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

CSI/CSSS/19/018

DÉLIBÉRATION N° 13/117 DU 19 NOVEMBRE 2013, MODIFIÉE LE 18 NOVEMBRE 2014 ET LE 15 JANVIER 2019, PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES RELATIVES À LA SANTÉ PAR L'AIM, LE SPF SANTÉ PUBLIQUE ET LA DIRECTION DE L'INFORMATION POLICIÈRE OPÉRATIONNELLE À 'VRIJE UNIVERSITEIT BRUSSEL' ET À L'INSTITUT BELGE POUR LA SÉCURITÉ ROUTIÈRE, DANS LE CADRE D'UNE ÉTUDE SCIENTIFIQUE SUR L'ENREGISTREMENT ET LE COÛT DES ACCIDENTS DE LA ROUTE (REKOVER)

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

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 13 décembre 2006 portant dispositions diverses en matière de santé;

Vu la délibération n° 13/117 du 19 novembre 2013 et du 18 novembre 2014;

Vu le rapport d'auditorat de la Plate-forme eHealth du 7 novembre 2014 et du 11 décembre 2018;

Vu le rapport de monsieur Bart Viaene;

Émet, après délibération, la décision suivante, le 15 janvier 2019:

I. OBJET DE LA DEMANDE

1. Le groupe de recherche '*Interuniversity Centre for Health Economics Research*' associé à la Vrije Universiteit Brussel et l'Institut belge pour la Sécurité routière planifient une étude scientifique commune sur la qualité de l'enregistrement, la sévérité et les implications des blessures et le coût des accidents de la route pour la société.

2. Cette étude scientifique requiert le couplage et le codage de données à caractère personnel relatives à la santé provenant de différentes sources, plus précisément:

   - de la banque de données des accidents de la CGO (Direction de l'information policière opérationnelle)

   - de la banque de données du SPF Santé publique contenant des résumés hospitaliers minimums (RHM), à l'intervention de la Cellule technique

   - de la banque de données de l'Agence intermutualiste (AIM).

3. Les personnes enregistrées dans l'étude sont toutes les personnes qui, dans la période de 2008 à aujourd'hui:

   - étaient hospitalisées en Belgique à cause de leur implication dans un accident de la route[1]

   - ont subi une consultation dans un service d'urgence en raison de leur implication dans un accident de la route[2]

   - sont mentionnées dans la banque de données des accidents de la CGO (unité de la Police fédérale)

4. Les chercheurs estiment que les critères de sélection donneront finalement lieu à la sélection d'environ 220.000 personnes par année.

5. Les données à caractère personnel suivantes seront communiquées à la banque de données des accidents de la CGO :

   - numéro de registre national (à coder), sexe et âge (code entre 0 et 99)

   - type d'usager de la route (piéton, cycliste, voiture, ...)

   - conséquences (tué, grièvement blessé, légèrement blessé, indemne)

   - conducteur/passager, place dans le véhicule

   - code-lettre par usager de la route (A, B, C, ...): par partie impliquée dans un accident de la route

---

[1] Les personnes sont sélectionnées dans la banque de données RHM lorsque pour la variable "CODE_DIAGNOSE" (M1/Veld8) un des codes suivants relatifs à des causes externes spécifiques à des accidents de la route a été complété: soit E810-E819, E827, E829, E929.0 of E988.5.

[2] Les personnes sont sélectionnées dans la banque de données RHM lorsque la variable "M6_TYPE_INFO_SPOED" (M6/Veld6) est égale à "O" (rôle dans l'accident de la route éventuel).

- pays d'immatriculation du véhicule

- année, mois, jour et heure de l'accident de la route

- types de route et régime de vitesse de la route, sur / en dehors d'un carrefour, agglomération, code postal du lieu de l'accident

- type d'accident

- usagers de la route impliqués dans les accidents suivant le code-lettre: première, deuxième et troisième collision

- facteurs d'accident usager de la route (p.ex. brûler un feu rouge, ne pas céder pas la priorité, ...)

