Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/18/262

DÉLIBÉRATION N° 13/104 DU 22 OCTOBRE 2013, MODIFIÉE LE 21 AVRIL 2015 ET LE 6 NOVEMBRE 2018, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL CODÉES RELATIVES À LA SANTÉ PAR DES MÉDECINS GÉNÉRALISTES À L'ACADEMISCH CENTRUM VOOR HUISARTSENGENEESKUNDE DANS LE CADRE D'UNE ÉTUDE SCIENTIFIQUE RELATIVE À L'EFFET D'UN SYSTÈME ÉLECTRONIQUE D'AIDE À LA DÉCISION SUR LES SOINS AUX PATIENTS

La chambre Sécurité sociale et Santé du Comité de sécurité de l'information (dénommée ci-après « le Comité »);

Vu le Règlement général sur la protection des données (ci-après : RGPD) ;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, en particulier l'article 97 ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu la loi du 3 décembre 2017 *relative à la création de l'Autorité de protection des données*, en particulier l'article 114;

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

Vu la délibération n° 13/104 du 22 octobre 2013, modifiée le 21 avril 2015 ;

Vu la demande de modification reçue le 13 septembre 2018 ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 26 octobre 2018 ;

Vu le rapport de monsieur Bart Viaene;

Émet, après délibération, la décision suivante, le 6 novembre 2018 :

A. OBJET DE LA DEMANDE

1. L'Academisch Centrum voor Huisartsengeneeskunde (centre académique de médecine générale) souhaite réaliser une étude scientifique visant à examiner l'effet de l'utilisation d'un système électronique d'aide à la décision par le médecin généraliste sur les soins aux patients diabétiques.

2. Le système électronique d'aide à la décision (EBMeDS) sera implémenté dans le dossier médical informatisé HealthOne. Le système EBMeDS fournit au sein du DMI des rappels factuels ("evidence-based reminders") spécifiques au patient pour les pathologies fréquentes en médecine générale. L'étude durera un an. Les cabinets de médecine générale belges qui utilisent le DMI de HealthOne et qui sont disposés à participer à l'étude seront répartis, de manière aléatoire, dans un groupe d'intervention ou dans le groupe de contrôle. Dans le groupe d'intervention, l'onglet EBMeDS sera visible dans HealthOne. Dans le groupe de contrôle, aucune modification ne sera apportée à HealthOne.

3. Pour la réalisation de l'étude, des données à caractère personnel codées seront communiquées aux chercheurs à cinq moments différents: au début de l'étude et ensuite après 3, 6, 9 et 12 mois. Le nombre de personnes dont les données seront traitées est estimé à 620 patients auprès de 120 médecins généralistes.

4. Il s'agit exclusivement de données à caractère personnel codées de patients ayant reçu un diagnostic de diabète à la date de début de l'étude. Les patients seront retenus dans la base de données du médecin généraliste dans la mesure où ils:

   - ont un code ICPC de diabète;

   - ont une prescription pour des médicaments liés au diabète;

   - disposent de résultats d'analyse de laboratoire confirmant le diagnostic de diabète.

4. Les données à caractère personnel codées suivantes seront communiquées par patient, tant pour le groupe de contrôle que pour le groupe d'intervention:

   - le NISS (codé), le sexe, l'âge, le nombre d'années de diabète, l'indication selon laquelle le patient réside ou non dans une maison de repos ou une institution (oui / non);

   - la glycémie, le taux de cholestérol, la tension artérielle et le risque cardiovasculaire;

   - les médicaments prescrits (oui / non): aspirine, clopidogrel, inhibiteurs ACE, sartans, statines.

5. Les données à caractère personnel codées suivantes seront communiquées concernant le médecin généraliste, tant pour le groupe de contrôle que pour le groupe d'intervention:

