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

CSI/CSSS/25/324

DÉLIBÉRATION N° 14/094 DU 18 NOVEMBRE 2014, MODIFIÉE LE 28 JUILLET 2015 ET LE 4 NOVEMBRE 2025, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES RELATIVES À LA SANTÉ PAR DES POSTES DE GARDE, LES PHARMACIES AFFILIÉES À LA KONINKLIJKE APOTHEKERSVERENIGING VAN ANTWERPEN (KAVA) ET DES SERVICES D'URGENCE AU CENTRUM VOOR HUISARTSENGENEESKUNDE DE L'UNIVERSITÉ D'ANVERS DANS LE CADRE DU PROJET ICAREDATA

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

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*;

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

Vu les demandes d'autorisation définitives reçues le 13 octobre 2014, le 5 juin 2015 et le 30 mai 2025 ;

Vu les rapports d'auditorat de la Plate-forme eHealth;

Vu le rapport de monsieur Michel Deneyer.

Émet, après délibération, les décisions suivantes, le 18 novembre 2014, le 28 juillet 2015 et le 4 novembre 2025 :

I. OBJET DE LA DEMANDE

1. Le Centrum voor Huisartsengeneeskunde, unité de recherche "Soins de première ligne et interdisciplinaires" (Eerstelijns- en Interdisciplinaire Zorg) de la Faculté de Médecine et des Sciences de la santé (Faculteit Geneeskunde en Gezondheidswetenschappen) de l'université d'Anvers (CHA-ELIZA) soumet pour approbation au Comité la communication de données à caractère personnel pseudonymisées par des postes de garde, ainsi que, dans un deuxième temps, par des pharmacies affiliées à la Koninklijke Apothekersvereniging van Antwerpen (KAVA) et par les services d'urgence de l'hôpital universitaire d'Anvers, ainsi que des deux plus grandes chaînes d'hôpitaux anversois et, dans une troisième phase, par le fournisseur d'un système numérique d'auto-triage dans le cadre de la création d'une banque de données de recherche clinique, nommée *Improve Care and Research Electronic Data Trust Antwerp* (iCAREdata).

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

3. Dans un second temps, les données à caractère personnel provenant des pharmacies affiliées à la KAVA et de certains services d'urgence permettraient de se former une image plus précise des médicaments délivrés sur ordonnance et de l'aide médicale apportée par les services d'urgence en dehors des heures de travail normales.

4. Dans une troisième phase, les données à caractère personnel des systèmes de triage, y compris d'auto-triage ou d'auto-évaluation par le patient[1], permettent de déterminer les besoins de soins préalablement à un contact de soins (poste de garde de médecine générale, pharmacien de garde ou service des urgences). Il est ensuite possible de dresser la carte du flux de patients à travers le système de soins non planifiables suite au triage. Cela permet de définir les objectifs suivants : les conséquences et l'impact de la mise en œuvre des systèmes de triage sur les contacts de patients avec les services de soins non planifiables, l'efficacité et la précision (sécurité médicale) du triage, le respect des recommandations de triage et l'impact des systèmes de triage (sur la charge de travail dans le système de soins non planifiables, sur l'usage abusif du système de soins non planifiables, sur la répartition des pathologies entre les différents services et sur la demande de soins).

[1] www.moetiknaardedokter.be

5. Les données à caractère personnel pseudonymisées sont analysées par les chercheurs du CHA-ELIZA. L'étude pourra être exécutée à l'initiative du CHA-ELIZA ou à la demande de chercheurs externes.

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

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

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

<u>Données relatives au contact :</u>
- identification du contact,[2] pseudonymisée par le TTP
- identification du poste de garde
- date et heure du contact et début du traitement, mode de prise de contact, type de contact, conseil d'urgence
- numéro INAMI du médecin qui a assuré le contact, pseudonymisé par le TTP
- renvoi éventuel, incapacité de travail ou non

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

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

    - date, nom du médicament, code CNK.

8. Les données à caractère personnel relatives à la santé qui seront transmises par les pharmacies sont les suivantes :
- identification de la pharmacie ;
- numéro INAMI du médecin prescripteur, pseudonymisé par le TTP ;
- NISS du patient, pseudonymisé par le TTP ;
- date et heure de la délivrance du médicament ;
- code CNK du médicament.

9. Les données transmises par les services des urgences seront les suivantes :

Données relatives au patient :
- NISS du patient, pseudonymisé par le TTP (si le patient n'a pas de NISS, le tiers de confiance lui octroiera un numéro) ;
- année de naissance du patient ;
- sexe du patient ;
- code postal du domicile du patient ;
- code assurabilité du patient.