- facteurs d'accident véhicule (p.ex. pas d'éclairage ou éclairage incorrect, pneus usés, ...)

- facteurs d'accidents conditions de la route ou de circulation (p.ex. mauvais état de la route ou de la piste cyclable, mauvaise signalisation, ...)

- code-lettre et lieu du deux-roues, modalité si le deux-roues emprunte la piste cyclable ou la quitte

- code-lettre et lieu du piéton, modalité si le piéton traverse la chaussée

6. Les données à caractère personnel suivantes provenant de la banque de données Résumés hospitaliers minimums sont communiquées par le SPF Santé publique:

Domaine 3: données administratives

- provenant du fichier PATHOSPI: année d'enregistrement et année de naissance

- provenant du fichier STAYHOSP: année d'enregistrement, dates d'admission et de sortie hôpital, nombre total de journées d'hospitalisation complètes à facturer (jusqu'à la fin de la période d'enregistrement) pour le séjour à l'hôpital, code de réadmission, type d'admission, sexe, code postal Belgique, code pays, indicateur nationalité, provenance, destination, type de sortie, diagnostic d'admission vérifié, type de séjour, code statut d'assurance patient

- provenant du fichier STAYSPEC: année d'enregistrement et code spécialité

- provenant du fichier STAYINDX: nombre de journées d'hospitalisation complètes à facturer au cours de l'année de référence, nombre de journées d'hospitalisation complètes à enregistrer au cours de l'année d'enregistrement précédente, code indice lit pour la facturation et ordre chronologique des différents indices lits

Domaine 5: Données médicales

- provenant du fichier Diagnostic (M1): numéro d'ordre spécialité, code diagnostic principal / complémentaire, code diagnostic

- provenant du fichier Urgadmin (M6): code info urgences, raison admission aux urgences/rôle dans l'accident/suivi/traitement/type de lésion

- Fichier calculé: APR_DRG 15 (catégorisation des blessures et lésions suivant le système de classification international appliqué), degré de sévérité des blessures, risque de mortalité.

7. Les données à caractère personnel suivantes sont communiquées par l'Agence intermutualiste:

- provenant du fichier Pharmanet : identification bénéficiaire (à coder), date de la délivrance, code de la catégorie du médicament, nombre, intervention AMI 1, part personnelle, réduction du montant de remboursement/contribution des pharmaciens, intervention AMI 2[3];

