Comité de sécurité de l'information

Chambre sécurité sociale et santé

CSI/CSSS/24/392

DÉLIBÉRATION N° 21/060 DU 2 MARS 2021, MODIFIÉE EN DERNIER LIEU LE 5 NOVEMBRE 2024, PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES RELATIVES À LA SANTÉ ISSUES D'ÉTABLISSEMENTS DE SOINS ACTIFS DANS LES SOINS DE SANTÉ MENTALE AUX GROUPES DE RECHERCHE « CENTRUM VOOR HUISARTSENGENEESKUNDE » ET « COLLABORATIVE ANTWERP PSYCHIATRIC RESEARCH INITIATIVE » DE L'UNIVERSITÉ D'ANVERS DANS LE CADRE D'UN PROJET VISANT À AMÉLIORER LA SANTÉ PUBLIQUE MENTALE

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 des groupes de recherche « Centrum voor Huisartsengeneeskunde » et « Collaborative Antwerp Psychiatric Research Initiative » de l'Université d'Anvers;

Vu le rapport d'auditorat de la Plate-forme eHealth du 17 octobre 2024;

Vu le rapport de monsieur Michel Deneyer;

Émet, après un projet de délibération, la décision suivante, le 5 novembre 2024:

I. OBJET DE LA DEMANDE

1. Le « Centrum voor Huisartsengeneeskunde » et le « Collaborative Antwerp Psychiatric Research Initiative », des groupes de recherche de la Faculté Médecine et Sciences de la santé de l'Université d'Anvers, introduisent une demande visant à obtenir une délibération du Comité de sécurité de l'information pour la communication de données à caractère personnel pseudonymisées relatives à la santé provenant d'établissements de soins actifs dans les soins de santé mentale, dans le cadre d'un projet d'amélioration de la santé publique mentale.

2. Toute organisation de soins enregistre dans le cadre de travaux cliniques de nombreuses variables par trajet de traitement. Les données sont toutefois uniquement conservées au niveau interne. L'enregistrement obligatoire actuel est par conséquent dispersé et ne permet pas de se faire une idée précise de qui reçoit quels soins et des trajets de soins parcourus par les patients.

3. Ce projet permet néanmoins d'étudier les données disponibles d'une manière plus approfondie et pendant une plus longue période. Le projet a pour objet d'améliorer la santé publique mentale par un meilleur équilibre entre l'offre et la demande. Les chercheurs souhaitent se faire une meilleure idée des soins de santé mentale (résidentiels) offerts actuellement, de la population qui y a recours et de la manière dont elle y a recours. Cette compréhension peut donner lieu à des recommandations pour une organisation des soins plus efficace avec une plus grande portée.

4. Étant donné que les données relatives aux soins de santé mentale sont disponibles de manière limitée, les chercheurs souhaitent utiliser au maximum pour ce projet, les données qui sont disponibles dans la pratique clinique, afin de se faire une meilleure idée des soins fournis et des besoins dans les soins de santé mentale.

5. Le groupe faisant l'objet de l'étude sont l'ensemble des patients en traitement dans les établissements de soins concernés au 01/08/2021. Ensuite, un transfert trimestriel des données est prévu. Dans ces transferts, les chercheurs reçoivent les données de toutes les personnes qui sont sorties de l'établissement de soins depuis le dernier transfert de données.

6. Les données à caractère personnel pseudonymisées relatives à la santé suivantes[1] sont communiquées par patient concerné:

- Données de l'établissement;
  - Numéro d'agrément;
- Données relatives au service;
  - Numéro;

[1] En ce qui concerne les variables catégorielles, voir aussi https://www.health.belgium.be/sites/default/files/uploads/fields/fpshealth_theme_file/manuel_rpm_troisieme_edition.pdf. Les chercheurs les ont reprises de l'enregistrement du RPM.

