pas non plus requise lorsque la communication est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.[2]

11. Vu le premier motif d'exception, la communication entre la fonction SMUR/PIT et l'hôpital ne requiert pas l'autorisation du Comité sectoriel. Il s'agit, en effet, de la communication entre professionnels des soins de santé dans le cadre du traitement du patient concerné. La communication des données SMUR sélectionnées, par l'hôpital au SPF Santé publique, fait

[1] Article 23 de l'arrêté royal du 27 avril 2007 déterminant les règles suivant lesquelles certaines données hospitalières doivent être communiquées au Ministre qui a la Santé publique dans ses attributions.
[2] Article 42, § 2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé.

aussi l'objet d'une dispense d'autorisation, étant donné que la communication est explicitement prévue dans l'arrêté royal précité du 27 avril 2007.

12. Bien que le SPF Santé publique n'ait pas un accès complet à l'ensemble des données d'identification, de santé et d'intervention que le SMUR communique à la banque de données SMUREG, il y a lieu de constater que la banque de données contenant des fiches est gérée par le SPF Santé publique et qu'il n'existe pas de cadre légal ou réglementaire explicite pour la communication de ces données en vue de la finalité en question, à savoir faciliter la transmission des données entre les fonctions SMUR/PIT et les hôpitaux. Le Comité sectoriel estime dès lors qu'il est compétent pour se prononcer sur la présente demande d'autorisation.

13. Enfin, conformément à la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*[3] , le Comité sectoriel est chargé 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. À cet effet, il peut formuler toutes recommandations qu'il juge utiles et aider à la solution de tout problème de principe ou de tout litige. Il estime dès lors qu'il est compétent pour se prononcer sur la demande d'autorisation.

III. EXAMEN DE LA DEMANDE

A. FINALITÉ

14. Les données à caractère personnel doivent être traitées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des attentes raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.

15. Le traitement de données à caractère personnel dans le cadre de l'application SMUREG vise, d'une part, à faciliter la communication entre les fonctions SMUR/PIT et les hôpitaux où les patients sont admis et, d'autre part, à organiser, sur la base de ces données, la communication des données SMUR dans le cadre de l'arrêté royal précité du 27 avril 2007. Le SPF Santé publique a pour mission générale de préparer et d'exécuter la politique au niveau de la santé publique (financement d'établissements de soins, organisation des professions des soins de santé, aide médicale urgente, organes de concertation). Le SPF prépare aussi l'exécution de la politique en matière de sécurité alimentaire, de protection de la santé publique et d'environnement. Le traitement de données à caractère personnel dans le cadre de l'application SMUREG vise dès lors des finalités déterminées, explicites et légitimes.

[3] Article 46, § 2, 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.

16. Le traitement de données à caractère personnel relatives à la santé est en principe interdit.[4] Cependant, cette interdiction ne s'applique pas, entre autres, lorsque le traitement est rendu obligatoire pour des motifs d'intérêt public importants par ou en vertu d'une loi, d'un décret ou d'une ordonnance, ce qui est en l'occurrence le cas vu l'arrêté royal précité du 27 avril 2011, et lorsque le traitement est nécessaire à la promotion et à la protection de la santé publique, dont notamment l'organisation de l'échange de données entre les fonctions SMUR/PIT et les hôpitaux[5].

B. PROPORTIONNALITÉ

17. Lors du traitement, les données à caractère personnel doivent être adéquates, pertinentes ou non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement[6].

18. Les données à caractère personnel échangées via l'application SMUREG entre les fonctions SMUR/PIT et les hôpitaux où le patient concerné est admis, concernent des données d'identification, des données médicales et des données relatives à l'intervention. Le Comité sectoriel constate que l'échange de ces données à l'aide de l'application est proportionnel par rapport à la finalité en question, à savoir le fonctionnement (la prestation de soins) et l'organisation des services concernés. Les données à caractère personnel qui sont communiquées au SPF Santé publique dans le cadre de l'arrêté royal précité du 27 avril 2007, sont explicitement mentionnées dans l'arrêté royal en question.

19. Les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.

20. En ce qui concerne la conservation de la sélection des données reçues par le SPF Santé publique, l'arrêté royal précité du 27 avril 2007 prévoit qu'elles sont conservées pendant un délai de 30 ans. La clé permettant de relier les données avec le dossier médical du patient dans l'hôpital concerné, à savoir le numéro d'enregistrement du patient et le numéro de séjour, est cependant détruite après un délai de 10 ans.

C. PRINCIPE DE TRANSPARENCE

21. Lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement doit, dès l'enregistrement des données, ou si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données,

[4] Article 7, § 1, de la LVP.
[5] Article 7, § 2, d) de la LVP.
[6] Article 4, § 1er, 3° de la LVP.

fournir en principe certaines informations[7]. Le responsable du traitement est cependant dispensé de cette obligation de notification lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.[8] Le SPF Santé publique est par conséquent dispensé de la notification aux personnes concernées, étant donné que les hôpitaux sont légalement obligés de communiquer les données SMUR au SPF Santé publique.

22. Le Comité sectoriel estime que le SPF Santé publique peut également être dispensé de la notification du traitement de données à caractère personnel dans le cadre de l'usage de l'application SMUREG par les fonctions SMUR/PIT et les hôpitaux en vue de l'échange de données à caractère personnel. En effet, comme décrit ci-après, il existe des garanties suffisantes au niveau de la gestion des utilisateurs et des accès permettant de garantir que les données à caractère personnel autres que celles dans le cadre de l'enregistrement SMUR obligatoire, sont uniquement accessibles aux fonctions SMUR/PIT et hôpitaux concernés.

