

Comité sectoriel de la sécurité sociale et de la santé
Section “Santé”

CSSSS/14/143

DÉLIBÉRATION N° 14/075 DU 16 SEPTEMBRE 2014 PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ PAR DES HÔPITAUX À LA SPRL IMS HEALTH, EN VUE DE LA RÉALISATION D'ACTIVITÉS DE BENCHMARKING, D'UNE PART, ET D'ÉTUDES ET D'ANALYSES, D'AUTRE PART

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 reçue le 1^{er} août 2014 ;

Vu les renseignements complémentaires du demandeur que l'auditorat a reçus le 12 septembre 2014;

Vu le rapport d'auditorat de la Plate-forme eHealth du 12 septembre 2014 ;

Vu le rapport de monsieur Yves Roger.

Émet, après délibération, la décision suivante, le 16 septembre 2014 :

I. OBJET DE LA DEMANDE

1. La sprl IMS Health a pour but la communication de données à caractère personnel codées relatives à la santé par un grand nombre d'hôpitaux¹, pour deux finalités:
 - la réalisation d'analyses comparatives, la sprl IMS Health² intervenant comme sous-traitant pour les hôpitaux concernés
 - l'exécution d'analyses et d'études en vue de leur commercialisation, la sprl IMS Health³ intervenant comme responsable du traitement ultérieur.
2. Les analyses comparatives doivent permettre aux hôpitaux de comparer leur performance interne à celle d'autres hôpitaux et d'ainsi détecter les endroits où des mesures peuvent être prises pour augmenter la performance et la qualité des hôpitaux. Dans le cadre des efforts financiers croissants qui sont demandés aux hôpitaux, ces analyses comparatives sont considérées comme étant de plus en plus importantes pour une bonne gestion hospitalière.
3. En ce qui concerne le deuxième objectif, la sprl IMS Health mettra les résultats à la disposition de ses clients, sous forme anonyme, après traitement des données à caractère personnel codées à des fins statistiques et/ou scientifiques. Ses clients sont les parties qui interviennent dans les soins de santé, notamment les entreprises pharmaceutiques, les entreprises actives au sein de l'industrie des accessoires médicaux, l'INAMI, les hôpitaux, les universités.
4. Pour pouvoir réaliser ces deux objectifs, les hôpitaux communiqueront les données à caractère personnel codées suivantes à la sprl IMS Health:
 - *Résumés hospitaliers minimums (RHM)*

Il s'agit des fichiers standard RHM (résumés hospitaliers minimums) que les hôpitaux sont obligés de créer dans le format imposé par les pouvoirs publics⁴. Ces données couvrent les domaines suivants:

- Données de structure: informations de base relatives à l'hôpital; données relatives aux sites d'un hôpital, aux unités de soins et aux index de lits; données relatives aux associations; données relatives aux séjours, aux spécialités, aux unités de soins et aux index de lits au sein de l'association.

¹ 23 hôpitaux sont concernés.

² Les analyses comparatives sont réalisées par la SA Forcea, une filiale de la sprl IMS Health.

³ Les analyses et les études sont réalisées par la sprl IMS Health Consulting, une filiale de l'IMS Health.

⁴ Les détails de ces fichiers sont disponibles sur le site du service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement à l'adresse suivante: [http://www.health.belgium.be/eportal/Healthcare/Healthcarefacilities/Registrationsystems/MHD\(MinimumHospitalData\)/Guidelines/index.htm#REGMZG](http://www.health.belgium.be/eportal/Healthcare/Healthcarefacilities/Registrationsystems/MHD(MinimumHospitalData)/Guidelines/index.htm#REGMZG). La composition du RHM est déterminée dans 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, M.B. 10 juillet 2007 (art. 11 et suivants).

- Données relatives au personnel: données périodiques et journalières du personnel.
- Données administratives: données relatives au patient; données relatives au séjour, au séjour en spécialité, au séjour en index de lit, au séjour en unité de soins, données relatives au moyen de transport utilisé, liste des ambulances non agréées.
- Données infirmières: items infirmiers.
- Données médicales: données relatives aux diagnostics, aux interventions et aux prestations INAMI; données relatives à la naissance (nouveaux-nés), résultats des examens; données relatives aux admissions par un service d'urgence.

