Comité de sécurité de l'information

Chambre sécurité sociale et santé

CSI/CSSS/25/102

DÉLIBÉRATION N° 25/050 DU 4 MARS 2025 PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES RELATIVES À LA SANTÉ PAR LE SPF SANTÉ PUBLIQUE, SÉCURITÉ DE LA CHAÎNE ALIMENTAIRE ET ENVIRONNEMENT ET L'INSTITUT NATIONAL D'ASSURANCE MALADIE ET INVALIDITÉ (INAMI) À L'UNIVERSITEIT HASSELT DANS LE CADRE DE LA CHAIRE : 'LIMBURGS KANKERFONDS EN STOP DARMKANKER: DATA IN DE STRIJD TEGEN DARMKANKER'

Le Comité de sécurité de l'information ;

Vu le 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* (Règlement général relatif à la protection des données ou RGPD);

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

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment l'article 37 ;

Vu la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé,* en particulier l'article 42, § 2, 3°, modifié par la loi du 5 septembre 2018 ;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant dispositions diverses* ;

Vu la demande de l'Universiteit Hasselt ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 24 février 2025 ;

Vu le rapport de monsieur Michel Deneyer ;

Émet, après délibération, la décision suivante, le 4 mars 2025 :

I. OBJET DE LA DEMANDE

1. La présente demande de données est introduite dans le cadre de la Chaire: 'Limburgs Kankerfonds en Stop Darmkanker: data in de strijd tegen darmkanker'. Dans le cadre de cette chaire, des travaux de recherche sont menés sur le cancer colorectal en Flandre, dans le but d'acquérir de nouvelles connaissances sur l'ensemble du trajet de soins des patients atteints de cancer colorectal. La recherche vise à améliorer les processus de soins et à identifier les évolutions et les facteurs à risques afin de contribuer aux progrès scientifiques et à la politique de santé publique.

2. Par ailleurs, dans le cadre de la chaire, il est développé un tableau de bord collectant toutes les données actuelles relatives au cancer colorectal. Ce tableau de bord permettra de mieux informer et sensibiliser la population flamande, les prestataires de soins et les responsables politiques. Le but est d'identifier le trajet de soins complet d'un cancer colorectal, en ce compris les hospitalisations en vue du diagnostic et de la prise en charge médicale.

3. Afin de bien comprendre et d'analyser ce trajet, les chercheurs demandent à obtenir un accès aux données relatives aux hospitalisations en Flandre liées aux diagnostics de cancer colorectal. Ces données sont cruciales pour une analyse approfondie du parcours de soins de patients, débutant avant le diagnostic pour se terminer après la prise en charge médicale et la sortie de l'hôpital. Les enseignements tirés de ces analyses contribueront à la fois à la recherche scientifique et à la connaissance et à la compréhension de la population générale.

4. Les analyses que les chercheurs souhaitent réaliser au moyen de ces données concernent des statistiques descriptives telles que le nombre d'admissions par jour, ventilé en fonction de l'âge, du sexe et du pourcentage de réadmissions. Tous les résultats sont exclusivement présentés à un niveau agrégé dans le tableau de bord et sont accompagnés des précisions et du contexte utiles, de sorte qu'ils soient accessibles et compréhensibles pour un large public.

