Comité sectoriel de la sécurité sociale et de la santé
Section "Santé"

CSSSS/14/114

DÉLIBÉRATION N° 14/059 DU 15 JUILLET 2014 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL CODÉES RELATIVES À LA SANTÉ DANS LE CADRE DU PROJET THALES

La section Santé du Comité sectoriel de la sécurité sociale et de la santé (dénommée 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 demande d'autorisation de Cegedim et vu les renseignements complémentaires;

Vu le rapport d'auditorat de la Plate-forme eHealth du 11 juin 2014;

Vu le rapport de monsieur Yves Roger;

Émet, après délibération, la décision suivante, le 15 juillet 2014:

I. OBJET DE LA DEMANDE

1. *Cegedim Strategic Data Belgium nv* (CSD), une succursale de Cegedim France, demande l'approbation du Comité sectoriel pour la communication de données à caractère personnel codées relatives à la santé par des prestataires de soins dans le cadre du projet Thales.

2. Le projet Thales vise à réaliser des recherches statistiques scientifiques qui sont basées sur des analyses longitudinales de pathologies, des profils de patients et des schémas thérapeutiques afin d'avoir une nouvelle vue actuelle sur certains problèmes médicaux et de santé liés à des facteurs socio-économiques et d'acquérir des connaissances approfondies de l'évolution épidémiologique de certaines pathologies. Les résultats des analyses seront commercialisés par CSD et vendus aux entreprises pharmaceutiques, à diverses autorités et au monde académique.

3. La réalisation de ce projet requiert la communication de données à caractère personnel codées relatives à la santé par un panel permanent de 300 médecins généralistes disposant du logiciel DMI Health One[1]. Les patients seront informés du traitement de données et auront la possibilité de s'opposer au traitement.

4. Les données suivantes seront recueillies de façon continue par patient :

- données du patient: l'identification du patient (à coder doublement, cf. infra) (qui est initialement attribuée par le logiciel Health One), la province, une des treize classes de profession, l'état civil, le nombre d'enfants
- identification du médecin codée
- antécédents (pathologies antérieures, pathologies familiales)
- allergies (type, date de début)
- données relatives aux consultations (raison, paramètres typiques tels que le poids, la tension)
- prescriptions
- traitement chronique
- renvois à un spécialiste
- vaccination
- traitements paramédicaux
- examens

5. Le flux de données se déroule comme suit :

a) Le médecin exporte les données des patients qui participent à la recherche
   - Le médecin a la possibilité de vérifier les données avant leur envoi
   - L'identification du patient est codée, une première fois, localement auprès du médecin

b) le logiciel en médecine générale envoie les données à Custodix (qui intervient en tant qu'organisation intermédiaire) par le biais d'un canal de communication authentifié et chiffré
   - les données sont filtrées quant à la présence de pathologies rares qui pourraient donner lieu à la réidentification indirecte

c) 2ième codage auprès de Custodix
   - l'identification codée du patient est codée une deuxième fois
   - l'identification du médecin est codée une première fois
   - il est vérifié si les données contiennent uniquement la liste fixée de données
   - Le contrôle sur le filtrage des données est effectué au niveau de l'organisation intermédiaire

d) Cegedim France reçoit les données à caractère personnel codées
   - les données à caractère personnel codées sont stockées de manière sécurisée en vue de leur traitement statistique scientifique ultérieur
   - les données seront supprimées après une période de trente ans

.

[1] Le producteur de logiciel en question est HDMP (Health One Data Management Partners). Le logiciel Health One a été enregistré en 2014 dans le cadre de la prime télématique. Cf. https://www.ehealth.fgov.be/fr/ehealth-en-pratique/homologation-des-logiciels-medicaux

6. Custodix n'a pas accès aux identifications du patient proprement dites. Custodix reçoit uniquement les pseudonymes du patient codés de façon irréversible. Le destinataire Cegedim n'a accès ni aux identifiants du patient, ni aux identifiants du médecin.

II. COMPÉTENCE

7. Conformément à l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, toute communication de données à caractère personnel relatives à la santé, sauf les exceptions prévues, requiert une autorisation de principe du Comité sectoriel.