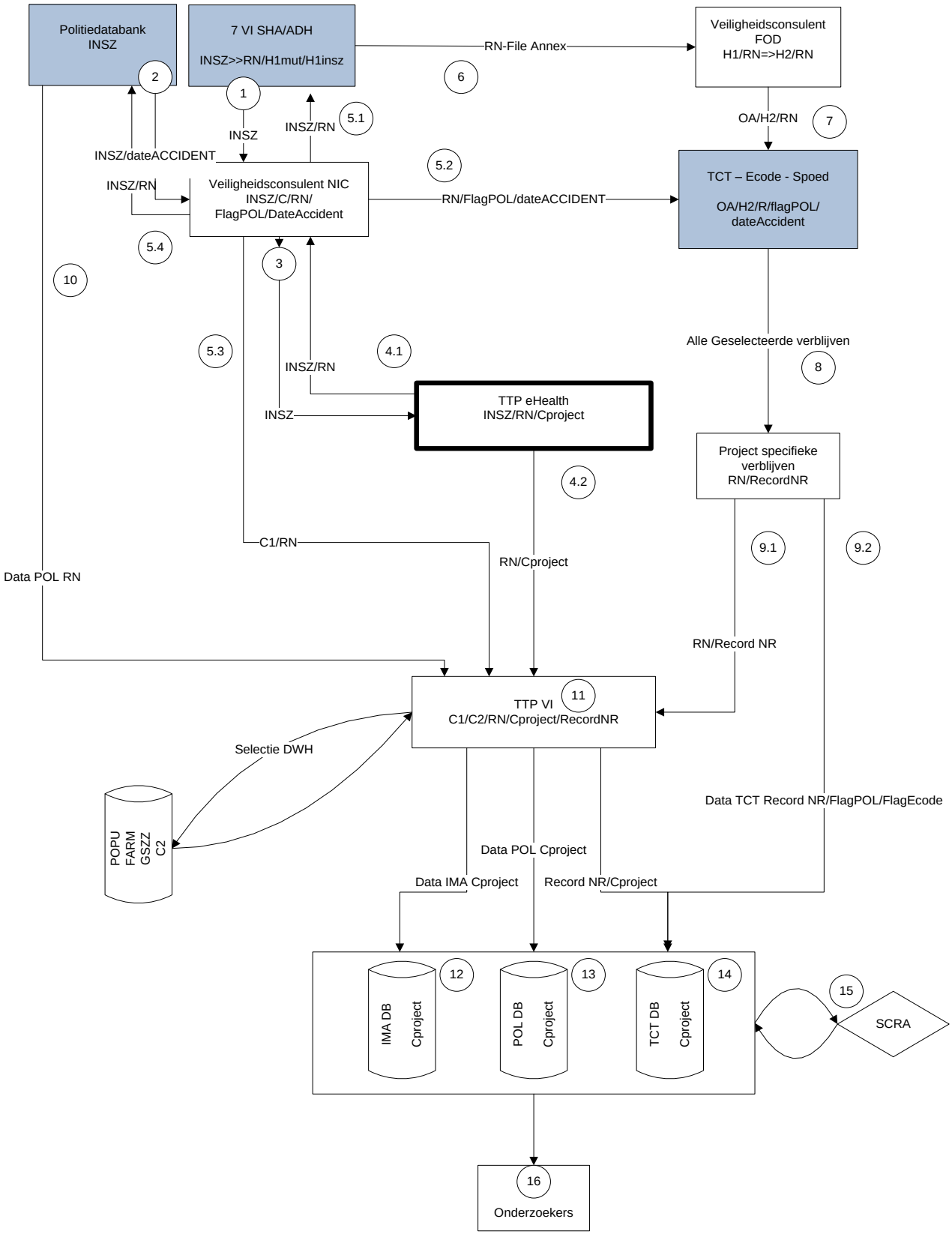
- provenant du fichier Données de soins de santé : identification du bénéficiaire (à coder), date de début de la prestation, code nomenclature, nombre de cas, nombre de jours, montant remboursement, qualification du prestataire de soins, code de service, date admission, date sortie, nuit/weekend, intervention personnelle, supplément, régime du tiers payant[4];

- provenant du fichier Population: identification bénéficiaire (à coder), année-mois de décès, situation sociale, nature montant des revenus, origine reconnaissance comme personne handicapée, omnio, forfait B soins infirmiers, forfait C soins infirmiers, kinésithérapie E ou physiothérapie, allocation d'intégration pour personnes handicapées, allocation d'invalidité majorée pour l'aide de tierces personnes, allocation forfaitaire pour l'aide de tierces personnes, MAF, droit à un revenu garanti, garantie de revenus aux personnes âgées ou revenu d'intégration sociale, droit à l'allocation aux personnes handicapées, droit à une aide du CPAS, nombre de jours d'incapacité de travail, nombre de jours de maladie en raison d'invalidité[5].

Les variables suivantes sont indispensables au couplage des RHM aux données provenant de la banque de données de l'AIM; toutefois, les données suivantes ne sont pas communiquées aux chercheurs: identification bénéficiaire, établissement de séjour, date du séjour, date de sortie[6].