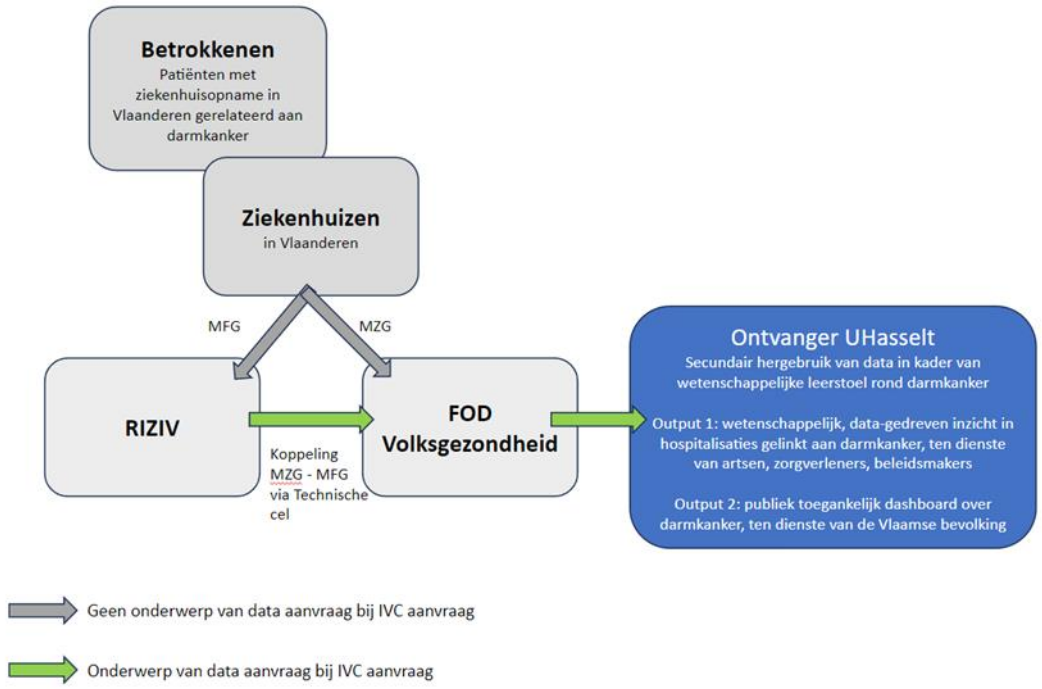
5. Par ailleurs, plusieurs analyses statistiques seront réalisées dont les résultats pertinents pourront être partagés et/ou publiés dans le tableau de bord. Les publications sur la base de ces analyses auront toujours lieu en accord avec le SPF et les autres parties prenantes.

6. Les personnes concernées sont tous les patients domiciliés en Flandre (domicile avec code postal flamand) qui sont hospitalisés sur la base d'un diagnostic lié à un cancer colorectal (sur la base des codes ICD-9-CM et ICD-10-BE) qui a été enregistré dans la banque de données des Résumés Hospitaliers Minimums (RHM) gérée par le SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement. De plus, un couplage est demandé entre les RHM et la banque de données des résumés financiers minimums (RFM) gérée par l'Institut national d'assurance maladie et invalidité (INAMI).

7. Les chercheurs disposent déjà de données relatives au dépistage et à l'incidence du cancer colorectal depuis 2010. Afin de pouvoir réaliser des analyses complètes et cohérentes, ils demandent à obtenir des données relatives à l'hospitalisation à partir de 2010. Vu la modification intervenue dans le codage et le passage de l'ICD-9-CM vers l'ICD-10-BE en 2014, l'absence des données de la Cellule technique pour l'année 2012 et l'absence des

données en 2015, ils utiliseront pour leurs analyses statistiques uniquement des données à partir de 2016. Pour les statistiques agrégées, les données à partir de 2010 seront utilisées, étant donné que ces analyses sont moins sensibles pour les petites différences en termes de codage et d'enregistrement. Certaines données qui sont seulement disponibles à partir d'une date ultérieure, ne sont pas non plus nécessaires pour les analyses descriptives envisagées. Compte tenu du nombre de 20.000 hospitalisations enregistrées par an, la banque de données contient pour la période de 2010 à 2022, au total, plus de 240.000 séjours pour l'ensemble de la Belgique. Si l'on tient compte du pourcentage de la population en Flandre, cela représente environ 139.000 enregistrements en Flandre. Toutes les données collectées dans cette banque de données sont pertinentes et nécessaires pour identifier et illustrer le trajet de maladie complet des patients souffrant d'un cancer colorectal.

8. Aperçu schématique des flux de données :



L'objet de la présente demande de données concerne la flèche verte dans la représentation schématique, à savoir le flux de données issues de la banque de données des Résumés hospitaliers minimums gérée par le SPF Santé publique qui sont couplées aux Résumés financiers minimums (INAMI) par l'intermédiaire de la Cellule technique, flux qui est transmis à l'équipe de recherche de l'Universiteit Hasselt. Le SPF transmettra les données au moyen du logiciel de chiffrement: GPG4win. L'UHasselt a recours à l'enregistrement de données dans le Google Cloud (sous-traitant) et souhaite traiter les données en vue de la réalisation d'une étude scientifique et du développement d'un tableau de bord informatif relatif au cancer colorectal, accessible à tous.

II. COMPÉTENCE

9. En vertu de l'article 42, § 2, 3° de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, la chambre sécurité sociale et santé du Comité de sécurité de l'information est compétente pour rendre une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé.