    - Population cible;
- Données relatives au patient;
    - NISS pseudonymisé;
    - Sexe;
    - Année de naissance;
    - Nationalité (en classes);
    - Code INS domicile;
    - État civil;
    - Enfants à charge ;
    - Situation professionnelle (statut professionnel lors de l'admission)[2];
    - Niveau de formation (niveau de la dernière formation achevée)[3];
    - Type de domicile (cadre de vie avant l'admission)[4];
    - Assurabilité code patient;
    - Assurance hospitalisation;
- Données relatives à l'admission (partielle);
    - Identification de l'admission (numéro d'admission)
    - Numéro INAMI (pseudonymisé) du médecin référent;
    - Numéro d'agrément organisation de renvoi;
    - Numéro du service si renvoi interne;
    - Date d'admission;
    - Numéro INAMI (pseudonymisé) du médecin traitant;
    - Index type de lit;
    - Quantième admission (dans ce service);
    - Date sortie;
    - Encadrement après sortie[5];
    - Numéro d'agrément établissement auquel le patient est renvoyé après sa sortie;
    - Numéro service où le patient est renvoyé après sa sortie;
- Données relatives au traitement (par admission partielle);
    - Plainte lors de l'appel (texte libre);

[2] Travail à temps plein, travail à temps partiel, travail intermittent, maladie ou accident, congé pour raisons familiales ou personnelles, au foyer (ménage), écolier/étudiant, invalide, handicapé, chômeur indemnisé, chômeur non indemnisé, bénéficiaire d'une allocation, pensionné, rentier, autre non spécifié, sans, inconnu.

[3] Maternelle, primaire, secondaire inférieur, secondaire supérieur, 1er degré / observation, 2e degré / orientation, 3e degré / détermination, secondaire complémentaire, secondaire indéterminé, supérieur non-universitaire, universitaire, autre non spécifié.

[4] Isolé, famille fondée, famille parentale, résident ou cohabitant, autre milieu familial ou de remplacement, résidence pour personnes âgées, institution de soins aux handicapés, centre d'accueil pour les sans-abris, vie communautaire, institution relevant de la justice, autre habitation collective, hôpital psychiatrique, service psychiatrique en hôpital général, maison de soins psychiatriques, habitation protégée, placement en milieu familial, accueil psychiatrique alternatif, hôpital général, autre milieu thérapeutique, autre milieu non spécifié, sans domicile fixe, inconnu.

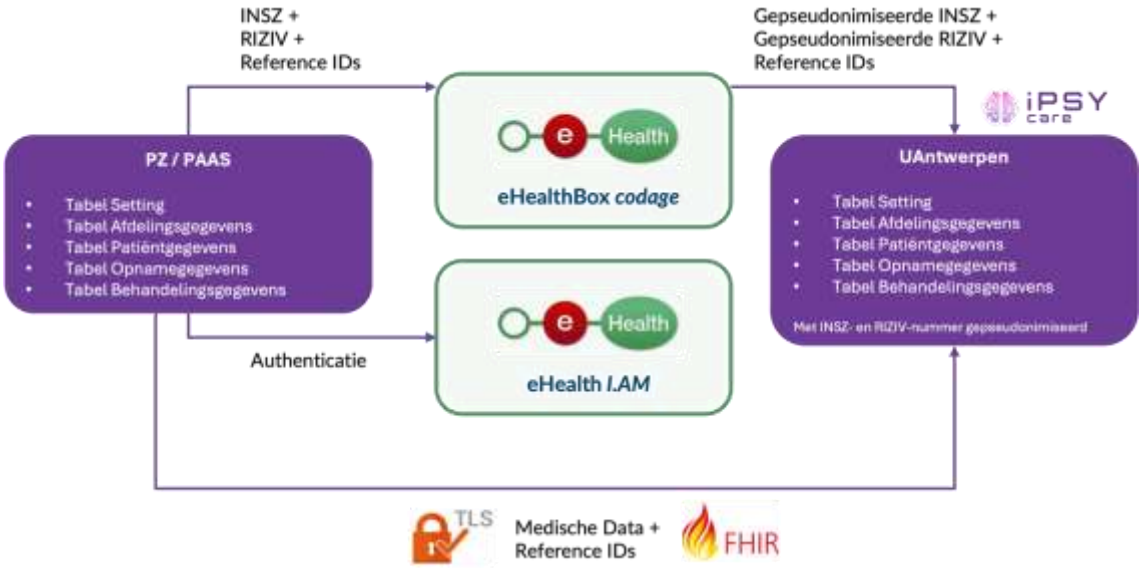
[5] Il s'agit de la destination (MD11) et éventuellement de la postcure et du traitement ultérieur proposés (MD10.01-MD10.09). Voir https://www.health.belgium.be/sites/default/files/uploads/fields/fpshealth_theme_file/manuel_rpm_troisieme_edition.pdf.