8. Le couplage et le codage des données à caractère personnel provenant des différentes sources de données interviendront comme suit:

[3] SS00010, SS00015, SS00020, SS00050, SS00060, SS00160, SS00165, SS00195.
[4] SS00010, SS00015, SS00020, SS00050, SS00055, SS00060, SS00065, SS00080, SS00110, SS00115, SS00145, SS00160, SS00165, SS00175.
[5] PP00165, PP0040, PP1003, PP1008, PP1009, PP1010, PP2001, PP2002, PP2003, PP2005, PP2008, PP2009, PP3001-2, PP3010, PP3011, PP3013, PP4002, PP4003.
[6] SS00010, SS00075, SS00110, SS00115.


Politiedatabank
INSZ
7 VI SHA/ADH
INSZ>>RN/H1mut/H1insz
RN-File Annex
Veiligheidsconsulent
FOD
H1/RN=>H2/RN
2
1
6
INSZ
INSZ/RN
5.1
OA/H2/RN
7
INSZ/dateACCIDENT
5.2
INSZ/RN
Veiligheidsconsulent NIC
INSZ/C/RN/
FlagPOL/DateAccident
RN/FlagPOL/dateACCIDENT
TCT – Ecode - Spoed
OA/H2/R/flagPOL/
dateAccident
5.4
3
10
5.3
4.1
Alle Geselecteerde verblijven
8
INSZ/RN
TTP eHealth
INSZ/RN/Cproject
INSZ
Project specifieke
verblijven
RN/RecordNR
4.2
C1/RN
RN/Cproject
9.1
9.2
Data POL RN
RN/Record NR
11
TTP VI
C1/C2/RN/Cproject/RecordNR
Selectie DWH
Data TCT Record NR/FlagPOL/FlagEcode
POPU
FARM
GSZZ
C2
Data POL Cproject
Data IMA Cproject
Record NR/Cproject
12
13
14
15
IMA DB
Cproject
POL DB
Cproject
TCT DB
Cproject
SCRA
16
Onderzoekers

Abréviation	Explication
NISS	Numéro d'identification de la sécurité sociale
C_1	Numéro d'identification pseudonymisé unique du patient qui est utilisé dans le flux de données entre les organismes assureurs et l'AIM.
C_2	Numéro d'identification pseudonymisé unique du patient attribué par la TTP des OA (BCSS). Il s'agit du numéro d'identification pseudonymisé unique du patient sous lequel les données sont enregistrées dans le DWH de l'AIM.
H_1	Numéro d'identification pseudonymisé du patient utilisé dans le circuit de codage RHM-SHA/HJA nécessaire au couplage des données des hôpitaux par la Cellule technique. Ce numéro est connu par les organismes assureurs et les hôpitaux.
H2	Numéro d'identification du patient doublement pseudonymisé qui est utilisé par la TCT
RN	Numéro aléatoire TTP-eHealth. Il s'agit du numéro sous lequel les données seront enregistrées pendant le transport des données. Cela garantit que les émetteurs ne recevront jamais le lien avec le Cproject.
RecordNR	Numéro d'enregistrement
Cproject	Numéro d'identification pseudonymisé unique spécifique pour ce projet
SPOC-POL	Signal point of contact banque de données des accidents (CGO)
CIN	Collège intermutualiste national
TTP	Trusted third party
MUT	Union d'affiliation
DateAccident	Date de l'accident dans la banque de données des accidents (CGO)
TCT	Cellule technique
OA	Organismes assureurs

Description détaillée du flux de données et du codage

1. Sélection des NISS auprès des 7 OA pour tous les SHA et HJA. Les 7 OA envoient au conseiller en sécurité du CIN tous les NISS pour la période 2008 à 2013.

2. Sélection des NISS (en ce compris le "pseudo" NISS) avec le DateAccident (date de l'accident dans la banque de données des accidents) dans la banque de données des accidents (CGO). Cette liste NISS/DateAccident est transmise au conseiller en sécurité du CIN.