8. Vu ce qui précède, la section Santé du Comité sectoriel de la sécurité sociale et de la santé estime qu'elle peut se prononcer sur la communication de données à caractère personnel relatives à la santé, telle que décrite dans la demande d'autorisation.

III. GÉNÉRALITÉS : LES CONDITIONS AUXQUELLES CHAQUE TRUSTED THIRD PARTY QUI CODE DES DONNÉES DOIT SATISFAIRE

9. Le Comité sectoriel souligne que la Commission de la protection de la vie privée a formulé dans sa recommandation n° 02/2011 du 4 mai 2011 quelques conditions pour la réalisation d'études basées sur des données à caractère personnel relatives à la santé issues de logiciels mis à la disposition d'un médecin. En outre, la Commission a précisé, dans sa recommandation n° 02/2010 du 31 mars 2010 par laquelle elle a donné un avis concernant les principes à respecter, le rôle qu'assurent les Trusted Third Parties (tierces parties de confiance) lors de l'échange de données, en ce qui concerne la protection de la vie privée.

10. Compte tenu des recommandations précitées, le Comité sectoriel estime qu'il est opportun de formuler, de manière générale, les conditions fonctionnelles, auxquelles chaque Trusted Third Party (TTP) qui code[2] des données à caractère personnel doit effectivement répondre:

- Le TTP doit être suffisamment indépendant vis-à-vis de l'émetteur (des émetteurs) des données à caractère personnel à coder et du (des) destinataire(s) des données à caractère personnel codées.

  La fonction de TTP doit être exercée par une organisation qui n'est, en aucune façon, liée à l'émetteur des données à caractère personnel non codées, ni au destinataire des données à caractère personnel codées.

- Si l'organisation qui intervient comme TTP est quand même liée d'une façon quelconque à l'émetteur ou au destinataire, le demandeur et le TTP doivent démontrer comment l'indépendance requise sera garantie.

[2] À l'exception de situations spécifiques qui sont réglées par ou en vertu de la loi, ces conditions s'appliquent tant aux TTP qui interviennent en tant qu'organisation intermédiaire au sens du chapitre II de l'arrêté royal du 13 février 2001, qu'aux TTP qui interviennent dans le codage en dehors du contexte du traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques.

- Le TTP doit effectuer le codage au moyen de techniques qui rendent raisonnablement impossible la conversion des données à caractère personnel codées en données à caractère personnel non codées. Ce codage doit en principe concerner toutes les personnes identifiées ou identifiables, c'est-à-dire tant les personnes auxquelles les données à caractère personnel relatives à la santé s'appliquent (ex. des patients) que les personnes qui fourniraient les données (ex. des prestataires de soins).

  Le TTP doit fournir une description technique et fonctionnelle du mode de codage.

  Le TTP doit au moins offrir les garanties suivantes:
  - Le codage des données à caractère personnel doit être réalisé en supprimant toutes les données à caractère personnel susceptibles de donner lieu à une identification directe (telles que le nom, le prénom, l'adresse, etc.) et en procédant au codage d'un numéro d'identification unique par personne concernée. Le codage du numéro d'identification doit être réalisé en transformant le numéro d'identification en un numéro codé au moyen d'une table de conversion ou d'une clé de codage dont la taille est suffisamment longue selon les normes de sécurité en vigueur.
  - Le TTP doit réaliser, pour tout projet, un codage unique, spécifique qui, sauf autorisation spécifique du Comité sectoriel, ne pourra être utilisé pour aucune autre mission de codage.
  - La communication, dans le cadre de la mission du TTP, de tout message comportant des données à caractère personnel au TTP ou par le TTP doit être chiffré, de sorte que seul le destinataire en question (le TTP ou le destinataire des données codées) soit en mesure de déchiffrer le message.
  - Pour autant que les messages communiqués au TTP contiennent des données à caractère personnel qui ne sont pas nécessaires à l'exécution des missions du TTP (codage ou analyse dite "small cell risk"), ces données à caractère personnel codées doivent être chiffrées par l'émetteur, de sorte que seul le destinataire des données à caractère personnel codées puisse les déchiffrer.
  - La clé de codage ou la table de conversion ne peut être conservée que durant le délai nécessaire à la mission de codage, conformément aux modalités telles que fixées dans l'autorisation du Comité sectoriel.