- *Fichiers de facturation*

Les fichiers de facturation que les hôpitaux créent de manière standard constituent le point de départ pour ces données⁵. Les fichiers de facturation contiennent les données d'identification des patients concernés, les données relatives à l'hôpital et les dates et la nature des prestations fournies.

5. Préalablement à l'intervention de la TTP (voir infra), les hôpitaux suppriment les champs « Identification bénéficiaire » et « Identification prescripteur » dans les fichiers précités. Le demandeur a confirmé au Comité sectoriel que le codage des données à caractère personnel sera assuré par un tiers de confiance (*trusted third party* - TTP), à savoir la société Custodix. Le demandeur déclare que la TTP satisfait aux conditions fixées par le Comité sectoriel dans sa délibération n° 14/059 du 15 juillet 2014 portant sur la communication de données à caractère personnel codées relatives à la santé dans le cadre du projet Thales. Dans ce contexte, Custodix veillera à ce que le set de données à caractère personnel codées mis à la disposition ne puisse, raisonnablement, pas donner lieu à la réidentification.
6. L'intervention de la TTP se compose de 2 phases :
 - Dans un premier temps, Custodix soumettra les données transmises par les hôpitaux à la sprl IMS Health à une analyse des risques. Cette analyse des risques a pour but d'identifier les éléments de données (et la combinaison d'éléments de données) pour lesquels il existe un risque de ré-identification du 'bénéficiaire' ou du 'prestataire de soins', compte tenu des principes de finalité et de proportionnalité.
 - Dans une seconde phase, dans la mesure où ceci s'avère nécessaire sur la base des résultats de cette analyse par Custodix, un processus sera initié auprès de Custodix afin de soumettre les données codées transmises par les hôpitaux à la sprl IMS Health, à un traitement supplémentaire en supprimant ou en regroupant ces éléments de données spécifiques.

⁵ Les détails de ces fichiers sont disponibles sur le site de l'INAMI à l'adresse suivante:
http://www.riziv.fgov.be/care/nl/infos/bill/pdf/2013/coordinated_version.pdf

II. COMPÉTENCE

7. Conformément à l'article 42, § 2, 3^o, 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. Dans sa délibération n° 12/004 du 17 janvier 2012⁶, le Comité sectoriel a précisé que la communication de données à caractère personnel relatives à la santé telle que prévue à l'article 42, § 2, 3^o de la loi du 13 décembre 2006, doit être considérée comme une communication entre un responsable du traitement et un tiers autre que la personne concernée ou un sous-traitant au sens de la loi relative à la vie privée⁷. Pour autant que la sprl IMS Health puisse effectivement être considérée comme un sous-traitant au sens de la loi relative à la vie privée, la communication des données à caractère personnel codées par les hôpitaux à des fins de benchmarking ne doit, en principe, pas faire l'objet d'une autorisation.
9. Cependant, vu le fait que les mêmes données à caractère personnel sont communiquées à la même partie dans ses différentes qualités, à savoir comme sous-traitant et comme responsable du traitement, le Comité sectoriel estime qu'il est impératif de prévoir un même niveau de protection pour les deux finalités, à savoir le niveau le plus strict qui devrait être appliqué pour une des deux finalités.
10. Le Comité sectoriel estime dès lors qu'il est compétent pour se prononcer sur le traitement de données à caractère personnel, à la lumière des deux finalités.

III. EXAMEN DE LA DEMANDE

A. PRINCIPE DE FINALITÉ

11. 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. Aux conditions fixées dans l'arrêté d'exécution, le traitement ultérieur des données à des fins historiques, statistiques ou scientifiques n'est pas considéré comme un traitement incompatible⁸.

⁶ Délibération n°12/004 du 17 janvier 2012 relative à la communication de données à caractère personnel codées relatives à la santé par la Vlaams Agentschap Zorg en Gezondheid (agence flamande soins et santé) au Studiecentrum voor Perinatale Epidemiologie (centre d'études épidémiologiques périnatales)

⁷ 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.* du 18 mars 1993.