- Mode d'admission[6];
- Diagnostics DSM-IV sur Axe 1 à 5 (avec dates d'octroi);
- Données DSM5 si disponibles;
- ICD9/10 si disponible;
- Nombre de contacts avec différents prestataires de soins (individuels/en groupe);
- Paramètres somatiques (lors de l'admission);
  - Poids;
  - Taille;
  - Tension artérielle;
  - Tour de taille;
  - Cholestérol HDL;
  - Tabagisme;
  - Toxicomanie;
- Dépistage du suicide;
- Autres échelles (Honos, …) si disponibles:
- Début mesures restrictives de liberté;
- Fin mesures restrictives de liberté;
- Prescriptions médicamenteuses;
  - Date;
  - Nom médicament;
  - Code CNK;
- Raison de la sortie;
- Type de sortie[7].

7. Pour réaliser la communication des données à caractère personnel aux chercheurs, la procédure suivante est appliquée:

[6] Volontaire, mise en observation, internement, maintien, probation, autre condition juridique, assistance à personne en danger, autre non-spécifié, inconnu.

[7] De commun accord, transfert et mise en observation dans une autre institution, maintien autre institution, postcure, soins en milieu familial, autres mesures légales, exigée par l'intéressé ou par une autre personne sans l'accord de l'équipe, exigée par l'équipe sans accord de la personne concernée, fugue, pas de retour, évasion, décès naturel prévisible (avec/sans autopsie), décès naturel imprévisible (avec/sans autopsie), accident (avec/sans autopsie), suicide (avec/sans autopsie), homicide (avec/sans autopsie), inconnu ou circonstances indéterminées (du décès).



- Les hôpitaux envoient, tous les trimestres, des données relatives aux patients qui ont quitté l'hôpital au cours des trois derniers mois. Il existe deux flux de données parallèles. Le premier flux de données concerne l'échange de données relatives au patient et au service, en ce compris des données telles le numéro NISS, le numéro INAMI et le numéro d'admission. Ces données sont d'abord pseudonymisées à l'aide du service « eHealthBox codage ». Des numéros d'identification personnelle sont ainsi remplacés par des pseudonymes. Le deuxième flux de données concerne des données médicales qui sont envoyées directement, selon le protocole FHIR et sous forme chiffrée (TLS), à la plateforme iPSYcare. Ces données médicales ne contiennent pas de données d'identification personnelle. Les codes de référence jouent un rôle crucial dans le couplage des données médicales aux données pseudonymisées du patient. Ces codes de référence sont envoyés dans un premier flux et permettent, lors de l'arrivée des données sur la plateforme iPSYcare, de coupler les pseudonymes aux données médicales exactes, sans qu'il ne soit porté atteinte à l'anonymat.
- Les hôpitaux se connectent toujours par le biais de la Plate-forme eHealth qui a recours à un contrôle d'identité sécurisé (l'I.AM Identity Provider de eHealth).
- EHealth intervient comme tierce partie de confiance (TTP), pseudonymise à l'arrivée les numéros INAMI des médecins concernés et le NISS et anonymise le numéro d'identification de l'admission. eHealth envoie les tableaux de codage à nouveau en format csv et d'une manière sécurisée, à la base de données sur un serveur de l'UAntwerpen.
- Les algorithmes utilisés pour pseudonymiser le numéro INAMI et le NISS sont réversibles de sorte que le mécanisme de feedback du service de codage eHealth puisse être utilisé. Ce mécanisme de feedback est utilisé pour contacter les fournisseurs de données, par exemple en cas d'anomalies dans les données fournies, et permet de garantir le respect des principes de la TTP. L'algorithme de pseudonymisation du numéro d'identification de l'admission est irréversible. Seul eHealth connaît les algorithmes. Par ailleurs, des codes de référence non chiffrés sont aussi envoyés au travers d'un standard sécurisé (FHIR). Sur le serveur iPSYcare, ces codes de référence sont remplacés par des nouveaux codes créés par eHealth. Les données médicales