10. 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

A. ADMISSIBILITÉ

11. Le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes et le traitement de données à caractère personnel relatives à la santé est en principe interdit.[1]

12. L'interdiction du traitement de données à caractère personnel relatives à la santé ne s'applique 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, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre, qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.[2]

13. Cette demande de données s'inscrit dans le cadre d'une étude statistique, épidémiologique et scientifique de la Data Science Institute de l'Universiteit Hasselt. L'Universiteit Hasselt est une institution publique. L'Universiteit Hasselt renvoie à la réglementation suivante: le « Codex Hoger Onderwijs » du 11 octobre 2013; le Décret du 20 juin 2008 portant le statut de l'Universiteit Hasselt et du 'Hoge Raad voor het Hoger Onderwijs in Limburg' (Conseil supérieur de l'Enseignement supérieur au Limbourg).

14. L'université a pour tâche de permettre des recherches à large but social. Elle demande de pouvoir traiter les données demandées vu qu'elle remplit une mission d'intérêt général. Le décret du 8 juin 2008 portant le statut de l'Universiteit Hasselt et du 'Hoge Raad voor het Hoger Onderwijs in Limburg' dispose que l'UHasselt est une institution universitaire dotée de la personnalité juridique. La réalisation de recherches scientifiques est une tâche qui est explicitement confiée aux universités en Flandre par l'article II.18 du « Codex Hoger Onderwijs » (Code de l'Enseignement supérieur).

[1] Art. 9, point 1 RGPD.
[2] Art. 9, point 2, j), du RGPD.

15. Le RHM est un système d'enregistrement pseudonymisé de données administratives, médicales et infirmières. Tous les hôpitaux non psychiatriques de Belgique sont tenus d'y contribuer. Les objectifs du RHM sont de:

a) soutenir la politique de santé du gouvernement, notamment, en vue de prévoir les besoins en matière de services hospitaliers, de définir la politique épidémiologique ;
b) soutenir la politique de santé au sein des hôpitaux, notamment, par la production d'un feed-back général et de feed-backs individuels.

16. Conformément à l'article 10 de 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*, les données qui sont reprises dans la base de données hospitalières (RCM/RHM) peuvent être mises à la disposition de tiers dans le cadre d'une étude unique et temporaire. Ces études doivent s'inscrire dans les objectifs visés à l'article 3 et 19 du présent arrêté. En outre, l'étude doit toujours être de nature purement scientifique et donc ne poursuivre aucun but commercial. À cet effet, le demandeur doit: a) adresser une demande motivée au responsable du traitement, précisant de quelles données il souhaite disposer et pour quelle étude, quelle application, quelle durée, ...; b) disposer de l'autorisation de principe du Comité sectoriel compétent visé à l'article 31bis 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 ; c) détruire les données après la finalisation de l'étude concernée.

17. A la lumière de ce qui précède, le Comité est d'avis qu'il existe un fondement admissible pour le traitement des données à caractère personnel pseudonymisées relatives à la santé envisagé.

B. FINALITÉ

18. Conformément à l'art. 5, b) du RGPD, le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes.

19. Les données ont initialement été recueillies pour d'autres finalités. Les chercheurs souhaitent réaliser un couplage entre les variables RHM et les frais de séjour. Ce couplage est possible dans le contexte de la collaboration entre le SPF Santé publique et l'INAMI. Pour tout patient hospitalisé, les hôpitaux envoient, sous forme anonyme, au SPF Santé publique, les diagnostics médicaux (RCM) ainsi que des informations relatives aux soins administrés et leur coût (SHA) à l'INAMI. La Cellule technique procède au couplage de ces données afin d'obtenir, par affection médicale, un aperçu des soins administrés et des frais remboursés par l'assurance maladie, et ce pour chaque hôpital individuellement ou pour tous les hôpitaux confondus (moyenne nationale).

20. L'objectif de cette demande de données est un objectif d'intérêt public, la Chaire ''Limburgs Kankerfonds en Stop Darmkanker: data in de strijd tegen darmkanker'.

1) *Soutien de la sensibilisation et des efforts de prévention*: Les Résumés hospitaliers minimums (données RHM) et les Résumés financiers minimums (données RFM) devront permettre de réaliser des études scientifiques visant à identifier les modalités de visite à l'hôpital par les patients souffrant d'un cancer colorectal, telles la fréquence et les différences régionales. Sur la base de ces constatations, les chercheurs pourront communiquer des informations aux prestataires de soins, aux médecins et aux responsables politiques et partager leurs visions avec des organisations responsables pour la mise au point de campagnes effectives et ciblées, par exemple afin de sensibiliser les gens et de promouvoir le dépistage du cancer colorectal.

2) *Enrichissement de la plateforme de recherche:* Ils examineront s'il est possible d'utiliser les données recueillies pour enrichir le tableau de bord relatif au cancer colorectal. En ajoutant des informations spécifiques relatives aux visites à l'hôpital par les patients ayant reçu un diagnostic de cancer, la plateforme permettra de donner davantage de détails sur les soins de santé liés à un cancer, ce qui est crucial pour les chercheurs, les prestataires de soins et les responsables politiques.