  Si le mode de codage s'écarte de ces modalités, le TTP doit prouver qu'il garantit un niveau de sécurité équivalent.

- Le TTP doit, en toute connaissance de cause, veiller à ce que l'ensemble de données à caractère personnel codées mis à la disposition ne permette raisonnablement pas une réidentification (il s'agit du "small cell risk"). Cela signifie que le TTP doit, le cas échéant, disposer de compétences spécifiques afin de pouvoir juger de la possibilité de réidentification au moyen de données à caractère personnel codées relatives à la santé.

  Le TTP doit fournir une description technique et fonctionnelle du mode d'exécution de l'analyse "small cell risk" et des traitements prévus pour éviter une réidentification à partir de la série de données à caractère personnel codées mise à la disposition.

Le TTP doit prouver qu'il dispose des compétences spécifiques pour la mission concrète.

- Le traitement de données à caractère personnel relatives à la santé par un TTP doit être effectué sous la surveillance et la responsabilité d'un professionnel des soins de santé, de préférence un médecin.

  L'identité et les qualifications pertinentes du médecin concerné doivent être communiquées. S'il ne s'agit pas d'un médecin, le TTP doit prouver que le professionnel des soins de santé proposé offre des garanties équivalentes.

- Le TTP doit désigner, en interne ou non, un conseiller en sécurité de l'information et en protection de la vie privée.

  Le TTP doit communiquer l'identité du conseiller en sécurité de l'information désigné et prouver qu'il dispose des qualifications nécessaires pour la mission.

- Le TTP doit veiller au respect correct de la législation en matière de protection de la vie privée et doit entreprendre toutes les actions nécessaires afin d'en assurer le respect.

  Le TTP doit déclarer sur l'honneur qu'il est satisfait à cette obligation.

- Le TTP ne peut pas utiliser les données qu'il a traitées dans le cadre de sa fonction de TTP pour des finalités autres que les finalités spécifiques qui lui ont été confiées.

  Le TTP doit déclarer sur l'honneur qu'il est satisfait à cette obligation.

- Le TTP 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.

- Le TTP et le demandeur doivent déclarer sur l'honneur qu'ils satisfont à cette obligation.

- Le TTP doit détruire l'ensemble des données que le responsable du traitement lui a communiquées dès qu'il a terminé sa mission de codage.

  Le TTP ne peut conserver le lien entre le numéro d'identification et le numéro codé (p.ex. pour des études longitudinales) que si cela est strictement nécessaire et moyennant l'autorisation du Comité sectoriel.

  Dans ce cas, le TTP doit prouver qu'il prend les mesures techniques et organisationnelles adéquates requises qui sont conformes aux mesures de référence établies par la Commission de la protection de la vie privée.

- Le TTP doit effectuer les traitements en toute transparence. Cela implique que:

- le responsable du traitement initial et/ou ultérieur reçoit de la part du TTP au moins des informations relatives au fonctionnement, aux conditions d'utilisation des services et à la portée de la responsabilité du TTP ;
- les personnes concernées doivent toujours savoir – sur la base des informations fournies par le TTP et par les responsables du traitement initial et/ou ultérieur – auprès de quelle personne ils peuvent exercer leur droit d'accès, de correction, de suppression ou de non-utilisation.

Le TTP et le demandeur doivent déclarer sur l'honneur qu'il est satisfait à cette obligation.

IV. EXAMEN DE LA DEMANDE

A. PRINCIPE DE FINALITÉ

11. En vertu de l'article 4, § 1er, 2°, 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 (dénommée ci-après 'loi relative à la vie privée') , le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes.

12. Le Comité sectoriel constate que le traitement de données visé a pour but d'effectuer des recherches scientifiques et/ou statistiques et des analyses, conformément aux principes précités. Le Comité sectoriel prend acte du fait que les résultats des recherches statistiques scientifiques seront commercialisés et mis sur le marché. Le traitement répond dès lors à des finalités déterminées, explicites et légitimes.

