

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

CSSSS/13/079

**DÉLIBÉRATION N° 13/026 DU 19 FÉVRIER 2013 RELATIVE À LA
COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL CODÉES
RELATIVES À LA SANTÉ, DANS LE CADRE DE LA CONSTITUTION, DE
L'UTILISATION ET DE LA MISE À LA DISPOSITION D'UN REGISTRE DES
RECHERCHES EN ÉPIDÉMIOLOGIE (INTEGO)**

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

Vu la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, notamment l'article 42, §2, 3°;

Vu la demande d'autorisation reçue le 31 octobre 2012 ;

Vu le rapport d'auditorat du 6 mars 2012 ;

Vu le rapport de monsieur Yves Roger;

Émet, après délibération, la décision suivante, le 19 mars 2013:

I. OBJET DE LA DEMANDE

1. La *Katholieke Universiteit Leuven* (KULeuven) soumet, à l'approbation du Comité sectoriel, la communication de données à caractère personnel codées relatives à la santé à l'*Academisch Centrum voor Huisartsengeneeskunde*, dans le cadre d'un système d'enregistrement général et continu de la morbidité, appelé projet Intego ('*Integrated Computerised Network*').

2. La banque de données INTEGO qui enregistre, depuis 1995, des données à caractère personnel codées relatives à la santé, est appelée à devenir la banque de données des maladies. Cette banque de données qui permettra, entre autres, de fournir des informations sur l'incidence et la prévalence de maladies en Flandre, sur les médicaments prescrits, sur les résultats de laboratoire et sur les antécédents, sera mise à jour en permanence. A l'heure actuelle, 54 pratiques de médecins généralistes totalisant 94 médecins généralistes font l'objet d'un rapport pour une population annuelle d'environ 266.000 patients. Les données à caractère personnel codées seront analysées par les chercheurs de l'*Academisch Centrum voor Huisartsengeneeskunde* (ACHG) de la KULeuven (qui est ou non associé au projet INTEGO) et seront mises à la disposition de tiers, à des fins de recherches scientifiques.
3. Les données à caractère personnel codées qui sont nécessaires, seront recueillies automatiquement auprès des médecins généralistes participants qui utilisent un logiciel déterminé pour la gestion de leurs dossiers médicaux informatisés, à savoir Medidoc. Les médecins généralistes concernés seront, chaque année, invités par le producteur de logiciel à participer à l'enregistrement. Ils recevront un lien vers le logiciel qui sélectionnera les données requises dans le dossier médical informatisé et qui enregistrera ces données dans un fichier sur l'ordinateur du médecin généraliste. Ce fichier sera chiffré, préalablement à l'envoi, et sera transmis à une Tierce partie de confiance qui procédera au codage des données à caractère personnel et au codage de l'identité du médecin généraliste concerné. Les patients seront informés au moyen d'une affiche apposée dans la salle d'attente. Le médecin généraliste pourra aussi fournir de plus amples informations pendant la consultation. Le patient pourra refuser de participer et le médecin généraliste sera en mesure d'enregistrer le refus dans le dossier médical informatisé.
4. Les données à caractère personnel codées relatives à la santé suivantes seront communiquées par patient concerné:
 - un numéro de patient. Le logiciel utilisé octroie un numéro à chaque patient. Ce numéro est totalement distinct du numéro de dossier utilisé dans le DMI. Un numéro est attribué en fonction de l'ordre de création du dossier dans la pratique du médecin. Seul le médecin généraliste concerné connaît, grâce à son logiciel, le lien entre l'identité du patient et le numéro de patient ;
 - l'année de naissance ;
 - le sexe ;
 - le nombre d'année(s) que le patient contacte la pratique du médecin ;
 - les données en matière de morbidité:
 - o le diagnostic (date, terme du thésaurus, code Medidoc, statut: archives ou actif) ;
 - o les résultats de laboratoire (date, code du test, résultat, unité) ;
 - o les prescriptions de médicaments (date, nom médicament, code CNK) ;
 - o les valeurs de mesure (date, code Medidoc du test, résultat, unité) ;
 - o les vaccins (date, nom du vaccin, code du produit, type de vaccin) ;
 - o le dossier médical global (DMG): date du DMG ;
 - les données relatives à la pratique du médecin généraliste:
 - o le numéro de code (attribué par la tierce partie) ;
 - o l'arrondissement.