mêmes ne sont pas transmises via eHealth et restent donc cachées. Par conséquent, eHealth n'a pas accès aux données médicales. Les chercheurs disposent quant à eux de cette clé et sont en mesure de décrypter les données médicales lors de leur réception. Toutefois, étant donné qu'ils ne disposent pas des algorithmes de pseudonymisation du NISS, du numéro d'admission et des numéros INAMI, l'identification n'est pas possible pour eux.
- La possibilité est offerte aux patients et aux médecins concernés de s'opposer au traitement de leurs données. Étant donné que les données doivent être pseudonymisées pour les chercheurs, il n'est pas possible d'introduire directement un recours auprès des chercheurs. Les hôpitaux participants enverront les NISS/numéros INAMI (qui seront pseudonymisés) de ceux qui s'opposent aux chercheurs via le service de codage eHealth, de sorte que ces derniers puissent supprimer les données de l'étude..

8. Le serveur de l'UAntwerpen se trouve dans un local qui est uniquement accessible à un nombre limité de collaborateurs ICT. L'accès à la banque de données se limite au gestionnaire de la banque de données et au sous-traitant des données. Une liste nominative est établie et approuvée par le comité directeur et les collaborateurs ayant accès signent une obligation de confidentialité. L'accès est uniquement possible via une connexion sécurisée. Des loggings de sécurité relatifs à l'accès à la banque de données sont prévus. Les données et les clés de pseudonymisation sont conservés pendant 10 ans.

9. Le Comité fait observer qu'une analyse « small cell risks » sera réalisée par la firme P95, afin d'éviter la réidentification à partir d'une combinaison de données à caractère personnel pseudonymisées. Au besoin, certaines données à caractère personnel pseudonymisées seront agrégées afin d'éviter que les intéressés ne puissent être identifiés. Le Comité doit être informé du résultat de l'analyse avant que les données en question ne puissent être traitées.

II. COMPÉTENCE

10. 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.

11. Le Comité de sécurité de l'information estime par conséquent qu'il est compétent.

III. EXAMEN

A. ADMISSIBILITÉ

12. 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.[8]

[8] Art. 9, alinéa 1er du RGPD

13. 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.

14. Le Comité prend note du fait que le Comité d'éthique de l'UZA a remis un avis positif concernant cette étude.

15. Vu ce qui précède, le Comité conclut que le traitement de données à caractère personnel est admissible.

B. FINALITÉ

16. 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.

17. Le projet a pour objectif d'améliorer la santé publique mentale par un meilleur équilibre entre l'offre et la demande. Les chercheurs souhaitent se faire une meilleure idée des soins de santé mentale (résidentiels) offerts actuellement, de la population qui y a recours et de la manière dont elle y a recours. Cette compréhension peut donner lieu à des recommandations pour une organisation des soins plus efficace avec une plus grande portée.

18. Au vu des objectifs du traitement tels que décrits ci-dessus, le Comité considère que le traitement des données à caractère personnel envisagé poursuit bien des finalités déterminées, explicites et légitimes.