13. Le traitement de données à caractère personnel relatives à la santé est en principe interdit en vertu de l'article 7, § 1er, de la loi relative à la vie privée. Conformément à l'article 7, § 2, k), de cette loi, cette interdiction n'est toutefois pas d'application, lorsque le traitement de données à caractère personnel relatives à la santé est nécessaire à la recherche scientifique et est effectué aux conditions fixées par le Roi. Le demandeur est plus précisément tenu de respecter les dispositions de l'arrêté royal du 13 février 2001 portant exécution de la loi relative à la vie privée.

B. PRINCIPE DE PROPORTIONNALITÉ

14. L'article 4, § 1er, 3°, de la loi relative à la vie privée 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.

15. Compte tenu du fait que les analyses scientifiques et/ou statistiques visées concernent des études longitudinales qui suivent les mêmes patients à travers le temps. Par conséquent, il est nécessaire que le traitement soit effectué sur la base de données à caractère personnel codées.

16. Les résultats des analyses des données à caractère personnel codées seront utilisés pour déterminer la consommation de médicaments (ex. des schémas thérapeutiques selon l'indication, des fins de compatibilité – utilisation hors indication, ...) afin de pouvoir réaliser des recherches sur les résultats et des évaluations au niveau de l'économie de santé et de pouvoir estimer le déroulement naturel d'une pathologie.

L'incidence et la prévalence de maladies, ainsi que les profils des patients constituent une source d'information importante pour les entreprises pharmaceutiques et les autorités en vue du soutien de dossiers market access et pour le monde académique dans le cadre de projets de recherche.

17. Le projet Thales vise uniquement des recherches statistiques selon les conditions suivantes:

- les résultats seront, de manière standard,fournis au niveau belge (agrégation): jamais à niveau individuel; le dernier niveau de granulation possible est une distinction entre la Flandre, la Wallonie et Bruxelles
- les résultats seront extrapolés à l'univers: aucune partie de la banque de données ne sera transmise; elle ne contient pas de données individuelles.
- il s'agit de résultats statistiquement fiables: une analyse d'une pathologie n'est pas possible lorsque son incidence est trop faible (les maladies orphelines sont exclues de la banque de données), une segmentation n'est pas possible, lorsque son volume est trop faible.

18. Les analyses suivantes seront effectuées au moyen des données Thales:

- des études épidémiologiques: prévalence, incidence, comorbidités, facteurs de risque, évolution (analyse longitudinale), traité/non traité
- consommation de médicaments: schéma de traitement thérapeutique, dynamique du marché (changement du schéma du traitement à travers le temps), profils/segments de patients (âge, sexe, IMC, périmètre abdominal, fumer, alcool), profil clinique (événements cliniques, diagnostics, indications, symptômes, résultats de labo, comorbidités, facteurs de risque, renvoi à un spécialiste), prescriptions – taille du marché (données Rx, ATC, molécule, posologie, durée du traitement, schéma du traitement, évolution Rx), compatibilité: consommation de médicaments par indication, stratégies de gestion de maladie.

19. Compte tenu de ce qui précède, le Comité sectoriel considère les données à caractère personnel comme adéquates, pertinentes et non excessives.

20. Conformément à l'article 4, § 1er, 5°, de la loi relative à la vie privée, les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées au-delà du délai nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. Le demandeur prévoit que les données à caractère personnel codées seront conservées pendant une période de 30 ans. Vu le caractère longitudinal des analyses visées, ce délai de conservation est acceptable.

C. PRINCIPE DE TRANSPARENCE

21. Conformément à l'article 9 de la loi relative à la vie privée, le responsable du traitement est tenu de communiquer à la personne concernée certaines données.

22. Le Comité sectoriel constate que les intéressés sont informés par l'affichage d'un poster dans la salle d'attente des médecins concernés, par la mise à disposition de brochures et par les médecins concernés eux-mêmes. Le Comité sectoriel estime cependant qu'il est opportun que la communication renvoie également explicitement à la présente délibération.

23. Afin d'offrir aux patients concernés suffisamment de temps de réflexion, le Comité sectoriel estime que ceux-ci doivent pouvoir disposer d'une période de sept jours civils afin de communiquer leur éventuel refus à leur médecin.