3. Le conseiller en sécurité du CIN (DBA) fusionne les listes des OA et de la banque de données des accidents, supprime les doublons, maintient le DateAccident et crée un FlagPOL avec l'indication selon laquelle le numéro était présent dans le fichier du SPOC-POL. Le conseiller en sécurité du CIN transmet la liste complète contenant les seuls NISS (et pseudo-NISS) à la TTP Ehealth.

4. La TTP-eHealth procède au codage NISS/RN/Cproject.

4.1. eHealth envoie la liste NISS/RN au conseiller en sécurité du CIN.

4.2. eHealth envoie la liste RN/Cproject à la TTP-OA (BCSS).

5. Le conseiller en sécurité possède un tableau principal NISS/C1/RN/FlagPOL/DateAccident.

5.1. Le conseiller en sécurité du CIN renvoie la liste NISS/RN aux OA pour les NISS que ces derniers ont communiqués au cours de l'étape 1.

5.2. Le conseiller en sécurité du CIN fournit la liste RN/FlagPOL/DateAccident à la TCT.

5.3. Le conseiller en sécurité du CIN fournit la liste C1/RN à la TTP-OA (BCSS).

Cette liste est utilisée par la TTP-OA (BCSS) qui transpose finalement toutes les données en Cproject.

5.4. Le conseiller en sécurité du CIN fournit la liste NISS/RN au gestionnaire de la banque de données des accidents pour les NISS contenant un FlagPOL.

6. Les OA remplacent les NISS dans leurs fichiers par RN et transmettent ceux-ci au conseiller en sécurité du SPF. Le conseiller en sécurité du SPF recevra la table de concordance RN/H1 par OA et la transformera en RN/H2.

7. Le conseiller en sécurité du SPF transmet la table de concordance RN/H2 par OA à la TCT.

8. Au cours de 5.2, le RN/FlagPOL/DateAccident est envoyé à la TCT. La sélection est réalisée par la TCT au moyen des critères de sélection élaborés sur les données des RHM et de FlagPOL.

9. La TCT crée, par séjour, un RecordNR et ainsi le tableau RN/RecordNR.

9.1. La TCT envoie la liste RN/RecordNR à la TTP-OA (BCSS).

9.2. La TCT transmet les données TCT (RHM) sous RecordNR à DWH-Project.

Au moyen du RecordNR/liste RN, le Cproject est introduit dans les données TCT.

10. Les données de la banque de données des accidents sont converties en RN au moyen de la table NISS/RN obtenue au point 4.2 et envoyées sous RN à la TTP-OA (BCSS).

11. La TTP-OA (BCSS) sélectionne pour tous les RN sélectionnés par la TCT ainsi que pour tous les RN présents dans la banque de données des accidents les données AIM dans le DWH AIM.

12. La TTP-OA (BCSS) prépare les données AIM dans le DWH_project sous Cproject.

13. Les données de la banque de données des accidents sont transposées par la TTP-OA (BCSS) en Cprojet et sont mises à la disposition dans le DWH_project.

14. Les données de la TCT (RHM) sont préparées sous Cproject dans le DWH_project au moyen de la liste RecordNR/Cproject fournie par la TTP-OA (BCSS).

15. Réalisation de l'analyse quant aux risques small cells (AIM ou cellule technique).

16. Les données sont toutes mises à la disposition des chercheurs sous Cproject dans le DWH_project.

9. Les résultats finaux de l'étude seront résumés dans des rapports scientifiques. Par ailleurs, des articles seront aussi rédigés et publiés dans des revues scientifiques spécialisées, nationales ou internationales. Les demandeurs confirment que ces publications contiendront uniquement des données agrégées. Nombre total de cas, type de lésions, type d'accident. Le coût sera toujours communiqué par catégorie (p.ex. personnes âgées, cyclistes, enfants, piétons).