5. Après les avoir séparées des données codées précitées, plusieurs données seront transmises par pratique de médecins-généralistes (pour des raisons administratives):
 - le numéro d'identification de la pratique du médecin ;
 - le numéro INAMI du médecin ;
 - l'âge et le sexe du médecin ;
 - l'année dans laquelle le médecin généraliste a commencé sa pratique ;
 - l'utilisation de la technologie du *terminal server* ;
 - commune dans laquelle la pratique du médecin généraliste est située.
6. Avant que le fichier contenant les données décrites ci-dessus est envoyé à la Tierce partie de confiance, il est chiffré au moyen d'un chiffrement AES dont la clé est uniquement connue par le fournisseur du logiciel et par le destinataire.
7. C'est l'*Expertisecentrum voor Digital Media* (EDM) de l'Université de Hasselt qui interviendra comme Tierce partie de confiance. Un seul collaborateur de l'EDM participera concrètement au codage. L'EDM procèdera au codage, au moyen d'un algorithme, des numéros de patient dans les données relatives à la santé (point 4) et au codage des numéros d'identification des pratiques (point 5). Le demandeur précise que seul l'EDM connaît l'algorithme de codage et qu'il n'est pas communiqué au groupe de recherche. L'EDM ajoutera ensuite l'arrondissement de la pratique concernée aux données de santé et transmettra ces données codées relatives à la santé à la banque de données INTEGO. Les données codées relatives à la pratique du médecin sont communiquées au groupe de recherche INTEGO.
8. Après le codage et la transmission des données, l'EDM devra détruire immédiatement les données à caractère personnel reçues. Seul le tableau de conversion contenant les numéros de patient (codés) et les numéros d'identification (codés) de la pratique du médecin généraliste sera conservé pour un feedback futur éventuel. Ce feedback sera utilisé pour réaliser un contrôle de qualité et améliorer l'enregistrement dans les pratiques de médecins généralistes. C'est ainsi qu'il sera vérifié dans la banque de données INTEGO si les patients prennent des médicaments pour une maladie donnée. Ensuite, il sera contrôlé si ce diagnostic (par exemple, diabète) a été noté à côté du nom de ce patient.
9. La banque de données INTEGO est enregistrée sur un serveur situé dans la salle informatique de l'hôpital universitaire de Louvain qui fait partie du réseau de Gbiomed. Les serveurs y sont observés et surveillés en permanence. L'accès est uniquement possible moyennant un nom d'utilisateur et un mot de passe spécifiques attribués par le gestionnaire réseau de l'UZLeuven. Tous les logins sont conservés et sont consultables à des fins de contrôle. Le personnel de l'UZLeuven n'a pas accès à ce serveur. A partir de 2013, l'enregistrement de la banque de données INTEGO aura lieu dans le nouveau datacenter de la section Information et Communication, à savoir du service *Technologie en Systemen (ICTS)* de la KULeuven à Heverlee. A l'heure actuelle, une seule personne a accès à la banque de données INTEGO, à savoir le coordinateur/gestionnaire de données du groupe de recherche. C'est lui qui exécute les traitements de données, une fois la procédure de demande finalisée (cf. infra)