Données de contact :
- identification du contact, pseudonymisée par le TTP ;
- identification du service des urgences ;
- numéro INAMI du médecin, pseudonymisé par le TTP ;
- la date et l'heure du contact avec le service des urgences et du début de la prise en charge, le mode de prise de contact, le type de contact et le degré d'urgence ;
- la prise en charge éventuelle.

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

10. Les systèmes de triage communiqueront les données suivantes:

Données relatives au patient :
- date de naissance du patient, pseudonymisée par le TTP ;
- année de naissance du patient ;
- sexe du patient.

Données de contact :
- code linguistique du triage ;

- région du poste de garde.

Données relatives à la morbidité:
- partie du corps concernée (chapitre de triage);
- symptômes déclarés;
- degré d'urgence attribué suite au triage;
- recommandation de renvoi;
- avis fourni.

11. Un fichier CSV (comma separated value) est créé sur le serveur ou l'ordinateur des postes de garde, de la Koninklijke Apothekersvereniging van Antwerpen (KAVA) qui gère la base de données des pharmacies, sur le serveur des services des urgences et sur le serveur du fournisseur du système de triage. La KAVA ne transmet que les données qui concernent les patients vu par un poste de garde ou un service d'urgence, sur base des numéros d'identification des patients reçus pendant le service de garde et qui seront envoyés par les postes de garde et les services d'urgence participants.

12. Les quatre premières colonnes du fichier CSV du poste de garde et du service des urgences contiennent respectivement le numéro NISS du patient, le numéro INAMI du médecin, la date de naissance du patient et le code d'identification du contact. Ces trois colonnes sont séparées par un point-virgule des colonnes suivantes qui contiennent les informations médicales. Ces colonnes avec les informations médicales sont chiffrées avant l'envoi. Le fichier CSV est transmis de manière sécurisée via le eHealthBox à la Plate-forme eHealth pour codage. Les fichiers pseudonymisés sont ensuite envoyés de manière sécurisée vers le eHealthBox de iCAREdata.

13. La première colonne du fichier CSV du système de triage contient la date de naissance de l'utilisateur. Cette colonne est séparée par un point-virgule des colonnes suivantes qui contiennent des informations médicales. Ces colonnes avec les informations médicales sont chiffrées préalablement à l'envoi. Le fichier CSV est transmis de manière sécurisée à eHealth via l'UZA en vue du codage au moyen d'eHealthBox. Ensuite, les fichiers pseudonymisés sont transmis de manière sécurisée vers l'eHealthBox de iCAREdata.

14. Dans cet eHealthBox, les quatre premières colonnes du fichier CSV des prestataires de soins et la première colonne du fichier CSV du système de triage sont pseudonymisés par la Plate-forme eHealth au moyen d'un algorithme que seule la Plate-forme eHealth connaît. Il s'agit d'un algorithme réversible. Les champs chiffrés avec les informations médicales ne peuvent pas être lus par la Plate-forme eHealth étant donné que cette dernière ne dispose pas de la clé de déchiffrement. Le fichier avec les champs d'identification pseudonymisés et les champs d'informations médicales chiffrées est extrait de l'eHealthBox à des intervalles réguliers par le serveur de l'UA.

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

16. Afin d'éviter la réidentification à partir d'une combinaison de données à caractère personnel pseudonymisées, une analyse de risque "small cell" est exécutée en collaboration avec la Cellule technique. Au besoin, certaines données à caractère personnel pseudonymisées seront agrégées afin d'éviter que les intéressés puissent être identifiés.

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

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

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

20. Le numéro INAMI des médecins concernés est pseudonymisé de manière réversible. Ainsi, il sera possible, moyennant l'intervention de la Plate-forme eHealth, de

procéder à une dépseudonymisation, mais uniquement pour le numéro INAMI codé des médecins en question, de sorte à pouvoir fournir le feed-back nécessaire au médecin concerné. Ceci permettra par exemple de communiquer à un médecin individuel combien d'antibiotiques et quels antibiotiques il a prescrit pour une infection déterminée. A aucun moment les chercheurs n'ont connaissance de l'identité des médecins concernés.

21. La banque de données du projet iCAREdata est conservée sur un serveur situé dans un local de serveurs du Campus Drie Eiken de l'université d'Anvers. Ce local n'est accessible qu'à un nombre limité de collaborateurs ICT. L'accès à la banque de données en tant que telle est limité au gestionnaire de données (médecin) et à un collaborateur ICT (bio-informaticien) du projet iCAREdata. Ils ont uniquement accès à travers une connexion sécurisée. Des loggings de sécurité relatifs à l'accès à la banque de données sont prévus.