21. Il est important de préciser que les données sont uniquement utilisées en vue de la réalisation d'études scientifiques, dont les résultats agrégés seront éventuellement repris dans le tableau de bord. Le tableau de bord n'est pas une plateforme de données, il constitue plutôt un aperçu informatif de toutes les données disponibles, qui sont résumées, analysées et visualisées de manière accessible, et qui sont accompagnées d'explications sur la manière d'interpréter ces résultats.

22. Au vu des objectifs, le Comité considère que le traitement des données à caractère personnel envisagé poursuit bien des finalités déterminées, explicites et légitimes.

C. PROPORTIONNALITÉ

23. Conformément à l'art. 5, b) et c) du RGPD, 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.

24. Une liste des variables demandées avec motivation et un aperçu des analyses envisagées sont joints en annexe.

25. Le Comité fait observer que le recours au NISS n'est pas d'application. Aucune donnée exacte n'est communiquée.

26. Dans le cadre de la Chaire 'Limburgs Kankerfonds en Stop Darmkanker', des recherches sont menées sur le cancer colorectal en Flandre, dans le but d'acquérir de nouvelles connaissances sur le trajet de soins complet des patients souffrant d'un cancer colorectal. Cette étude vise à améliorer les processus de soins et à identifier les tendances et les facteurs à risques qui sont susceptibles de contribuer à des progrès scientifiques et à la politique de santé publique. En outre, il est développé un tableau de bord qui recueillera en un endroit

central, toutes les données disponibles relatives au cancer colorectal. L'objectif de la Chaire Cancer colorectal est d'offrir un ensemble de données pertinentes et accessibles, de sorte que la population générale, les prestataires de soins et les responsables politiques puissent aisément avoir accès à toutes les données nécessaires. Cette collecte contient notamment des données relatives aux hospitalisations qui sont directement liées au diagnostic du cancer colorectal, telles les colonoscopies et les prises en charge médicales.

27. L'étude vise à identifier des modèles en ce qui concerne le comportant et les trajets hospitaliers des patients souffrant d'un cancer colorectal. Les chercheurs étudieront la durée du séjour en relation avec des facteurs démographiques tels l'âge, le sexe, la nationalité et l'arrondissement, ainsi que des changements dans le temps. En recueillant et en analysant ces données, les chercheurs souhaitent mieux comprendre les besoins et résultats de soins de patients souffrant d'un cancer colorectal, ce qui peut finalement donner lieu à une amélioration des stratégies et de la politique de soins.

28. Dans le cadre de la Chaire, les chercheurs développeront un tableau de bord/site web qui regroupe des informations pertinentes relatives au cancer colorectal. Cette plateforme permettra de présenter des statistiques de synthèse concernant l'incidence, le pronostic, les participations aux dépistages, etc. en Flandre. Ces données seront représentées par des histogrammes, des diagrammes à barres, des graphiques circulaires et des graphiques linéaires.

29. Les chercheurs ont exclusivement recours à des données agrégées et ne visualiseront pas de données individuelles de patients. Chaque visualisation sera, en outre, accompagnée d'explications décrivant en détail et de manière accessible les données présentées et la manière dont la visualisation peut être interprétée. L'objectif est de rendre ces informations compréhensibles pour un large public.

30. Il est à cet effet important de noter que le site web des chercheurs contiendra des informations et des données relatives au cancer colorectal et que les graphiques et figures seront accompagnés de descriptions complémentaires. Toutefois, les données sous-jacentes ne seront jamais rendues accessibles au public. Cela signifie que le site web affichera uniquement des figures que les chercheurs auront sélectionnées au préalable et que les visiteurs ne pourront pas exécuter de *queries* ou générer de figures. S'il existe un risque de *small cell identification,* les résultats ne seront pas visualisés (ou avec un indicateur tel « ≤5 »). Les résultats publiés constituent toujours des résultats anonymes.

31. Le Comité fait observer qu'aucune SCRA ne sera réalisée. Les chercheurs motivent ceci par le fait que les mesures de pseudonymisation sont suffisantes. Les résultats contiendront toujours des données agrégées qui rendent impossible toute identification de patients individuels.

D. LIMITATION DE LA CONSERVATION

32. Conformément à l'article 5, §1er, e), du RGPD, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, §1er, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation).