10. A la demande de la Commission de la protection de la vie privée¹, deux comités consultatifs ont été créés pour la gestion de la banque de données INTEGO, à savoir un comité scientifique et un comité éthique. Le comité scientifique se compose de représentants du projet INTEGO, de diplômés de l'enseignement supérieur (médecins) et d'un médecin externe. Ce comité surveille la qualité des données recueillies, leur traitement et leurs analyses. Le comité éthique se compose de représentants du projet INTEGO, de diplômés de l'enseignement supérieur (non médecins) et d'un médecin externe. Le comité éthique veille à l'application de la réglementation relative à la protection de la vie privée et surveille les applications éthiques du traitement des données. Par ailleurs, pour des projets individuels, l'avis de la Commission médico-éthique de la Faculté de médecine de la KULeuven est, le cas échéant, demandé.
10. Les données à caractère personnel codées de la banque de données INTEGO peuvent, à des fins de recherches scientifiques, être mises à la disposition :
- des collaborateurs de l'ACHG qui sont spécifiquement associés (par contrat) au projet INTEGO;
 - d'autres collaborateurs de l'ACHG;
 - de chercheurs non associés à l'ACHG.
- 10.1 Les chercheurs non associés à l'ACHG et les chercheurs associés à l'ACHG mais non au projet INTEGO doivent introduire une demande spécifique d'accès à la banque de données INTEGO. Ensuite, un contrat qui prévoit les éléments suivants sera conclu: l'identification du responsable du traitement des données et des chercheurs ainsi que leurs fonctions respectives, l'objectif de l'étude, les données nécessaires, la durée de l'étude, l'indication de la date à laquelle le tableau de conversion sera détruit (cf. infra) et l'indication selon laquelle les chercheurs doivent respecter la législation relative à la vie privée. Ces contrats sont examinés par les deux comités consultatifs. Le demandeur fait savoir que ces contrats sont tenus à la disposition du Comité sectoriel. Cette catégorie de chercheurs reçoit en principe uniquement des données agrégées. Si la finalité de l'étude en question requiert effectivement des données à caractère personnel codées individuelles, seule une sélection de données à caractère personnel codées disponibles sera communiquée. Si des données à caractère personnel codées non agrégées sont communiquées à cette catégorie de chercheurs, les numéros de patient codés seront, au préalable, codés une troisième fois² par le gestionnaire de données de la banque de données INTEGO. Les codes sont différents pour chaque question de l'étude externe et les tableaux de conversion seront détruits dès que l'étude est terminée (cf. supra). Le gestionnaire de la banque de données INTEGO est un médecin qui possède une connaissance approfondie de la législation relative à la vie privée et qui, pour rappel, est le seul à disposer d'un accès direct à la banque de données INTEGO.
- 10.2 Les chercheurs de l'ACHG associés spécifiquement au projet INTEGO³ peuvent solliciter un accès aux données dans le cadre de l'étude épidémiologique du projet INTEGO. Ces

¹ Les modalités du traitement de données ont été élaborées en 2007 en concertation avec la Commission de la protection de la vie privée.

² Après un premier codage par le logiciel et un second par la Tierce partie de confiance.

³ Il s'agit de trois personnes dont le Comité sectoriel a reçu les coordonnées.

personnes se concertent à des intervalles réguliers et peuvent procéder à des analyses exploratoires et préparatoires, par exemple, en se basant sur la littérature. Si ceci donne lieu à une analyse formelle des données à caractère personnel codées enregistrées dans la banque de données INTEGO, ceci est communiqué aux deux comités consultatifs. Les résultats de l'étude épidémiologique sont publiés et diffusés à des intervalles réguliers.

II. COMPÉTENCE

11. Conformément à la loi du 13 décembre 2006, toute communication de données à caractère personnel relatives à la santé doit faire l'objet d'une autorisation de principe de la section santé du Comité sectoriel de la sécurité sociale et de la santé, sauf dans les cas d'exception prévus dans la loi.⁴
12. La communication de données à caractère personnel codées relatives à la santé par les médecins généralistes à l'ACHG de la KULeuven, 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. ADMISSIBILITÉ

13. Le traitement de données à caractère personnel relatives à la santé est en principe interdit.⁵
14. 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.⁶ Le demandeur est tenu de respecter les dispositions de l'arrêté royal du 13 février 2001 portant exécution de la loi relative à la vie privée. Le demandeur est dès lors tenu de respecter les obligations prévues aux articles 21 (concernant l'extension de la déclaration obligatoire), 23 (concernant la publication des résultats) et 25 (concernant la mise à disposition d'une liste des catégories de destinataires) de l'arrêté d'exécution précité.

B. FINALITÉ

15. Les données à caractère personnel doivent être obtenues pour des finalités déterminées, explicites et légitimes.
16. Le traitement des données a pour objectif de constituer une banque de données codées relatives à la santé à des fins de recherches scientifiques ou en épidémiologie. En tant qu'université autonome, la KULeuven doit, en vertu de ses statuts, notamment réaliser des

⁴ Article 42, § 2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, *M.B.* du 22 décembre 2006.

⁵ 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 »).

⁶ Article 7, § 2, k) de la loi relative à la vie privée.

recherches scientifiques spécifiques. Vu ce qui précède, le Comité sectoriel constate dès lors que le traitement envisagé poursuit une finalité déterminée, explicite et légitime.

17. 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 sont respectées.