D. MESURES DE SÉCURITÉ

24. Conformément à l'article 7, § 4, de la loi relative à la vie privée, 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. Même si cela n'est pas strictement requis par la loi relative à la vie privée, le Comité sectoriel estime qu'il est préférable de traiter ces données sous la responsabilité d'un médecin[3]. Ce qui est le cas en l'espèce. Le Comité sectoriel rappelle en outre 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.

25. Conformément à l'article 16, § 4, de la loi relative à la vie privée, le demandeur doit prendre toutes les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

26. Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est tenu de prendre des mesures dans les onze domaines d'action suivants liés à la sécurité de l'information: politique de sécurité; désignation d'un conseiller en sécurité de l'information; organisation et aspects humains de la sécurité (engagement de confidentialité du personnel, information 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 tolérance de panne, de sauvegarde, …); respect et documentation. Le Comité sectoriel a reçu l'Information System Security Policy de Cegedim. Il en ressort qu'il est satisfait aux conditions au niveau de la confidentialité et de la sécurité. Le Comité sectoriel a également reçu le Security Practice Statement et l'Information Governance Policy de Custodix. Il en ressort qu'il est satisfait aux conditions au niveau de la confidentialité et de la sécurité. Le Comité sectoriel prend acte du fait que les deux institutions ont désigné un conseiller en sécurité de l'information et que le traitement des données relatives à la santé est effectué sous la responsabilité d'un médecin.

27. En ce qui concerne le rôle de l'organisation intermédiaire, la Commission de la protection de la vie privée a confirmé que l'institution concernée doit être indépendante du responsable initial du traitement (en l'espèce, les médecins généralistes) et des destinataires des données à caractère personnel qui les traiteront à des fins statistiques ou scientifiques. Une telle organisation ne peut donc pas examiner ou analyser le contenu à de telles fins. L'organisation intermédiaire peut tenir à jour un tableau de concordance qui contient le lien entre les données à caractère personnel

[3] 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 ».

codées qui sont mises à disposition et l'identité des personnes sur lesquelles elles portent, de sorte qu'elle puisse fournir de nouvelles données à caractère personnel ou des données complémentaires relatives à ces mêmes personnes à un moment ultérieur. Outre les données identifiables issues de ce tableau de concordance qui peuvent être codées, l'organisation intermédiaire n'est pas tenue de conserver des données à caractère personnel.[4] En l'espèce, il est prévu que l'organisation intermédiaire reçoit déjà des données à caractère personnel une première fois et qu'elle les code une deuxième fois, avant de les communiquer aux destinataires. L'organisation intermédiaire supprime l'ensemble des données à caractère personnel après leur transmission au destinataire. Le Comité sectoriel constate dès lors que la méthode d'organisation intermédiaire proposée satisfait aux conditions fixées.

28. 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*, d'entreprendre toute action visant à convertir les données à caractère personnel codées en données à caractère personnel non codées. Le non-respect de cette interdiction est assorti d'une amende en vertu de l'article 39, 1°, de la loi relative à la vie privée. 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[5].

Par ces motifs,

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

autorise, conformément aux modalités telles que décrites dans cette délibération, la communication de données à caractère personnel codées relatives à la santé par des médecins généralistes à Cegedim dans le cadre du projet Thales, dans la mesure où:

- le TTP qui code les données à caractère personnel répond aux conditions qui sont imposées dans le texte sous le numéro 10 de cette délibération ;

- il est fait explicitement référence à cette délibération dans la communication aux intéressés ;

- il est prévu que l'intéressé dispose d'un temps de réflexion de sept jours civils afin de communiquer leur éventuel refus à leurs médecins respectifs.

En outre, le Comité sectoriel dispose à titre général que chaque responsable du traitement doit garantir qu'il soit satisfait aux conditions telles que décrites sous le point 10 de cette délibération, si un TTP intervient pour le codage lors du traitement de données à caractère personnel relatives à la santé.

---

[4] Point 24 de la recommandation n° 02/2011 du 4 mai 2011.
[5] Article 41 de la loi relative à la vie privée.

Yves ROGER
Président

Le siège du comité sectoriel de la sécurité sociale et de la santé est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles (tél. 32-2-741 83 11).