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

CSSSS/14/173

DÉLIBÉRATION N° 14/094 DU 18 NOVEMBRE 2014 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL CODÉES RELATIVES À LA SANTÉ PAR DES POSTES DE GARDE AU CENTRUM VOOR HUISARTSENGENEESKUNDE DE L'UNIVERSITÉ D'ANVERS DANS LE CADRE DU PROJET ICAREDATA

La section santé du Comité sectoriel de la sécurité sociale et de la santé (dénommée 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*;

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 définitive reçue le 13 octobre 2014;

Vu le rapport d'auditorat de la Plate-forme eHealth 7 novembre 2014;

Vu le rapport de monsieur Yves Roger.

Émet, après délibération, la décision suivante, le 18 novembre 2014:

I. OBJET DE LA DEMANDE

1. Le Centrum voor Huisartsengeneeskunde, unité de recherche "Soins de première ligne et interdisciplinaires" (Eerstelijns- en Interdisciplinaire Zorg) de la Faculté de Médecine et des Sciences de la santé (Faculteit Geneeskunde en Gezondheidswetenschappen) de l'université d'Anvers (CHA-ELIZA) soumet pour approbation au Comité sectoriel la communication de données à caractère personnel codées par des postes de garde dans le cadre de la création d'une banque de données de recherche clinique, nommée *Improve Care and Research Electronic Data Trust Antwerp* (iCAREdata).

2. Le but du projet est de permettre des études relatives aux soins en dehors des heures de travail normales ("out-of-hours" - OOH) et d'améliorer la qualité des soins OOH. Actuellement, les données relatives à un contact avec le patient ne peuvent être conservées au-delà de 18 mois dans un poste de garde. Les données ne sont dès lors disponibles à des fins de recherche que pendant une période restreinte. Grâce au projet de recherche iCAREdata, il serait possible d'étudier ces données de manière codée pendant une période plus longue, ce qui permettra une analyse plus approfondie. Les données à caractère personnel codées sont analysées par les chercheurs du CHA-ELIZA. L'étude pourra être exécutée à l'initiative du CHA-ELIZA ou à la demande de chercheurs externes.

3. Les données à caractère personnel nécessaires sont recueillies de façon automatique auprès des postes de garde participants dans le logiciel du poste de garde. Les données à caractère personnel sont ensuite transmises, via le eHealthBox, à la Plate-forme eHealth qui intervient comme tiers de confiance (*trusted third party* - TTP) pour le codage des données d'identification du patient et des prestataires de soins concernés. Les données à caractère personnel codées sont ensuite communiquées au CHA-ELIZA. Les patients sont informés au moyen d'une affiche apposée dans la salle d'attente. Le médecin peut aussi fournir de plus amples informations pendant la consultation. Le patient peut refuser de participer et le médecin généraliste est en mesure d'enregistrer le refus dans le dossier médical informatisé.

4. Les données à caractère personnel codées relatives à la santé suivantes sont communiquées par patient concerné:

<u>Données relatives au patient</u> :
- le numéro d'identification de la sécurité sociale (NISS), qui est codé par le TTP. Si le patient ne possède par de NISS, un numéro est attribué par le TTP.
- l'année de naissance du patient
- le sexe du patient
- le code postal du domicile du patient
- le code assurabilité du patient

<u>Données relatives au contact :</u>

- identification du contact,[1] codée par le TTP
- identification du poste de garde
- date et heure du contact et début du traitement, mode de prise de contact, type de contact, conseil d'urgence
- numéro INAMI du médecin qui a assuré le contact, codé par le TTP
- renvoi éventuel, incapacité de travail ou non

Données de morbidité :
- diagnostic
    - date, motif du contact (terme du thésaurus et code), diagnostic (terme du thésaurus et code)
    - texte libre présentant les plaintes subjectives du patient
    - texte libre présentant les constatations résultant de l'examen
- prescriptions médicamenteuses
    - date, nom du médicament, code CNK

5. Un fichier CSV (comma separated value) est créé sur le serveur ou l'ordinateur du poste de garde. Les trois premières colonnes contiennent respectivement le numéro NISS du patient, le numéro INAMI du médecin et le code d'identification du contact. Ces trois colonnes sont séparées par un point-virgule des colonnes suivantes qui contiennent les informations médicales. Ces colonnes avec les informations médicales sont chiffrées avant l'envoi. Le fichier CSV est transmis de manière sécurisée via le eHealthBox à la Plate-forme eHealth pour codage. Les fichiers codés sont ensuite envoyés de manière sécurisée vers le eHealthBox de iCAREdata.