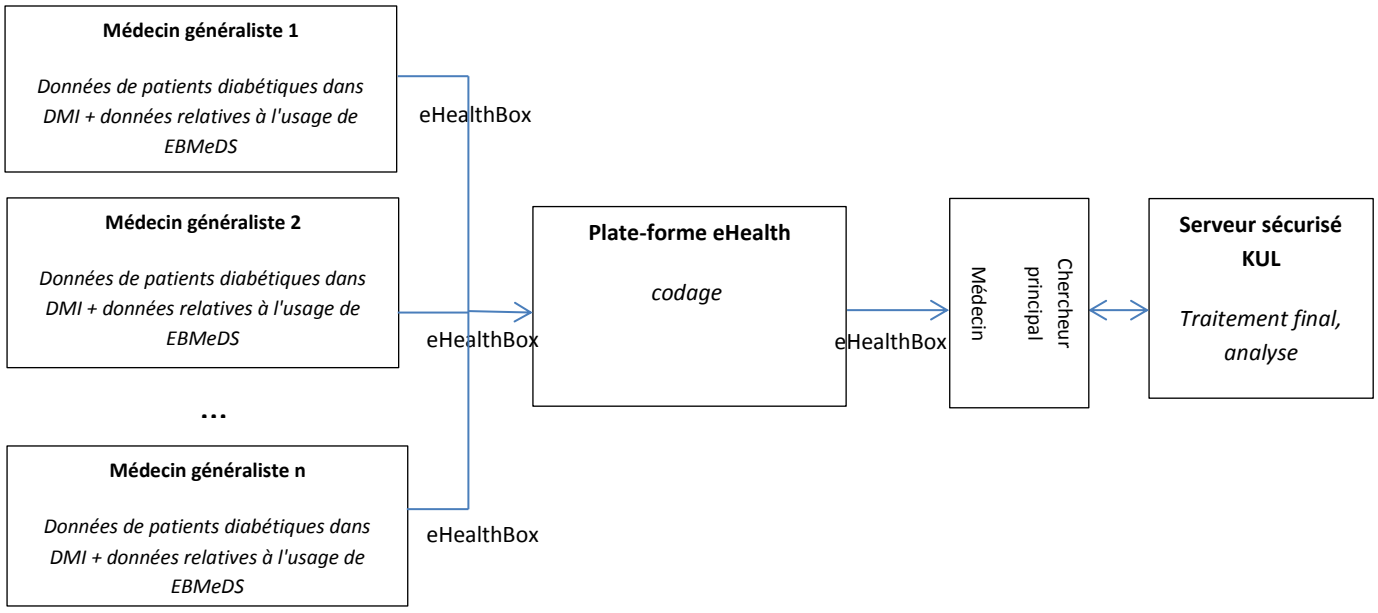
   - le NISS (codé), le sexe, l'âge, le nombre d'années d'expérience en médecine générale et la langue maternelle.

6. Les données codées suivantes relatives à l'usage de EBMeDS seront uniquement collectées pour le groupe d'intervention:

   - nombre et type de scripts EBMeDS déclenchés;

- nombre et type de scripts EBMeDS qui ont été ouverts;

7. De manière schématique, la collecte de données s'effectuera comme suit:



8. A des intervalles fixes, des données seront automatiquement collectées dans les DMI des médecins généralistes participants sur la base du NISS (numéro d'identification de la sécurité sociale) du patient. Le médecin en sera informé et pourra, s'il le souhaite, visualiser les données exportées. Les médecins participants ne pourront pas apporter de modifications à ce fichier.

9. Les fichiers output seront envoyés par le médecin généraliste à la Plate-forme eHealth via eHealthBox. Le NISS de chaque fichier sera codé au moyen du service de base de codage de la Plate-forme eHealth. Les données codées seront ensuite transmises par la Plate-forme eHealth, au moyen d'eHealthBox, au chercheur principal (médecin généraliste) de cette étude. Ce dernier placera les fichiers sur un serveur sécurisé de la KUL où aura lieu le traitement et l'analyse des données. Les chercheurs ne seront pas en mesure de retrouver l'identité des patients ou des médecins.

10. Le serveur sur lequel les données codées sont enregistrées est géré par la KU Leuven, qui se charge des mesures de sécurité techniques et organisationnelles nécessaires, y compris la désignation d'un conseiller en sécurité.

11. Le projet sera définitivement terminé lorsque les résultats de l'étude auront été publiés. Il est estimé qu'un délai de trois ans est nécessaire à cet effet. Les résultats finaux et/ou agrégats entièrement anonymes seront archivés pendant dix ans. Les publications ne contiendront en aucun cas des données (à caractère personnel) identifiables.

II. COMPÉTENCE

12. En vertu de 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 requiert une autorisation préalable du Comité, sauf exceptions prévues.

13. Compte tenu de ce qui précède, le Comité estime qu'il peut se prononcer sur la communication de données à caractère personnel relatives à la santé, telle que décrite dans la demande d'autorisation.