⁸ 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, *M.B.* 13 mars 2001, dénommée ci-après 'arrêté d'exécution'.

12. Le Comité sectoriel constate que le traitement des données décrit poursuit deux objectifs: d'une part, le benchmarking à la demande des hôpitaux concernés et, d'autre part, la réalisation d'études et d'analyses, en vue de leur commercialisation par la sprl IMS Health. Les finalités telles que décrites dans la demande peuvent être considérées comme déterminées, explicites et légitimes dans le chef des hôpitaux et de la sprl IMS Health.
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, sauf dans les exceptions prévues au § 2 du même article. En ce qui concerne le traitement des données à caractère personnel à la lumière des analyses comparatives, les arguments peuvent être formulés selon lesquels ce traitement est nécessaire à la gestion des services de santé dans l'intérêt de la personne concernée, toutefois, à la condition que les données soient traitées sous la surveillance d'un professionnel des soins de santé (art. 7, § 2, j). Le demandeur confirme que le traitement au sein de la sprl IMS Health a lieu sous la responsabilité d'un médecin. En ce qui concerne la réalisation d'études et d'analyses, le traitement ultérieur à des fins statistiques, scientifiques et historiques est admissible, pour autant qu'il soit satisfait aux conditions prévues dans l'arrêté d'exécution (art. 7, § 2, k). Cela implique notamment que, s'il est impossible d'utiliser des données anonymes, le responsable du traitement (à savoir les hôpitaux) ou une organisation intermédiaire doit procéder au codage des données à caractère personnel (art. 9 de l'arrêté d'exécution).
14. Le Comité sectoriel prend acte du fait que Custodix interviendra en tant que TTP en vue du codage des données à caractère personnel et qu'elle satisfait, conformément à la déclaration du demandeur, aux conditions imposées aux *trusted third parties* qui procèdent au codage de données à caractère personnel relatives à la santé, comme décrit dans la délibération n° 14/059 du 15 juillet 2014 portant sur la communication de données à caractère personnel codées relatives à la santé dans le cadre du projet Thales⁹.

B. PRINCIPE DE PROPORTIONNALITÉ

15. 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.
16. Les données (à caractère personnel et autres) qui seraient traitées dans le cadre des deux finalités, ont, d'une part, trait à la totalité des résumés hospitaliers minimums et, d'autre part, à la totalité des fichiers de facturation, après codage par la TTP.

⁹ Les délibérations du Comité sectoriel peuvent être consultées à l'adresse suivante: <https://www.ehealth.fgov.be/fr/a-propos-de-ehealth/organisation/comite-sectoriel/presentation>

17. Le demandeur avance les arguments selon lesquels les fichiers intégraux sont demandés pour les deux finalités pour les raisons suivantes:
- d'une part, les hôpitaux s'attendent à ce que la sprl IMS Health satisfasse, rapidement et de manière très dynamique, aux nouveaux besoins des hôpitaux et, d'autre part, les hôpitaux espèrent que la charge de travail due à la participation aux études comparatives restera minimale. Le demandeur déclare qu'il est satisfait à leurs souhaits par la demande de fichiers standard qui existent déjà au sein des hôpitaux
 - afin de pouvoir réaliser des études qui soient suffisamment dynamiques pour les clients (les parties qui participent aux soins de santé), il est, selon le groupe ISM Health, absolument nécessaire de disposer de l'ensemble des informations jusqu'au niveau le plus détaillé possible. Selon le demandeur, il serait, d'un point de vue logistique, impossible et irréalisable de réaliser, pour chaque demande individuelle, une consultation adaptée de données auprès des différents hôpitaux. Ceci donnerait à nouveau lieu à une inefficacité très handicapante dans le secteur; inefficacité qui est certes évitable.
18. Compte tenu des finalités du traitement, le Comité sectoriel estime que la communication envisagée est pertinente et non excessive.
19. En ce qui concerne le délai de conservation des données, il est prévu que les données à caractère personnel codées seront conservées pendant une période de dix ans à compter de leur réception. Selon le demandeur, cela doit permettre de comparer les données relatives aux différents produits médicaux/médicaments à travers le temps. Le cycle de vie d'un produit médical s'élève en moyenne à environ 10 ans, de sorte qu'un délai de conservation plus long n'est pas nécessaire. Le Comité sectoriel est d'accord avec ce délai de conservation.