6. Dans cet eHealthBox, les trois premières colonnes sont codées par la Plate-forme eHealth au moyen d'un algorithme que seule la Plate-forme eHealth connaît. Pour le numéro INAMI du médecin, il s'agit d'un algorithme réversible, tandis que pour le NISS et l'identification du contact il s'agit d'un algorithme irréversible. Les champs chiffrés avec les informations médicales ne peuvent pas être lus par la Plate-forme eHealth étant donné que cette dernière ne dispose pas de la clé de déchiffrement. Le fichier avec les champs d'identification codés et les champs d'informations médicales chiffrées est extrait de l'eHealthBox à des intervalles réguliers par le serveur de l'UA.

7. Sur le serveur de l'UA, l'équipe de recherche du projet iCAREdata déchiffre les champs médicaux, tandis que les champs d'identification restent codés. Cette méthode de travail permet d'éviter que la Plate-forme eHealth puisse lire les données médicales et que l'équipe de recherche d'iCAREdata puisse identifier les données.

8. Afin d'éviter la réidentification à partir d'une combinaison de données à caractère personnel codées, une analyse de risque "small cell" est exécutée en collaboration

[1] Dans le DMI du poste de garde, un numéro est attribué à tout contact avec un patient.

avec la Cellule technique. Au besoin, certaines données à caractère personnel codées seront agrégées afin d'éviter que les intéressés puissent être identifiés.

9. Pour la gestion de la banque de données iCAREdata, deux conseils consultatifs ont été institués: un comité scientifique et un comité directeur. Le comité scientifique est composé de représentants du CHA-ELIZA (médecins), de représentants des postes de garde participants, d'un représentant de la UA-Herculesstichting et d'un représentant des patients. Il évalue la recevabilité et la faisabilité des demandes de recherche et veille à l'application de la législation relative à la protection de la vie privée. Il renvoie les demandeurs avec des finalités non-scientifiques et purement commerciales. Il vérifie la qualité des données recueillies et l'output fourni par iCAREdata. Le comité directeur est quant à lui composé du superviseur, du promoteur, du co-promoteur du projet iCAREdata, du gestionnaire de données (médecin) et des membres du CHA concernés, ainsi que d'un représentant de la UA-Herculesstichting. Les fournisseurs de données peuvent participer de manière active ou passive aux réunions. Le comité directeur est responsable de la gestion de iCAREdata (construction et maintenance de l'infrastructure), du suivi du fonctionnement de l'infrastructure (y compris le site web), de l'évaluation des loggings, de la gestion financière, du feed-back à la Herculesstichting, du maintien des contacts et de la communication, de la réaction aux plaintes et du traitement des demandes d'opting-out (chercheurs, médecins, patients, tiers) et du suivi de l'avis du comité scientifique.

10. Les données à caractère personnel codées du projet iCAREdata font l'objet d'une analyse scientifique à l'initiative de chercheurs au sein du CHA-ELIZA associés au projet iCAREdata ou à la demande de chercheurs externes. Les chercheurs externes peuvent uniquement recevoir les résultats des analyses (sous forme d'agrégations ou non). Aucune donnée à caractère personnel codée ne sera communiquée à des chercheurs externes sans avoir obtenu l'autorisation de la section Santé du Comité sectoriel.

11. Les chercheurs non associés au CHA-ELIZA doivent introduire une demande spécifique. Ensuite, un contrat relatif aux analyses demandées sera conclu. Ces contrats sont examinés par les deux comités consultatifs.

12. Le numéro INAMI des médecins concernés est codé de manière réversible. Ainsi, il sera possible, moyennant l'intervention de la Plate-forme eHealth, de procéder à un décodage, mais uniquement pour le numéro INAMI codé des médecins en question, de sorte à pouvoir fournir le feed-back nécessaire au médecin concerné. Ceci permettra par exemple de communiquer à un médecin individuel combien d'antibiotiques et quels antibiotiques il a prescrit pour une infection déterminée. A aucun moment les chercheurs n'ont connaissance de l'identité des médecins concernés.