33. La Chaire a été inaugurée le 15/03/2023 pour une durée de 3 ans. La date de fin officielle de la Chaire se situe donc début 2026. Si les chercheurs souhaitent que le tableau de bord soit tenu à jour à l'issue de la Chaire, ils peuvent éventuellement demander une prolongation. Les données finalement couplées seront conservées dans le Google Cloud sur des serveurs dans l'UE et auront fait l'objet d'un chiffrement standard.

E. TRANSPARENCE

34. Conformément à l'art. 12 du RGPD, le responsable du traitement doit prendre des mesures appropriées pour fournir toute information en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique.

35. L'article 14 du RGPD fixe les conditions auxquelles le responsable du traitement doit satisfaire lorsque des données à caractère personnel sont collectées concernant la personne concernée. Ainsi, les informations suivantes doivent notamment être communiquées: les coordonnées du responsable du traitement et du délégué à la protection des données, les catégories de données à caractère personnel si les données ne sont pas obtenues auprès des personnes concernées, les finalités du traitement et le fondement du traitement, les catégories de destinataires et, si le responsable du traitement a l'intention de transmettre les données à caractère personnel à un destinataire dans un pays tiers, les garanties appropriées.

36. L'équipe de recherche de l'UHasselt recevra des données pseudonymisées qui ne permettent pas de retrouver l'identité des personnes concernées[3]. Les chercheurs de l'UHasselt ne sont donc pas en mesure d'informer les personnes concernées à un niveau individuel. En mettant les connaissances scientifiques et le tableau de bord à la disposition du public, l'UHasselt s'engage à transférer les connaissances au grand public, ainsi qu'aux médecins, aux prestataires de soins de santé et aux acteurs politiques. Par ailleurs, la délibération (si elle est approuvée) sera aussi mentionnée sur le site internet de la Data Science Institute, sur la page déjà prévue pour la Chaire.

37. Le Comité est par conséquent d'avis que la demande répond aux exigences de transparence.

[3]Art. 14, § 5, b) du RGPD.

F. MESURES DE SÉCURITÉ

38. Conformément à l'article 5, f) du RGPD, le demandeur doit prendre toutes les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel. 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.

39. 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, …); documentation.

40. En exécution de l'article 35 du RGPD, l'UHasselt doit réaliser une analyse d'impact relative à la protection des données.

41. Le Comité renvoie à la délibération n° 24/044 du 5 mars 2024 relative aux bonnes pratiques à appliquer en cas d'utilisation de services cloud publics. Lors de l'utilisation de services cloud, le responsable du traitement doit s'assurer que la protection des données soit correctement mise en place et que les opérations de traitement sur cette plateforme soient réalisées en conformité avec le RGPD.

42. Lors de l'établissement de la liste de bonnes pratiques, on part du principe que le fournisseur de service Cloud public ne peut pas avoir accès aux informations traitées sur la plateforme. Ceci est réalisé grâce à l'informatique confidentielle (« *confidential computing* ») qui permet de garantir, au moyen du chiffrement, que le fournisseur de service n'a pas accès à des données et codes lisibles, dans la mémoire et dans le processeur. Cet environnement sécurisé est aussi appelé enclave.

43. Lors du recours à l'informatique confidentielle, les conditions suivantes doivent au moins être remplies:

a. Le fournisseur de service Cloud public ne peut pas avoir accès aux informations traitées.

   i. Les données au repos « data at rest » doivent être protégées, peuvent uniquement être déchiffrées dans l'enclave sécurisée et doivent à nouveau être chiffrées avant de quitter l'enclave.

ii. Les données en transit « data in transit » doivent être protégées, peuvent uniquement être déchiffrées dans une enclave sécurisée et doivent à nouveau être chiffrées avant de quitter l'enclave.
iii. Les informations ne peuvent pas être transférées, de manière lisible, sur les réseaux Cloud, y compris au sein de la plateforme mise en place par l'utilisateur. Ceci s'applique donc aussi à la communication entre deux serveurs au sein de la même plateforme.
iv. L'échange d'informations avec la plateforme de cloud doit avoir lieu de manière sécurisée.

b. L'attestation de l'informatique confidentielle de la plateforme de cloud public

i. Avant que le logiciel ne traite des informations sensibles sur la plateforme d'informatique confidentielle, il doit être certain que la plateforme offre les garanties utiles au niveau de la protection. Ceci a lieu au moyen d'une attestation de l'informatique confidentielle.
ii. L'attestation doit permettre de vérifier que l'environnement d'exécution est confidentiel et véridique, doit être réalisée de manière fiable et doit aussi être protégée. L'attestation doit pouvoir être exécutée indépendamment du fournisseur de service Cloud public.