14. Le Comité attire l'attention sur le fait que l'usage du numéro de registre national (comme partie du NISS) n'est pas libre. Le Comité constate que les médecins généralistes concernés sont autorisés, conformément à l'article 8/1 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la Plate-forme eHealth, à enregistrer et à utiliser le numéro de registre national. Par ailleurs, la Plate-forme eHealth est elle-même autorisée, dans le cadre de l'exécution de ses missions légales, en ce compris le codage de données à caractère personnel, à utiliser le numéro de registre national.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

15. Le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes et le traitement de données à caractère personnel relatives à la santé est en principe interdit.

16. L'interdiction ne s'applique cependant pas lorsque le traitement est nécessaire à la recherche scientifique[1] et est effectué selon les conditions spécifiques de la réglementation relative à la protection de la vie privée.

17. Le Comité est par conséquent d'avis qu'il existe un fondement pour le traitement des données à caractère personnel relatives à la santé concerné.

B. LIMITATION DE LA FINALITÉ

18. Le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes.

19. Le Comité constate que le traitement de données à caractère personnel codées en question vise une étude scientifique qui sera réalisée par l'Academisch Centrum voor Huisartsengeneeskunde (ACHG) de la KU Leuven concernant l'effet d'un système électronique d'aide à la décision sur les soins aux patients diabétiques.

20. L'ACHG est un département clinique lié au département "Maatschappelijke Gezondheidszorg" de la KU Leuven. La section co-organise la formation de plus de la moitié de tous les médecins (généralistes) en Flandre et réalise des études épidémiologiques et diagnostiques qualitatives.

[1] Article 9, point 2, j), RGPD.

21. Le Comité constate que le traitement visé poursuit des finalités déterminées, explicites et légitimes.

C. MINIMISATION DES DONNÉES

22. L'article 5, b) et c), du RGPD 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.

23. Le demandeur argumente que le traitement des données à caractère personnel codées précitées est nécessaire afin d'analyser l'effet éventuel de l'intervention sur les soins aux patients diabétiques. Les données de santé sélectionnées reflètent le degré de contrôle du diabète et des risques cardio-vasculaires y associés.

24. Compte tenu de l'objectif de l'étude scientifique, le Comité estime que le traitement de ces données à caractère est en principe adéquat, pertinent et non excessif.

25. 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. Le Comité prend acte du fait que l'étude se terminera par la publication des résultats et qu'un délai de 3 ans est prévu à cet effet. En raison de problèmes techniques, l'étude a toutefois pris un certain retard. Les demandeurs souhaitent dès lors prolonger la durée de conservation. Le Comité dispose que les données à caractère personnel codées devront être détruites au plus tard le 31 décembre 2019.

26. Le Comité souligne que les résultats de l'étude ne peuvent pas être publiés sous une forme qui permet l'identification des personnes concernées.

D. TRANSPARANCE

27. Lorsque les données n'ont pas été obtenues auprès de la personne concernée, l'article 14 du RGPD prévoit que le responsable du traitement lui communique certaines informations 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.

28. Toutefois, le responsable du traitement est dispensé de cette obligation d'information lorsque l'organisation intermédiaire est une autorité administrative chargée explicitement, par ou en vertu de la loi, de rassembler et de coder des données à caractère personnel et qu'elle est soumise, à cet égard, à des mesures spécifiques visant à protéger la vie privée. Compte tenu de l'intervention de la Plate-forme eHealth pour le codage des données à caractère personnel, le demandeur est dispensé de la notification aux intéressés.

E. MESURES DE SÉCURITÉ

30. 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, ce qui est le cas en l'espèce. Le Comité 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.

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

32. 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 délégué à la protection des données; 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, …); documentation[2].

33. À condition qu'elles soient appliquées de manière correcte et intégrale, le Comité 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 du RGPD.

36. Le Comité rappelle qu'il est interdit d'entreprendre toute action visant à convertir les données à caractère personnel codées qui ont été communiquées en données à caractère personnel non codées.

[2] « Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel », document rédigé par la Commission de la protection de la vie privée disponible à l'adresse: http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

conclut que la communication de données à caractère personnel, telle que décrite dans la présente délibération, est autorisée moyennant le respect des mesures de protection des données qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Bart VIAENE