10. La fourniture des données des accidents visées par la police fédérale doit faire l'objet d'un arrêté d'exécution spécifique, en raison d'une modification de la loi relative à la gestion de l'information policière qui est survenue après l'obtention de l'autorisation originale du 19 novembre 2013. Étant donné que la désignation du personnel de recherche est limitée dans le temps, le demandeur estime qu'il n'est pas opportun d'attendre que l'arrêté d'exécution soit réalisé et il souhaite dès lors avoir uniquement recours, dans un premier temps, aux banques de données du SPF Santé publique et de l'AIM. Lors du codage, il ne sera donc pas fait appel à la banque de données de la CGO, dans une première phase. Concrètement, cela implique que, dans la première phase de l'extraction des données, la police fédérale n'apportera pas de données (voir les démarches 2, 5.2, 10 et 13 sous le point 8).

11. Dès que l'arrêté d'exécution sera signé, les données provenant de la banque de données de la CGO seront, dans une deuxième phase, ajoutées et couplées aux données à caractère personnel couplées du SPF Santé publique et de l'AIM selon la description détaillée ci-dessus. Toutefois, il est nécessaire que la Plate-forme eHealth soit autorisée à conserver le lien entre le numéro d'identification réel (NISS) et le numéro pseudonymisé, jusqu'à ce que le couplage avec les données de la banque de données des accidents ait lieu.

12. Le demandeur demande également que la Plate-forme eHealth procède au décodage afin de rapporter des problèmes relatifs à la qualité des données (par exemple, l'absence du contenu des variables, l'occurrence de valeurs impossibles) aux fournisseurs de données. Concrètement, cela signifie que les chercheurs communiqueront les problèmes de qualité survenus avec des numéros pseudonymisés, ainsi qu'une description de ces problèmes, à la Plate-forme eHealth qui ensuite décodera les numéros pseudonymisés et communiquera les numéros d'identification et la description du problème de qualité aux fournisseurs de données respectifs.

II. COMPÉTENCE

13. 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.

14. Par ailleurs, toute communication de données à caractère personnel par l'Agence intermutualiste requiert une autorisation de principe du Comité sectoriel, à l'exception de la mise à la disposition d'un échantillon représentatif permanent pseudonymisé.

15. 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.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

16. Le traitement de données à caractère personnel relatives à la santé est en principe interdit, et ce conformément au prescrit de l'article 9, 1er point, du Règlement (UE) n° 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 (dénommé ci-après RGPD).

17. L'interdiction ne s'applique cependant pas lorsque le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques et est effectué selon les conditions spécifiques de la réglementation relative à la protection de la vie privée.

B. FINALITÉ

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

19. Le Comité constate que le traitement de données à caractère personnel pseudonymisées est réalisé dans le cadre d'une étude scientifique sur les conséquences des accidents de la route. Cette étude est réalisée par une section de recherche de la VUB en collaboration avec l'IBSR. L'objectif de l'étude est d'inventorier le nombre total de victimes d'accidents de la route en Belgique et d'estimer, le plus correctement possible, le coût engendré par les accidents de la route pour la société. Les demandeurs déclarent que cet input de données plus correctes et pertinentes sera bénéfique pour la politique de la sécurité routière en Belgique. De plus, l'étude scientifique permettra d'améliorer l'instrument d'évaluation pour les analyses coût-bénéfice des mesures politiques prises en matière de sécurité routière (p.ex. stratégies de prévention pour certains groupes cibles).

C. PROPORTIONNALITÉ

20. 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. Le responsable du traitement ne peut traiter des données à caractère personnel pseudonymisées que si la finalité scientifique ne peut être réalisée au moyen de données anonymes. Etant donné que l'étude en question requiert le couplage de données à caractère

personnel provenant de différentes sources de données, la communication de données anonymes ne suffit pas. Des données à caractère personnel pseudonymisées sont effectivement nécessaires.