C. PRINCIPE DE TRANSPARENCE

20. Tant la loi relative à la vie privée que l'arrêté d'exécution prévoient une obligation d'information de la personne concernée par le responsable du traitement.
21. Le Comité sectoriel prend acte du fait que les hôpitaux prévoient la notification du traitement de données à caractère personnel à des fins d'activités de benchmarking, d'une part, et, la communication des données à caractère personnel pour le traitement ultérieur à la lumière d'études et d'analyses, d'autre part.
22. Le Comité sectoriel prend acte du fait que les personnes concernées seront informées du traitement en exécution de l'article 14 de l'arrêté d'exécution. Cela implique que les informations suivantes seront communiquées: l'identité du responsable du traitement, les catégories de données à caractère personnel qui sont traitées, l'origine des données, une description précise des fins historiques, statistiques ou scientifiques du traitement, les destinataires ou les catégories de destinataires des données à caractère personnel, l'existence d'un droit de consultation de ses propres données à caractère personnel et d'un droit de

rectification de celles-ci, l'existence d'un droit d'opposition de la personne concernée.

D. MESURES DE SÉCURITÉ

- 23.** Conformément à l'article 16, § 4, de la loi relative à la vie privée, les demandeurs doivent 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.
- 24.** 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 documentation¹⁰.
- 25.** Le Comité sectoriel prend acte du fait que les données à caractère personnel codées seront traitées sous le contrôle et la surveillance d'un professionnel des soins de santé, plus précisément un médecin. La sprl IMS Health confirme également la désignation d'un conseiller en sécurité de l'information. Elle déclare qu'elle organise, à des intervalles réguliers, des cours pour l'ensemble du personnel concernant la sécurité et la confidentialité des données à caractère personnel. Elle dispose d'une version papier de la politique de sécurité qui contient une mention du secret professionnel et une obligation d'information ainsi que des dispositions relatives à l'utilisation d'un ordinateur fixe ou portable et à la surveillance par caméra. Des mesures techniques et contractuelles ont été prises afin d'éviter l'accès non autorisé aux données à caractère personnel. Elle dispose d'un plan de *business contingency* qui contient des mesures permettant d'éviter des dégâts physiques qui risqueraient de compromettre les données à caractère personnel. Ce plan décrit aussi les procédures d'urgence en cas d'incidents de protection ainsi que les différentes mesures de gestion prises. La sprl IMS Health a, en outre, établi une

¹⁰ « 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 suivante: 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

liste actualisée des différentes personnes qui ont accès aux données à caractère personnel et a communiqué celle-ci au Comité sectoriel. Elle propose, par ailleurs, d'organiser annuellement un audit interne afin de contrôler la validité et l'efficacité des mesures techniques et organisationnelles mises en place. Le Comité sectoriel confirme en effet l'opportunité de cet audit. Le Comité sectoriel prend finalement acte du fait que la sprl IMS prévoit les dispositifs de loggings et de détection adéquats pour la réalisation des contrôles nécessaires, de sorte qu'en cas de nécessité, il est possible de retrouver l'identité de toute personne qui a eu accès aux données à caractère personnel ou les a traitées.

26. Le Comité sectoriel rappelle qu'il est interdit, conformément à l'article 6 de l'arrêté d'exécution, 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 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 personnel¹¹.

Par ces motifs,

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

accorde une autorisation pour la communication de données à caractère personnel codées relatives à la santé par les hôpitaux à la sprl ISM Health, en vue de la réalisation d'activités de benchmarking, d'une part, et d'études et d'analyses, d'autre part.

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.

¹¹ Article 41 de la loi relative à la vie privée.