C. PROPORTIONNALITÉ

19. 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.

20. L'utilisation de données à caractère personnel se justifie comme suit:

- Le numéro d'agrément de l'établissement et le numéro du service permettent de suivre les admissions et les sorties par établissement, respectivement par service, en vue d'un contrôle des données[9], afin de comparer des populations de patients similaires dans des établissements différents, afin d'optimaliser les soins et, en combinaison avec le

[9] Le transfert des données est ensuite comparé avec le nombre de places disponibles dans l'établissement concerné, respectivement dans le service concerné.

numéro NISS pseudonymisé du patient (ou équivalent), l'identification de l'admission (numéro d'admission) et les informations de renvoi (voir données d'une admission partielle), de répertorier d'une manière fiable le trajet de soins de groupes de patients;

- Une description de la population cible d'un service est pertinent dans le cadre de la comparaison de populations de patients similaires dans différents établissements. Ensuite, un aperçu de la population cible est important pour vérifier si les patients reçoivent les soins les plus appropriés en fonction de leur profil clinique;
- Le NISS pseudonymisé (ou équivalent s'il fait défaut) est la clé permettant de coupler des admissions dans différents établissements ou à différents moments d'une seule et même personne et donc de déterminer le trajet de soins;
- La nationalité constitue une variable pertinente, d'une part pour décrire qui reçoit quel type de soins, d'autre part pour détecter la divergence au niveau des soins entre les différents groupes cibles. Cette variable est divisée en groupes, à savoir la Belgique, l'Europe autre, l'Afrique, l'Asie, autre et manquant.
- Les autres données à caractère personnel sont, en combinaison avec les données relatives à l'admission (partielle) et au traitement, pertinentes pour bien pouvoir décrire qui reçoit quel type de soins. Par ailleurs, les données à caractère personnel sélectionnées sont pertinentes pour décrire les groupes pour lesquels les soins sont organisés de manière sous-optimale (p.ex.: qui sont les patients multirécidivistes?) ;
- L'identification de l'admission (numéro d'admission – pseudonymisé de manière irréversible), le numéro INAMI pseudonymisé du médecin référent, le numéro d'agrément de l'organisation de renvoi, le numéro du service si renvoi interne, la date d'admission, le numéro INAMI pseudonymisé du médecin traitant, la date de sortie, l'encadrement après la sortie, le numéro d'agrément de l'établissement où le patient est renvoyé après sa sortie et le numéro du service où le patient est renvoyé après sa sortie permettent, en combinaison avec des informations relatives à l'établissement et au service et avec le NISS pseudonymisé du patient (ou équivalent), de répertorier de manière fiable le trajet de soins de patients;
- La date d'admission, la date de sortie, l'index type de lit et la quantième admission (dans ce service) sont, en combinaison avec les données relatives au patient et les données relatives au traitement, pertinentes pour une bonne description de qui reçoit quels soins;
- Les paramètres somatiques (lors de l'admission) sont pertinents pour évaluer l'état somatique des patients et pour, de manière plus spécifique, déterminer en combinaison avec les médicaments prescrits le risque de syndrome métabolique;
- Les autres données de traitement sont, en combinaison avec les données à caractère personnel et les données relatives à l'admission (partielle), pertinentes pour bien pouvoir décrire qui reçoit quel type de soins.

21. Étant donné que les chercheurs souhaitent savoir quels trajets les personnes parcourent dans les soins, à savoir vérifier si une personne qui a été admise au service x et qui séjourne maintenant dans le service y est passée directement de x à y, ou si la date de

sortie de x est égale à la date d'admission au service y (ou éventuellement de y + 1), il faut disposer de dates exactes. S'ils ne disposent pas de dates exactes, le risque existe qu'il y ait un délai d'attente à domicile (ou ailleurs, dans un établissement qui ne fournit pas de données). Cela les empêche de faire de solides déclarations sur le parcours de soins. Les chercheurs n'examineront jamais des parcours de soins individuels. Ils étudient uniquement les parcours de soins de groupes présentant certaines caractéristiques.[10]