c. Moyens de chiffrement et secrets

i. Les clés de chiffrement et les secrets sont protégés jusque dans l'enclave et ne quitteront jamais l'enclave sous forme lisible.
ii. Les clés de chiffrement et les secrets sont gérés sur un système auquel le fournisseur de service Cloud public n'a pas accès.

d. Moyens d'authentification

i. Les moyens d'authentification doivent être traités de la même manière que les secrets.
ii. Le fournisseur de service Cloud public n'a pas accès au système gérant les moyens d'authentification ou au système réalisant l'authentification.
iii. Le fournisseur de service Cloud public n'a pas d'accès logique aux serveurs ou aux enclaves, ni même avec des moyens d'authentification propres.

e. Moyens d'autorisation

i. Le fournisseur de service Cloud public n'a pas accès au système gérant les autorisations.

f. Suppression des données

i. Le fournisseur de service Cloud public offre les garanties utiles que les données seront effectivement supprimées dans les systèmes de stockage lorsque

l'utilisateur donne l'ordre à cet effet et fait régulièrement attester ces procédures par une partie externe.

g. Surveillance de la technologie utilisée

i. L'utilisateur doit conclure un contrat avec le fournisseur de service Cloud public selon lequel l'utilisateur est immédiatement informé de vulnérabilités éventuelles de la plateforme ou de ses composants de sorte que l'utilisateur puisse prendre des mesures adéquates pour limiter le risque.

h. Service level agreement

i. La relation avec le fournisseur de service Cloud public doit comprendre un service level agreement qui offre des garanties suffisantes que le fournisseur de service Cloud public réagira, de manière adéquate, aux menaces éventuelles susceptibles d'avoir un impact sur la protection des informations.

j. Réglementation applicable et litiges

i. Les contrats avec le fournisseur de service Cloud public doivent être conclus sous le droit belge ou le droit d'un autre pays européen. Les litiges relatifs au RGPD doivent être traités par l'Autorité de protection des données belge.

Principe de collecte et enregistrement uniques de données à caractère personnel

44. Les hôpitaux en Belgique constituent la source authentique. L'équipe de l'UHasselt n'a pas introduit de demandes de données et n'introduira pas de demandes de données auprès des hôpitaux; néanmoins, elle souhaite avoir recours aux données qui sont disponibles auprès du SPF Santé publique.

45. Conformément à l'article 9, point 3, du RGPD, 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. Le Comité rappelle que lors du traitement de données à caractère personnel, le professionnel des soins de santé ainsi que ses préposés ou mandataires sont soumis au secret, conformément à l'article 458 du Code pénal.

46. Tous les membres de la communauté universitaire sont soumis à un code de bonne conduite en matière d'ICT en vertu de la réglementation et d'un règlement relatif au traitement de données à caractère personnel. En fonction de leur statut, ils sont par ailleurs tenus à un devoir de confidentialité à l'égard des données à caractère personnel en vertu du règlement de travail ou du règlement d'enseignement et d'examen, sous peine de mesures disciplinaires.

47. Le Comité attire explicitement l'attention sur les dispositions du Titre 6 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à

caractère personnel, qui prévoit des sanctions administratives et pénales sévères dans le chef du responsable du traitement et des sous-traitants pour la violation des conditions prévues dans le RGPD et la loi du 30 juillet 2018 précitée.

Par ces motifs,

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 de la vie privée qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

La présente délibération entre en vigueur le 19 mars 2025.

Michel DENEYER
Président

Bijlage 1 ICD-codes

Selectie van de gegevens	Registratiesysteem	MZG
	Periode of datum waarop de gegevens betrekking hebben	2010 - 2022 (behalve 2015)
	Type ziekenhuis	Algemene ziekenhuizen
	Datum van extractie	30/08/2024
	Versie	1.0

Uitleg bij selectie en variabelen		Hoofddiagnose : prindiag
		Darmkanker : zie codelijsten
		Scheiding tussen primair darmkanker of in-situ darmkanker op basis van ICD codes
	MZG 2015	De gegevens in verband met diagnosen en procedures voor het registratiejaar 2015 zijn niet beschikbaar omwille van een overgangsperiode in het kader van de overgang van het classificatiesysteem ICD-9-CM naar ICD-10-BE.