C. PROPORTIONNALITÉ

18. Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.⁷
19. 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, l'année ou les années au cours desquelles l'intéressé a contacté la pratique du médecin et l'arrondissement de la pratique du médecin généraliste. Chaque patient sera identifié dans la pratique au moyen d'un numéro de patient qui est spécifiquement attribué pour cette collecte. Ce numéro sera codé par une Tierce partie de confiance, à savoir l'*Expertisecentrum voor Digitale Media* de l'Université de Hasselt. Quant aux données de santé, elles ont trait à la quasi-totalité des données de morbidité qui sont enregistrées dans le dossier médical de l'intéressé: le diagnostic, les résultats de laboratoire, les prescriptions de médicaments, les vaccins et la date de création du dossier médical global. Le Comité sectoriel constate que l'étude épidémiologique et clinique envisagée par le groupe de recherche INTEGO requiert effectivement des données spécifiques relatives à l'incidence et à la prévalence de maladies, à la prise de médicaments, aux résultats de laboratoire et à certains antécédents.
20. En ce qui concerne les données relatives à la pratique du médecin telles que décrites au point 5, le Comité sectoriel prend acte du fait que les données sont nécessaires pour le suivi administratif du projet INTEGO, plus précisément pour l'organisation de la formation et le paiement des prestations.
21. 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 la nécessité pour un patient de ne pas être enregistré deux ou plusieurs fois, par pratique, dans la banque de données (il n'y a pas de couplage de données relatives à un même patient entre les différentes pratiques) et la nécessité de pouvoir suivre un patient d'une même pratique à travers le temps, il est acceptable que des données à caractère personnel codées soient utilisées.

⁷ Article 4, 2°, de la loi relative à la vie privée.

22. En ce qui concerne la communication de données à caractère personnel codées par l'ACHG aux chercheurs qui ne sont pas associés au projet INTEGO, le Comité sectoriel constate qu'il est prévu que la finalité et la proportionnalité du traitement des données réalisé par les destinataires seront évaluées par un comité scientifique et par un comité éthique qui se composent de médecins et de juristes. Le Comité sectoriel prend également acte du fait que les contrats qui seront conclus avec les destinataires, seront tenus à la disposition à des fins de surveillance.
23. 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.
24. 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 que les données à caractère personnel codées seront conservées dans la banque de données INTEGO pour une durée illimitée. Le Comité sectoriel souligne que ce type de délai ne peut pas être accepté. Il déclare que les données à caractère personnel codées doivent être transformées, après une période de trente ans, en données anonymes, plus précisément en supprimant le lien entre le code de patient attribué par le logiciel et le numéro codé attribué par l'EDM. Le Comité sectoriel souligne que le demandeur peut toujours demander une prolongation de ce délai, à la condition toutefois qu'il puisse avancer les arguments requis.

D. TRANSPARANCE

25. 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.⁸
26. 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 de la possibilité de demander davantage d'informations au médecin généraliste pendant la consultation.
27. Le Comité sectoriel estime que les données suivantes doivent compléter l'affiche :
 - le logo du projet INTEGO ;
 - les informations suivantes relatives au Comité sectoriel.

"La communication des données à caractère personnel codées a également fait l'objet d'une autorisation de la section Santé du Comité sectoriel de la sécurité sociale et de la santé, par sa délibération n° (XXX) du 19 mars 2013. Vous trouverez davantage d'informations sur le site web suivant: www.privacycommission.be"

⁸ Article 14 de l'arrêté royal du 13 février 2001.

E. MESURES DE SÉCURITÉ

28. 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 santé⁹. 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 médecin¹⁰. 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 professionnel des soins de santé ainsi que ses préposés ou mandataires sont soumis au secret.
29. 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 personnel¹¹. Le Comité sectoriel renvoie à ce propos aux mesures de référence qui sont applicables à la protection de tout traitement de données à caractère personnel, qui ont été établies par la Commission de la protection de la vie privée.¹² 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.
30. 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 de la confirmation par le demandeur de la prise de toutes les mesures de sécurité requises, en ce compris la désignation d'un conseiller en sécurité de l'information.
31. 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 cette interdiction est assorti d'une amende en vertu de l'article 39, 1^o, de la loi relative à la vie privée. Le Comité sectoriel

⁹ Article 7, § 4, de la loi relative à la vie privée.

¹⁰ Délibération nr. 07/034 du 4 septembre 2007

¹¹ Article 16 de la loi relative à la vie privée.

¹²

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, selon les modalités de la présente délibération, la communication de données à caractère personnel codées relatives à la santé, dans le cadre de la constitution, de l'utilisation et de la mise à la disposition d'un registre de recherches en épidémiologie (INTEGO), pour autant que:

- le délai de conservation des données à caractère personnel codées tel que décrit sous le point 24 de la présente délibération soit respecté;
- la notification aux personnes concernées soit adaptée, conformément aux dispositions du point 27 de la présente délibération.

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.
--