22. Le principe de proportionnalité implique que le traitement doit en principe être réalisé au moyen de données anonymes. Cependant, si la finalité ne peut être réalisée au moyen de données anonymes, des données à caractère personnel pseudonymisées peuvent être traitées. Vu la nécessité de réaliser une analyse détaillée sur la base de ces données, les chercheurs ont besoin d'avoir accès à des données pseudonymisées afin d'être en mesure de réaliser ces analyses qu'il ne serait pas possible de réaliser à l'aide de données anonymes. Cette finalité justifie donc le traitement de données à caractère personnel pseudonymisées.

23. Les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant la durée nécessaire à la réalisation des finalités pour lesquelles les données à caractère personnel sont traitées.

24. Les données sont conservées pendant 20 ans à compter de la dernière collecte des données. Le contrat conclu par les parties est valable jusque fin décembre 2025. La dernière collecte des données aura donc au plus tard lieu en décembre 2025. Le délai de conservation est par conséquent fixé à fin 2045 au plus tard. La disponibilité des données permet aux chercheurs d'analyser les données plus en détail par rapport à ce qui est actuellement possible et donc de formuler des recommandations pour une organisation plus efficace des soins. Les données collectées seront utilisées pour la réalisation d'analyses et pour répondre à des questions de recherche, notamment concernant les parcours de soins accomplis, les groupes cibles critiques ou concernant des éléments de traitement spécifiques. Le Comité est d'accord avec ce délai de conservation.

25. 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.

D. TRANSPARENCE

26. Le responsable du traitement de données à caractère personnel, collectées à des fins déterminées, explicites et légitimes ou, le cas échéant, l'organisation intermédiaire doit en principe, préalablement à la pseudonymisation des données à caractère personnel, communiquer certaines informations relatives au traitement à la personne concernée.

27. Dans la mesure du possible, tout patient et tout prestataire de soins concernés seront activement informés sur base individuelle concernant l'étude, leurs droits d'opposition et de consultation. Les nouveaux patients le seront lors de l'admission. L'étude est

[10] Par exemple, diagnostic.

également annoncée sur les sites web des établissements de soins participants et les patients seront informés sur leurs droits au moyen d'affiches et d'annonces dans les salles d'attente des établissements de soins.

28. Le Comité estime donc que les principes de transparence sont suffisamment respectés.

E. MESURES DE SÉCURITÉ

29. Le demandeur doit, conformément à l'art. 5, f) du RGPD, prendre toutes les mesures techniques et organisationnelles nécessaires à la protection des 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.

30. Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est 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.

31. Le Comité constate qu'une analyse d'impact relative à la protection des données a été réalisée conformément à l'article 35 du Règlement général relatif à la protection des données.

32. Conformément à l'article 9, alinéa 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, ce qui est le cas en l'espèce.

33. 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.

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

35. Enfin, le Comité fait observer qu'une analyse « small cell risks » (SCRA) est prévue et qu'elle sera réalisée par la firme P95. Le Comité doit être informé du résultat de l'analyse avant que les données en question ne puissent être traitées.

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, à la condition qu'une analyse de risque "small cell" soit réalisée par la firme P95, afin d'exclure toute possibilité de réidentification des intéressés, et que le Comité soit informé du résultat de l'analyse avant que les données en question ne soient traitées.

que la Plate-forme eHealth est autorisée à conserver le lien entre le set de données pseudonymisées et le numéro d'identification réel, étant donné que les chercheurs souhaitent se faire une idée de la manière dont les personnes évoluent dans les soins et de la manière dont elles y ont recours, ce qui justifie pourquoi il est important de conserver le lien.

Les modifications de cette délibération, approuvées par le comité de sécurité de l'information le 5 novembre 2024, entrent en vigueur le 21 novembre 2024.

Michel DENEYER
Président