ICD-9-CM codes en ICD-10-CM codes van darmkanker

ICD-9-CM codes primair darmkanker
152.0 Malignant neoplasm of duodenum
152.1 Malignant neoplasm of jejunum
152.2 Malignant neoplasm of ileum
152.3 Malignant neoplasm of Meckel's diverticulum
152.8 Malignant neoplasm of other specified sites of small intestine
152.9 Malignant neoplasm of small intestine, unspecified site
153.0 Malignant neoplasm of hepatic flexure
153.1 Malignant neoplasm of transverse colon
153.2 Malignant neoplasm of descending colon
153.3 Malignant neoplasm of sigmoid colon
153.4 Malignant neoplasm of cecum
153.5 Malignant neoplasm of appendix vermiformis
153.6 Malignant neoplasm of ascending colon
153.7 Malignant neoplasm of splenic flexure
153.8 Malignant neoplasm of other specified sites of large intestine
153.9 Malignant neoplasm of colon, unspecified site
154.0 Malignant neoplasm of rectosigmoid junction
154.1 Malignant neoplasm of rectum
154.2 Malignant neoplasm of anal canal

154.3 Malignant neoplasm of anus, unspecified site
154.8 Malignant neoplasm of other sites of rectum, rectosigmoid junction, and anus
159.0 Malignant neoplasm of intestinal tract, part unspecified
209.00 Malignant carcinoid tumor of the small intestine, unspecified portion
209.01 Malignant carcinoid tumor of the duodenum
209.02 Malignant carcinoid tumor of the jejunum
209.03 Malignant carcinoid tumor of the ileum
209.10 Malignant carcinoid tumor of the large intestine, unspecified portion
209.11 Malignant carcinoid tumor of the appendix
209.12 Malignant carcinoid tumor of the cecum
209.13 Malignant carcinoid tumor of the ascending colon
209.14 Malignant carcinoid tumor of the transverse colon
209.15 Malignant carcinoid tumor of the descending colon
209.16 Malignant carcinoid tumor of the sigmoid colon
209.17 Malignant carcinoid tumor of the rectum
ICD-9-CM codes in-situ darmkanker
230.3 Carcinoma in situ of colon
230.4 Carcinoma in situ of rectum
230.5 Carcinoma in situ of anal canal
230.6 Carcinoma in situ of anus, unspecified
230.7 Carcinoma in situ of other and unspecified parts of intestine

ICD-10-CM codes primair darmkanker
C17 Malignant neoplasm of small intestine
C18 Malignant neoplasm of colon
C19 Malignant neoplasm of rectosigmoid junction
C20 Malignant neoplasm of rectum
C21 Malignant neoplasm of anus and anal canal
C26.0 Malignant neoplasm of intestinal tract, part unspecified
C7A.01 Malignant carcinoid tumors of the small intestine
C7A.02 Malignant carcinoid tumors of the appendix, large intestine, and rectum
ICD-10-CM codes in-situ darmkanker
D01.0 Carcinoma in situ of colon
D01.1 Carcinoma in situ of rectosigmoid junction
D01.2 Carcinoma in situ of rectum
D01.3 Carcinoma in situ of anus and anal canal
D01.40 Carcinoma in situ of unspecified part of intestine
D01.49 Carcinoma in situ of other parts of intestine

Bijlage 2 : OVERZICHT GEVRAAGDE VARIABELEN – MZG FOD VVV

1. A2_YEAR_HOSP_IN - Jaar van opname in het ziekenhuis
2. A2_MONTH_HOSP_IN - Maand van opname in ziekenhuis

>> Deze variabelen geven inzicht in de timing van ziekenhuisopnames, wat belangrijk is om seizoensgebonden trends of veranderingen in opnamecijfers over de jaren te analyseren.

3. A2_YEAR_HOSP_OUT - Jaar van ontslag uit ziekenhuis
4. A2_MONTH_HOSP_OUT - Maand van ontslag uit ziekenhuis

>> Deze variabelen zijn belangrijk voor het analyseren van ontslagpatronen.

5. A2_HOSPTYPE_CAT - Categorie ziekenhuisverblijf
6. A2_HOSPTYPE_FAC - Type ziekenhuisverblijf (gebaseerd op facturatie)

>> Deze variabelen geven informatie over het soort verblijf, wat relevant kan zijn voor het onderscheiden van verschillende types van benodigde zorg (bijv. daghospitalisatie versus langdurige opnames).

7. LOSHOS* - Dit is de verblijfsduur uitgedrukt in aantal dagen (ontslagdatum-opnamedatum)

>> Dit is een directe maat voor de duur van het ziekenhuisverblijf en is essentieel voor het analyseren van de zorglast.