22. Les demandeurs avancent les arguments selon lesquels les données à caractère personnel pseudonymisées provenant de la banque de données des accidents contiennent les caractéristiques nécessaires de l'accident et des personnes impliquées dans l'accident de la route. Les données hospitalières minimales provenant du SPF Santé publique contiennent des informations relatives aux lésions ainsi que les données hospitalières des personnes impliquées dans l'accident de la route. Les données à caractère personnel pseudonymisées de la banque de données de l'AIM, qui contient des informations relatives à la consommation des soins de santé, sont demandées pour l'année antérieure à l'accident et pour l'année postérieure à l'accident. C'est ainsi que le coût attribuable à l'accident de la route peut être déterminé. Le Comité a reçu une justification détaillée pour toutes les données.

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

24. 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 les analyses seront réalisées au plus tard dans une période de trois ans à compter de la réception des données à caractère personnel pseudonymisées et couplées.

Le Comité a cependant reçu une demande de prolongation du délai de conservation d'un an car les chercheurs sont d'avis que les possibilités de recherche en vue de la finalité sociale envisagée n'ont pas encore été suffisamment exploitées. Dans l'année qui vient, les chercheurs souhaitent, au sein de I-CHER, se concentrer sur les sous-groupes de victimes d'accidents de la route (p.ex. les usagers doux ou par type de lésion). Cette série de données au niveau de la population permet de réaliser de telles analyses de sous-groupes. Un premier pas en ce sens fut l'étude visant à déterminer le coût incrémental des personnes victimes d'une lésion cérébrale traumatique. Outre une subdivision sur la base d'informations diagnostiques, il est possible de définir des sous-groupes sur la base d'autres facteurs, par exemple des caractéristiques personnelles, les circonstances de l'accident, les traitements pendant la phase aiguë ou pendant la phase subaiguë, les caractéristiques du trajet de soins, etc. Cette valorisation de la série de données détaillée n'est toutefois pas possible endéans le délai pour lequel une autorisation a été accordée (initialement jusqu'au 31 décembre 2018). Vias Institute souhaite pouvoir réaliser des analyses supplémentaires et plus détaillées concernant la nature des lésions et la gravité des lésions par type d'usager de la route et catégorie d'âge. Outre MAIS, ISS et NISS, le Vias Institute souhaite calculer d'autres indicateurs de gravité sur la base des données REKOVER. Finalement, les chercheurs souhaitent exécuter des analyses de séries chronologiques et notamment prédire le nombre de victimes MAIS3+ après 2011.

Le Comité décide que le délai de conservation peut être prolongé d'un an et que les données à caractère personnel pseudonymisées devront être détruites au plus tard le 31 décembre 2019.

25. Le Comité souligne que les résultats de l'étude ne peuvent pas être publiés sous une forme qui permet l'identification de la personne concernée.

26. Le Comité prend acte du fait que la Plate-forme eHealth interviendra, conformément à l'article 5, 8° de la loi du 21 août 2008 relative à l'institution et à l'organisation de la Plate-forme eHealth, lors du codage des numéros d'identification des personnes concernées. Etant donné que les données de la banque de données des accidents de la CGO seront ajoutées et couplées, à un stade ultérieur, aux données à caractère personnel couplées de l'AIM et du SPF Santé publique, il est nécessaire que le lien entre le numéro d'identification réel et le numéro pseudonymisé soit conservé jusqu'à la fin de la recherche qui est prévue au 31 décembre 2019.

27. La possibilité de décodage par la Plate-forme eHealth est acceptable, mais uniquement afin de rapporter d'éventuels problèmes de qualité ou de complétude des données aux fournisseurs de données. Concrètement, cela signifie que les chercheurs communiqueront les problèmes de qualité survenus avec des numéros pseudonymisés et la description de ces problèmes à la Plate-forme eHealth qui ensuite procèdera au décodage des numéros pseudonymisés et communiquera les numéros d'identification et la description des problèmes de qualité aux fournisseurs de données respectifs.