II. COMPÉTENCE

22. 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 de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

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

24. En application de l'article 5, § 1, de la loi garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier, le Comité est compétent pour autoriser l'utilisation du numéro du Registre national lorsqu'il prend une décision à propos d'un flux de données à caractère personnel. L'envoi des numéros d'identification des patients reçus par les postes de garde et les services d'urgence vers la KAVA tel que décrit au point 9, peut donc être autorisé.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

25. Le traitement de données à caractère personnel relatives à la santé est en principe interdit, conformément au prescrit de l'article 9, §1er du Règlement (UE) 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

(RGPD)Cependant, cette interdiction ne s'applique pas lorsque, comme en l'espèce, 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[3].

26. Selon l'article 5 du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

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

B. MINIMISATION DES DONNÉES

28. Selon l'article 5 du RGPD, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées..

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

30. 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 pseudonymisées peuvent être traitées. Etant donné qu'il est indispensable qu'un patient soit identifié de manière unique et qu'il est primordial de suivre un patient

[3] Art. 9, §2, j) du RGPD.

dans le temps, il est acceptable que des données à caractère personnel pseudonymisées soient utilisées.

31. En ce qui concerne le traitement des données à caractère personnel pseudonymisées à la demande de chercheurs externes, le Comité constate que les analyses scientifiques qui sont nécessaires pour répondre aux questions de l'étude seront effectuées par les chercheurs du CHA-ELIZA associés au projet iCAREdata. Toute communication de données à caractère personnel pseudonymisées relatives à la santé en provenance de la banque de données du projet iCAREdata doit être soumise au préalable au Comité pour approbation.

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

C. LIMITATION DE LA DURÉE DE CONSERVATION

33. Selon 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). Le demandeur prévoit un délai de conservation de 30 ans à compter de l'enregistrement dans la banque de données. Ce délai de conservation doit permettre d'étudier les évolutions dans le temps. Le demandeur déclare que les soins OOH constituent un phénomène relativement récent et que le fonctionnement peut prendre une direction imprévue. De même, les tendances en termes de comportement de prescription ne peuvent être étudiées qu'après plusieurs années. Le Comité accepte dès lors le délai de conservation proposé.

D. TRANSPARANCE

34. Conformément à l'article 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 doivent être fournies par écrit ou par d'autres moyens, y compris, lorsque c'est approprié, par voie électronique.

35. Lorsque les données à caractère personnel ne pas collectées auprès de la personne concernées, le responsable du traitement lui communique toutes les informations mentionnées à l'article 14, §1 et §2 du RGPD.

36. 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 ou dans la pharmacie (clairement lisible, à un endroit visible) et la possibilité de la communication d'informations plus détaillées par le médecin généraliste pendant la consultation ou par le pharmacien. La notification au moyen de l'affiche renvoie également à la présente délibération.

37. Le Comité estime que la notification prévue est suffisante.

E. SÉCURITÉ DE L'INFORMATION

38. Le traitement de données à caractère personnel relatives à la santé doit être effectué sous la surveillance et la responsabilité d'un professionnel des soins de santé.Le Comité a effectivement reçu l'identité du médecin concerné. 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.

39. Selon l'article 5, §1er, f) du RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité). 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.

40. 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 délégué à la protection des données; 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 prend acte du fait que le demandeur confirme qu'un délégué à la protection des données a été désigné. Les locaux où les données à caractère personnel pseudonymisées sont enregistrées, sont sécurisés et ne sont accessibles qu'aux seules personnes autorisées. L'accès 'on-campus' au serveur via le réseau est strictement

réglementé et intervient sur la base de l'adresse IP et de données de compte. Les protocoles utilisés sont, si possible, protégés au moyen de SSL. L'accès à distance au serveur n'est possible qu'au moyen d'un accès VPN SSL et sur la base de droits d'accès spécifiques. L'accès fait également l'objet de loggings. Le serveur est équipé d'éléments redondants: alimentation double, technologie RAID, monitoring automatique du hardware et prise de backups.

41. Le Comité rappelle qu'en vertu de l'article 9 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, le responsable du traitement prend les mesures suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé :
1° les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;
2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;
3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

42. Le Comité estime nécessaire de rappeler que depuis le 25 mai 2018, l'UZ Leuven est tenu de respecter les dispositions et les principes du Règlement (UE) 2016/679 du Parlement 8 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 sur la protection des données). Ces instances sont également tenues de respecter les dispositions de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

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.