8. A2_CODE_READMISSION Code heropname
9. TCT_HEROPNAME*

>> Heropnames zijn een belangrijke kwaliteitsindicator in de gezondheidszorg, en deze variabelen kunnen helpen bij het evalueren van zorguitkomsten. Dit is ook een belangrijke variabele om het volledige zorgtraject van een darmkanker patiënt in beeld te brengen en het herkennen van eenzelfde patiënt binnen de dataset. Deze variabele stelt ***het aantal verblijven voor een hoofddiagnose van darmkanker voor dezelfde patiënt (d.w.z. de rangorder van het verblijf in de selectie) voor.***

10. A2_CODE_SEX - Geslacht

>> Geslacht is een fundamentele demografische variabele die kan worden gebruikt om verschillen in zorguitkomsten en opnames te onderzoeken. Stratificatie van analyses naar geslacht.

11. ARRONDISSEMENT* - Domicilie van de patient op arrondissementniveau (variabele gebaseerd op A2_CODE_ZIP)

>> Geeft informatie over de geografische spreiding van opnames, wat nuttig kan zijn voor het identificeren van regionale verschillen in zorg / aantal diagnoses.

12. A2_CODE_INDIC_NAT - Indicator nationaliteit

>> Deze variabele biedt inzicht in de diversiteit van de patiëntpopulatie en kan helpen bij het onderzoeken van zorgverschillen op basis van nationaliteit of herkomst.

13. A2_CODE_STAT_INSURANCE - Code verzekeringsstatus patiënt gedurende dit verblijf

>> Verzekeringsstatus kan een indicator zijn voor toegang tot zorg en daarmee een belangrijke variabele voor analyses gericht op zorgongelijkheid.

14. A2_CODE_PLACE_BEFOR E_ADM - Plaats vóór opname
15. A2_CODE_ADRBY - Verwezen door

>> Deze variabelen bieden context over de gezondheidstoestand van de patiënt vóór opname en het type opname (bijv. spoed vs. geplande opnames).

16. AGE*

>> Leeftijd is een fundamentele demografische variabele die kan worden gebruikt om verschillen in zorguitkomsten en opnames te onderzoeken. Stratificatie van analyses naar leeftijd.
>> Deze variabele geeft de leeftijdscategorie van de patiënt weer. Categorieën worden gedefinieerd in stappen van 5, startend vanaf een volwassen leeftijd en gelijkaardig aan de gegevens van het Belgisch Kankerregister, i.e. 15-19, 20-24, 25-29, …, 80-84, 85+.

17. A2_CODE_DISCHARGE - Type ontslag
18. A2_CODE_DESTINATE - Bestemming

>> Deze variabelen geven inzicht in de doorverwijzingspatronen en de opvolging van zorg na ontslag, wat belangrijk is voor het analyseren van continuïteit van zorg.

19. A2_CODE_DIAG_VERIF_ ADM Geverifieerde opnamediagnose

>> Inclusie variabele voor gevraagde database: Alle opnames met als hoofddiagnose darmkanker.

20. CODE_DIAGNOSE

>> ***Deze variabele geeft alle (neven)diagnoses voor het verblijf.***

21. M2_CODE_PROCEDURE

>> Informatie over de procedures die zijn uitgevoerd tijdens het ziekenhuisverblijf. De variabele is noodzakelijk om het ziektetraject van een darmkanker patiënt te kunnen beschrijven.

22. TYPE ZIEKENHUIS* – Een variabele die aangeeft of een ziekenhuis een universitair / niet-universitair karakter heeft en/of een bepaalde erkenning heeft voor een zorgprogramma. Deze variabele is gebaseerd op CODE_AGR - Erkenningsnummer ziekenhuis. Interessante zorgprogramma's: Zorgprogramma oncologie en Zorgprogramma oncologische basiszorg.

23. TCT_HNEW - gehercodeerde NIS-code (proxy voor Patiëntennummer)

>> Nodig om heropnames te kunnen linken aan dezelfde patiënt.
>> Het is noodzakelijk dat we in staat zijn om dezelfde patiënt met terugkerende hospitalisaties te herkennen, zodat heropnames aan dezelfde persoon kunnen worden gelinkt. Dit is de reden voor het opvragen van de patiëntennummers. Echter, deze patiëntnummers moeten niet gekoppeld worden aan het INSZ-nummer, zodat de identiteit van de patiënten niet achterhaald kan worden. Een andere indicator voor patiënt is dus toegestaan.

24. TCT_facturatie – totale facturatie voor het hele verblijf

>> Deze variabele is belangrijk om een idee te krijgen van de ziektekost gelinkt aan een hospitalisatie.

** Nieuwe variabelen gebaseerd op bestaande variabelen in de MZG database*