13. La banque de données du projet iCAREdata est conservée sur un serveur situé dans un local de serveurs du Campus Drie Eiken de l'université d'Anvers. Ce local n'est

accessible qu'à un nombre limité de collaborateurs ICT. L'accès à la banque de données en tant que telle est limité au gestionnaire de données (médecin) et à un collaborateur ICT (bio-informaticien) du projet iCAREdata. Ils ont uniquement accès à travers une connexion sécurisée. Des loggings de sécurité relatifs à l'accès à la banque de données sont prévus.

II. COMPÉTENCE

14. 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.

15. La communication de données à caractère personnel codées relatives à la santé par des postes de garde au CHA-ELIZA, en vue de la constitution d'un registre à des fins de recherches, ne correspond pas à l'une des exceptions précitées. Une autorisation du Comité sectoriel est par conséquent requise.

III. EXAMEN DE LA DEMANDE

A. PRINCIPE DE FINALITÉ

16. En vertu de l'article 4, § 1er, de la loi relative à la vie privée, les données à caractère personnel ne peuvent être traitées que 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.

17. Le traitement des données a pour objet de constituer une banque de données codées relatives à la santé à des fins de recherches scientifiques. En tant qu'université autonome, l'université d'Anvers doit, en vertu de ses statuts, notamment réaliser des recherches scientifiques spécifiques. Vu ce qui précède, le Comité sectoriel constate dès lors que le traitement envisagé poursuit une finalité déterminée, explicite et légitime.

18. Conformément à la loi relative à la vie privée, les données à caractère personnel ne peuvent pas être traitées ultérieurement de manière incompatible avec les finalités pour lesquelles elles ont été initialement obtenues, compte tenu de tous les facteurs pertinents, notamment des attentes raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. Le Comité sectoriel constate qu'en l'espèce, la finalité du traitement ultérieur n'est réputée compatible que si les dispositions du chapitre II de l'arrêté royal du 13 février 2001 portant exécution de la loi relative à la vie privée sont respectées.

19. Le traitement de données à caractère personnel relatives à la santé est en principe interdit.[2] Cependant, cette interdiction ne s'applique pas lorsque, comme en l'espèce, le traitement est nécessaire à la recherche scientifique et est effectué conformément aux conditions fixées par le Roi.[3] Le demandeur est tenu de respecter les dispositions de l'arrêté royal du 13 février 2001. Le demandeur est dès lors tenu de respecter les obligations telles que prévues aux articles 21 (relatif à l'extension de la déclaration obligatoire), 23 (relatif à la publication des résultats) et 25 (relatif à la mise à la disposition d'une liste de catégories de destinataires) de l'arrêté royal précité.

B. PRINCIPE DE PROPORTIONNALITÉ

20. 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.

21. En ce qui concerne les données codées relatives à la santé recueillies, le Comité sectoriel prend acte du fait que seul un nombre limité de données d'identification directe seront recueillies, à savoir l'année de naissance, le sexe et le code postal du domicile. Tout patient est identifié, de manière unique, au moyen d'un NISS qui est codé par la Plate-forme eHealth. Les données de santé ont trait au diagnostic et à la consommation de médicaments. Le Comité sectoriel constate que l'étude clinique envisagée par le CHA-ELIZA requiert effectivement des données spécifiques relatives à l'incidence et à la prévalence de maladies et à la prise de médicaments ainsi que des données concernant le contact avec le poste de garde. Le demandeur déclare que les données décrites permettent de répondre à diverses questions de recherche relatives aux soins OOH. La méta-analyse des données permet de mieux comprendre le fonctionnement des postes de garde.

22. Un traitement ultérieur de données à caractère personnel à des fins scientifiques doit en principe être réalisé au moyen de données anonymes. Si la finalité ne peut être réalisée au moyen de données anonymes, des données à caractère personnel codées peuvent être traitées. Etant donné qu'il est indispensable qu'un patient soit identifié de manière unique et qu'il est primordial de suivre un patient dans le temps, il est acceptable que des données à caractère personnel codées soient utilisées.

23. En ce qui concerne le traitement des données à caractère personnel codées à la demande de chercheurs externes, le Comité sectoriel constate que les analyses scientifiques qui sont nécessaires pour répondre aux questions de l'étude seront effectuées par les chercheurs du CHA-ELIZA associés au projet iCAREdata. Toute

[2] Article 7er, § 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, *M.B.* 18 mars 1993 (dénommée ci-après "loi relative à la vie privée").
[3] Article 7, § 2, k) de la loi relative à la vie privée.

communication de données à caractère personnel codées relatives à la santé en provenance de la banque de données du projet iCAREdata doit être soumise au préalable au Comité sectoriel pour approbation.