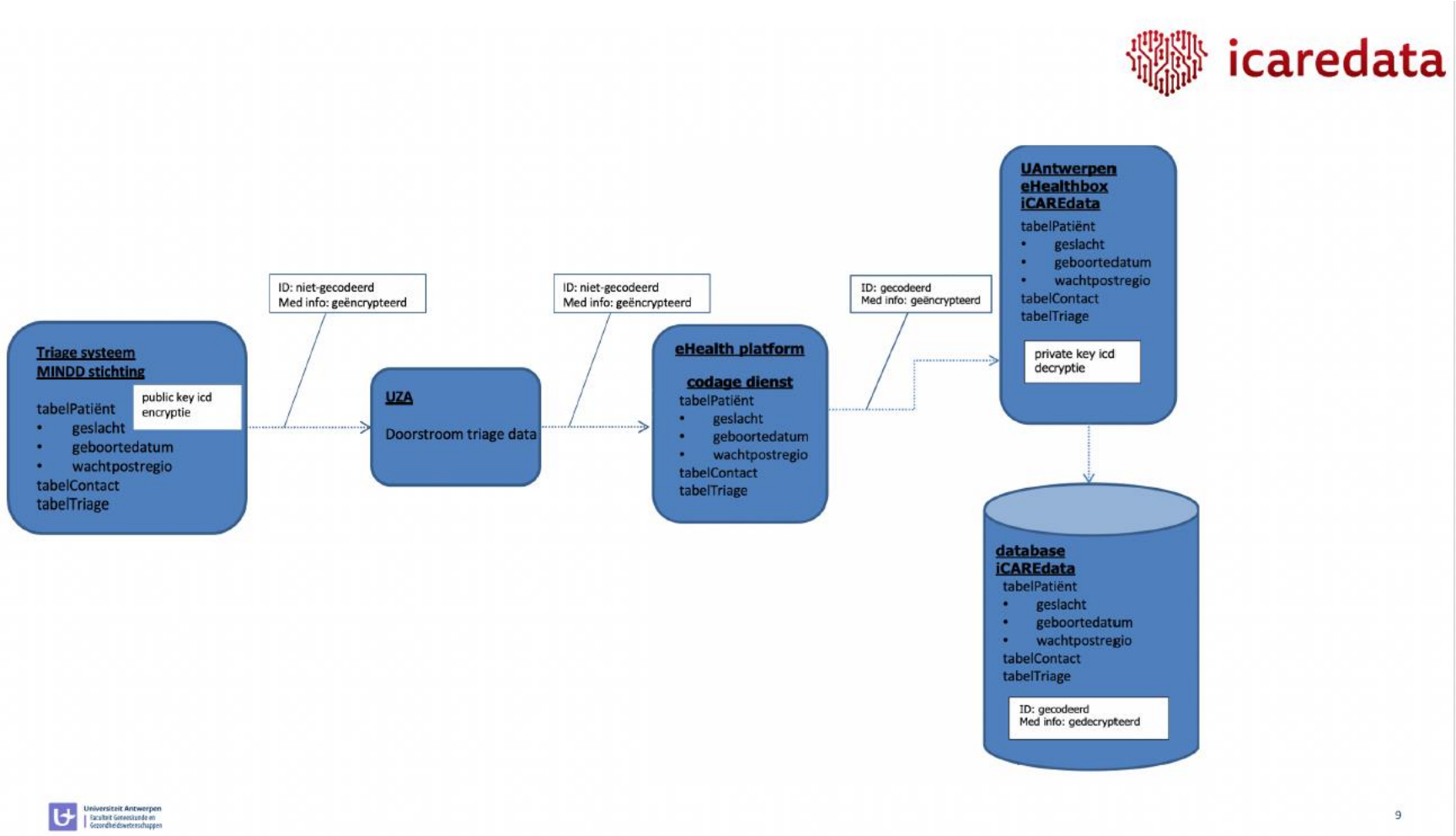
La Plate-forme eHealth est autorisée à conserver le lien entre le numéro pseudonymisé et le numéro d'identification réel, vu le caractère longitudinal du projet. Par ailleurs, la Plate-forme eHealth est autorisée à procéder à la dépseudonymisation, cependant, uniquement du numéro INAMI pseudonymisé des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

Les modifications de cette délibération, approuvées par le comité de sécurité de l'information le 4 novembre 2025, entrent en vigueur le 20 novembre 2025.

Michel DENEYER
Président

Bijlage: schematische voorstelling stroom

Schematische voorstelling extra datastroom betreffende de triagesystemen



Schematische voorstelling van alle datastromen