28. Afin de s'assurer qu'il n'y ait pas de risque de réidentification à partir des données à caractère personnel codées, le Comité estime qu'il est nécessaire qu'une analyse de risque "small cell" soit effectuée sur les données à caractère personnel pseudonymisées et couplées, comme proposé par les chercheurs. Si nécessaire, les agrégations requises doivent être réalisées, afin d'éviter que le caractère exceptionnel de certaines combinaisons de données à caractère personnel (appelées les "small cells") donnent lieu à une réidentification. Le Comité sectoriel confirme que l'Agence intermutualiste s'en chargera, vu son intervention lors de la mise à la disposition matérielle des données à caractère personnel pseudonymisées.

D. TRANSPARANCE

29. Si les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement doit fournir certaines informations, dès l'enregistrement des données à caractère personnel, ou lorsqu'une communication de données à caractère personnel à un tiers est envisagée, au plus tard au moment de la première communication des données à caractère personnel.

30. 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 pseudonymiser des données à caractère

personnel et qu'elle est soumise, à cet égard, à des mesures spécifiques visant à protéger la vie privée. Vu l'intervention de la Plate-forme eHealth lors de la pseudonymisation des données à caractère personnel, les demandeurs sont par conséquent dispensés de la notification aux intéressés.

E. DÉCLARATION DU TRAITEMENT À LA COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE

31. En vertu de l'article 17 de la loi relative à la vie privée[7], le responsable du traitement devait, avant de mettre en œuvre un traitement entièrement ou partiellement automatisé, faire une déclaration à la Commission de la protection de la vie privée. Les demandeurs devront donc s'en charger.

F. MESURES DE SÉCURITÉ

32. 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 ce n'est pas strictement requis dans la loi relative à la vie privée, le Comité estime qu'il est préférable de traiter de telles données sous la responsabilité d'un médecin. 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.

33. Le Comité prend acte du fait que le traitement des données à caractère personnel pseudonymisées par les demandeurs se fera effectivement sous la surveillance et la responsabilité d'un médecin associé à l'UZ Brussel.

34. 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.

35. 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;

[7] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

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[8].

36. Les demandeurs ont établi une liste de personnes qui ont accès aux serveurs de l'AIM, sur lesquels les données à caractère personnel pseudonymisées et couplées sont mises à la disposition via une connexion VPN sécurisée. Les demandeurs font savoir que les chercheurs sont obligés, en vertu d'un contrat, de traiter les données, de manière déontologique et éthique. Ils doivent également respecter la confidentialité des données.

37. Le Comité prend acte du fait que la VUB a désigné un conseiller en sécurité. L'IBSR désignera à l'avenir un conseiller en sécurité pour l'institution dans son ensemble. Pour la présente étude, il fera toutefois appel à un conseiller en sécurité de l'AIM. Les chercheurs de l'IBSR et de la VUB ont accès au datawarehouse qui est stocké à l'AIM, via une connexion VPN par chercheur (toute connexion VPN est sécurisée au moyen d'un mot de passe personnel). L'AIM possède un système de loggings qui permet de conserver en permanence quels objets ont été créés, consultés ou supprimés par chaque chercheur au moyen de sa connexion VPN. Bien que les chercheurs puissent télécharger des données agrégées du datawarehouse central vers le serveur de l'institution même, l'AIM veille à ce qu'il soit impossible pour les chercheurs de télécharger le datawarehouse complet (ainsi que des données à un niveau individuel).

38. Il est interdit d'entreprendre toute action visant à convertir les données à caractère personnel pseudonymisées qui ont été communiquées en données à caractère personnel non pseudonymisées.

[8] « 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.pdf

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

conclut que la communication des 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 conservation des données et de sécurité de l'information.

La Plate-forme eHealth est autorisée à conserver le lien entre le numéro d'identification réel et le numéro pseudonymisé jusqu'au 31 décembre 2019 en vue du codage qui se fera en étapes et du couplage des données à caractère personnel, tels que décrits sous les points 10, 11 et 28. La Plate-forme est également autorisée à procéder au décodage, mais uniquement dans la situation spécifique qui est décrite sous les points 12 et 29.

Bart VIAENE