24. Vu ce qui précède, le Comité sectoriel estime que le traitement des données à caractère personnel envisagé est adéquat, pertinent et non excessif à la lumière des finalités envisagées.

25. Les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant un délai n'excédant pas celui nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. Le demandeur prévoit un délai de conservation de 30 ans à compter de l'enregistrement dans la banque de données. Ce délai de conservation doit permettre d'étudier les évolutions dans le temps. Le demandeur déclare que les soins OOH constituent un phénomène relativement récent et que le fonctionnement peut prendre une direction imprévue. De même, les tendances en termes de comportement de prescription ne peuvent être étudiées qu'après plusieurs années. Le Comité sectoriel accepte dès lors le délai de conservation proposé.

C. PRINCIPE DE TRANSPARENCE

26. Le responsable du traitement de données à caractère personnel, collectées à des fins déterminées, explicites et légitimes ou, le cas échéant, l'organisation intermédiaire doit en principe, préalablement au codage de données à caractère personnel, communiquer certaines informations relatives au traitement à la personne concernée.

27. Le demandeur prévoit une notification du traitement des données à l'intéressé au moyen de l'apposition d'une affiche dans la salle d'attente et la possibilité de la communication d'informations plus détaillées par le médecin généraliste pendant la consultation. La notification au moyen de l'affiche renvoie également à la présente délibération.

28. Le Comité sectoriel estime que la notification prévue est suffisante.

D. MESURES DE SÉCURITÉ

29. 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[4]. 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[5]. Le Comité sectoriel a effectivement reçu l'identité du médecin concerné. Le Comité sectoriel rappelle que lors du traitement de données à caractère personnel, le

[4] Article 7, § 4, de la loi relative à la vie privée.
[5] Délibération n° 07/ du 4 septembre 2007.

professionnel des soins de santé ainsi que ses préposés ou mandataires sont soumis au secret.

30. 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[6]. Le Comité sectoriel renvoie à ce propos aux mesures de référence qui sont applicables en vue de la protection de tout traitement de données à caractère personnel, qui ont été établies par la Commission de la protection de la vie privée.[7] Ces mesures doivent garantir 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.

31. Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est, en fonction du contexte et de la nature des données à caractère personnel, 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 prend acte du fait que le demandeur confirme qu'un conseiller en sécurité de l'information a été désigné. Les locaux où les données à caractère personnel codées sont enregistrées, sont sécurisés et ne sont accessibles qu'aux seules personnes autorisées. L'accès 'on-campus' au serveur via le réseau est strictement réglementé et intervient sur la base de l'adresse IP et de données de compte. Les protocoles utilisés sont, si possible, protégés au moyen de SSL. L'accès à distance au serveur n'est possible qu'au moyen d'un accès VPN SSL et sur la base de droits d'accès spécifiques. L'accès fait également l'objet de loggings. Le serveur est équipé d'éléments redondants: alimentation double, technologie RAID, monitoring automatique du hardware et prise de backups.

32. Le Comité sectoriel souligne, dans un souci d'exhaustivité, que conformément à l'article 6 de l'arrêté royal du 13 février 2001, 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. Le non-respect de

---

[6] Article 16 de la loi relative à la vie privée.

[7] http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf

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 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.

Par ces motifs,

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

autorise la communication de données à caractère personnel relatives à la santé par des postes de garde au Centrum voor Huisartsengeneeskunde de l'Université d'Anvers, dans le cadre du projet iCAREdata, à l'intervention de la Plate-forme eHealth qui se chargera de coder les données à caractère personnel.

La Plate-forme eHealth est autorisée à conserver le lien entre le numéro codé et le numéro d'identification réel, vu le caractère longitudinal du projet. Par ailleurs, la Plate-forme eHealth est autorisée à procéder au décodage, cependant, uniquement du numéro INAMI codé des médecins concernés, afin de pouvoir leur fournir le feed-back nécessaire. Des données à caractère personnel (codées ou non) relatives aux patients individuels ne peuvent cependant jamais être communiquées.

Yves ROGER
Président