D. SÉCURISATION ET CONFIDENTIALITÉ

23. Le traitement de données à caractère personnel relatives à la santé doit être effectué sous la surveillance et la responsabilité d'un professionnel des soins de santé. Même si ce n'est pas strictement requis, le Comité sectoriel estime qu'il est préférable de traiter de telles données sous la responsabilité d'un médecin[9]. L'identité du médecin responsable a été communiquée au Comité sectoriel.

24. Le responsable du traitement doit prendre les mesures techniques et organisationnelles appropriées qui sont nécessaires à la protection des données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel[10].

25. Afin de garantir que seules des personnes compétentes aient accès à l'application et à la banque de données de SMUREG, il est fait appel au service de base gestion des utilisateurs et des accès de la plate-forme eHealth. Conformément à la délibération n° 09/008 du 20 janvier 2009 du Comité sectoriel, le traitement de données à caractère personnel dans le cadre de ce service de base a fait l'objet d'une autorisation du Comité sectoriel[11].

---

[7] Article 9, § 2, alinéa premier, de la LVP.

[8] Article 9, § 2, alinéa deux, de la LVP.

[9] Le Comité sectoriel a formulé cette préférence dans le paragraphe 61 de la 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 ».

[10] Article 16 de la LVP.

[11] Délibération n°09/008 du 20 janvier 2009, modifiée le 16 mars 2010 et le 15 juin 2010, du Comité sectoriel de la sécurité sociale et de la santé relative à l'application de la gestion intégrée des utilisateurs et des accès par la plate-forme eHealth, lors de l'échange de données à caractère personnel.

26. Dans la pratique, l'application peut être utilisée par trois types d'organisation: un hôpital, un SMUR et un PIT. Par ailleurs, il existe quatre rôles différents: write (créer ou modifier une fiche), read (visualiser ou imprimer une fiche), download (télécharger une fiche) et admin (administration). Les rôles accessibles varient en fonction du type d'organisation. Un utilisateur au sein d'un SMUR/PIT possède les rôles suivants: read, write et download. Un utilisateur au sein d'un hôpital dispose des rôles suivants: read et download. L'administrateur de chaque hôpital, SMUR et PIT a accès à tous les quatre rôles.

27. Tout SMUR ou PIT dépend directement d'un seul hôpital, qui dispose éventuellement de plusieurs sites. Dans certains cas, un SMUR ou PIT peut également être lié à plusieurs hôpitaux. Dans le cadre de la gestion des utilisateurs et des accès, tout hôpital dispose d'un gestionnaire local qui est chargé de la gestion des accès. Le gestionnaire local peut attribuer et gérer les droits d'accès au sein de:
    - l'hôpital dont il est le gestionnaire local;
    - un ou plusieurs sites qui dépendent de l'hôpital;
    - la fonction SMUR ou PIT qui dépend de son hôpital.

    Le gestionnaire local doit ensuite déterminer pour tout utilisateur auquel il a conféré un accès dans le chef d'une organisation spécifique, son rôle dans l'application SMUREG.

28. Un utilisateur reçoit un accès via l'application web, s'il a été ajouté par un gestionnaire local à la gestion des utilisateurs et des accès dans le chef de l'organisation pour laquelle il souhaite s'authentifier. L'authentification de l'identité de l'utilisateur est réalisée au moyen de la carte d'identité électronique.

29. Dans la mesure où les fonctions SMUR et PIT ne disposent pas d'une infrastructure informatique logique et dépendent directement des hôpitaux dans lesquels ils sont situés, elles ne peuvent utiliser ce service web. Seuls les hôpitaux ont accès au service web, pour lequel ils doivent disposer d'un certificat eHealth. Une fois authentifiés, les hôpitaux peuvent exécuter toutes les opérations prévues pour les hôpitaux, mais aussi celles prévues pour les fonctions SMUR ou PIT pour lesquelles ils sont responsables. La vérification du lien de dépendance entre les fonctions SMUR et PIT d'une part et les hôpitaux d'autre part est réalisée dans la gestion des utilisateurs et des accès.

30. Enfin, les centrales 100 doivent s'authentifier à l'aide d'un certificat eHealth.

31. En ce qui concerne les autres mesures de sécurité, la banque de données même est chiffrée à l'aide d'un certificat selon la méthode AES (Advance Encryption Standard).

32. Dans le cadre de l'application web, outre l'identification au moyen de la carte d'identité électronique, l'échange entre les utilisateurs et l'application SMUREG intervient sur la base du protocole https qui garantit la confidentialité et l'intégrité des données échangées.

33. Dans le cadre du service web, outre l'authentification au moyen du certificat eHealth, l'échange entre le système de l'utilisateur et le système du serveur SMUREG intervient également sur la base d'un protocole https. Par ailleurs, toutes les requêtes qui contiennent des données à caractère personnel distinctives ou des données médicales, sont chiffrées à l'aide du service de base chiffrement end-to-end.

34. En ce qui concerne la communication de données dans le cadre de l'enregistrement SMUR obligatoire, les données entre l'application SMUREG et le SPF Santé publique sont transmises au travers d'un protocole SFTP (Secure file transfert protocol).

35. 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.

36. Le Comité sectoriel fait observer que conformément à l'article 458 du Code pénal, toutes les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où elles sont appelées à rendre témoignage en justice ou devant une commission d'enquête parlementaire et celui où la loi les oblige à faire connaître ces secrets, les auront révélés, seront punies d'un emprisonnement de huit jours à six mois et d'une amende de cinq cents cinquante euros à deux mille sept cents cinquante euros.

Par ces motifs,

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

autorise, aux conditions de la présente délibération, le traitement des données à caractère personnel par le service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement dans le cadre de l'application SMUREG.

Yves ROGER
Président