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

CSI/CSSS/19/388

DÉLIBÉRATION N° 14/011 DU 21 JANVIER 2014, MODIFIÉE LE 3 DÉCEMBRE 2019, PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES RELATIVES À LA SANTÉ À L'AGENCE FÉDÉRALE DES MÉDICAMENTS ET DES PRODUITS DE SANTÉ (AFMPS) DANS LE CADRE DU REGISTRE CENTRAL DE TRAÇABILITÉ

Le Comité de sécurité de l'information, chambre sécurité sociale et santé (dénommé ci-après « le Comité »);

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

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 3 décembre 2017 relative à la création de l'Autorité de protection des données, en particulier l'article 114, modifié par la loi du 25 mai 2018;

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 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre 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, notamment l'article 97;

Vu la délibération n° 14/011 du 21 janvier 2014, modifiée le 15 juillet 2014 et le 17 novembre 2017;

Vu la demande de modification;

Vu le rapport d'auditorat de la Plate-forme eHealth;

Vu le rapport de monsieur Bart Viaene;

Émet, après délibération, la décision suivante, le 3 décembre 2019:

I. OBJET DE LA DEMANDE

1. Suite à l'incident de la rupture d'implants mammaires en France, la Belgique en est venue à la constatation qu'elle a besoin d'un système d'enregistrement permettant de tracer les implants médicaux.

2. La loi du 15 décembre 2013 en matière de dispositifs médicaux (*M.B.* 20 décembre 2013) prévoit la création d'un tel registre.[1] Conformément à cette loi, tout distributeur qui met à disposition des implants en Belgique ainsi que tout praticien professionnel qui procède à l'implantation, au retrait ou remplacement d'un dispositif médical implantable, doit obligatoirement enregistrer certaines données auprès de l'Agence fédérale des médicaments et des produits de santé (AFMPS). L'entrée en vigueur des dispositions concernées de la loi ainsi que les modalités du traitement des données doivent cependant encore être précisées dans un arrêté royal, ce qui n'a pour l'instant pas encore été fait.

3. L'AFMPS soumet, à présent, à l'approbation du Comité, un projet pilote relatif à la communication de données à caractère personnel relatives à la santé dans le cadre du "Registre central de traçabilité".

4. Le registre a spécifiquement pour but de centraliser les notifications sur le cycle de vie d'un implant au moyen de la création d'une banque de données, d'interfaces utilisateurs et d'interfaces de système à système qui permettent aux prestataires de soins traitants (médecins et dentistes) du patient (dans ou en dehors d'un établissement de soins), à d'autres registres (Orthopride/Qermid) et à l'AFMPS d'introduire et de consulter la pose ou le retrait d'implants.

5. Le Registre central de traçabilité enregistre les données suivantes par notification:

- identification du patient : numéro d'identification de la sécurité sociale pseudonymisé[2] (NISS), sexe, année de naissance, code postal du domicile et date de décès ;

- identification (NISS) du médecin-spécialiste qui a posé ou retiré l'implant, du prescripteur de l'implant, du pharmacien qui l'a fourni et identification de l'établissement de soins (numéro INAMI) où l'implant a été posé ou retiré ;

- numéro de référence de l'implant posé/retiré et données supplémentaires relatives au produit (marque, producteur, distributeur)[3] ;

- date de la prescription, date de la délivrance et date de la pose ou du retrait ;

---

[1] Art. 51 de la loi du 15 décembre 2013 en matière de dispositifs médicaux, *M.B.*, 20 décembre 2013, p. 101490..

[2] Le NISS correspond au numéro de registre national ou au numéro d'identification attribué par la Banque Carrefour de la sécurité sociale.

[3] Le projet pilote concerne les implants suivants: les prothèses de hanches, les prothèses de genoux, les tuteurs coronaires, les pacemakers, les valves cardiaques, les défibrillateurs, les endoprothèses, les cœurs artificiels, les prothèses disque, les prothèses de cheville, les moniteurs cardiaques, les implants cochléaires, les implants mammaires.

- le numéro INAMI du médecin-spécialiste traitant, le numéro INAMI du médecin prescripteur. Seuls les 3 derniers chiffres (spécialité) seront disponibles à l'analyse ;

- date d'implantation, date de prescription, code d'identification de l'implant, code de notification SADMI, code d'identification INAMI, numéro INAMI du pharmacien, numéro INAMI de la pharmacie, date de délivrance, nombre d'implants, localisation anatomique.

- Identification du pharmacien via NISS et de la pharmacie via NIHII (RIZIV/INAMI) sera rendue optionnelle dans le registre de traçabilité, ce qui implique que ces données ne seront pas toujours présentes dans la database.

- la collecte du UDI (Unique Device Identification) sera également rendue optionnelle étant donné le report de l'assemblage EUDAMED (European database on medical devices)

6. Le Registre central de traçabilité est alimenté comme suit:

- Le registre peut être alimenté par certaines catégories de médecins[4] et par des dentistes au moyen d'une application web (pour les prestataires de soins en dehors d'un établissement de soins) ou au moyen d'un service web (pour les prestataires de soins travaillant dans un établissement de soins).[5] Avant qu'un prestataire de soins ne puisse enregistrer une notification, il est vérifié si le prestataire de soins possède effectivement une relation thérapeutique avec l'intéressé.

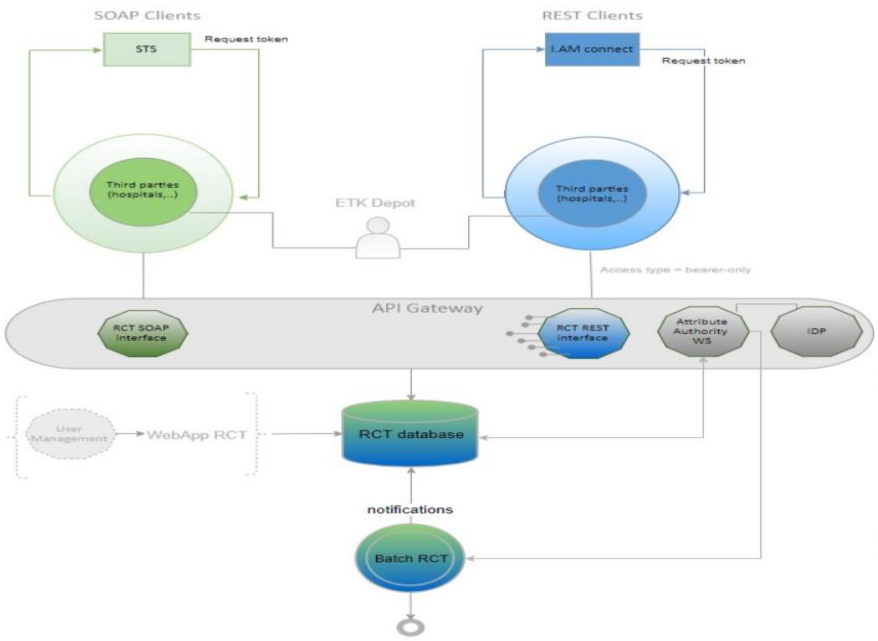
- Les centres d'implantation extra-muros continueront à effectuer les enregistrements via l'application web RCT.

En ce qui concerne la partie service web, un API REST sera rajouté aux opérations SOAP existantes permettant ainsi une intégration plus flexible dans l'échange machine-to-machine. Dans les 2 cas, il faut que toutes les données soient présentes de manière structurée dans les systèmes primaires de l'hôpital.

Un schéma permettra d'en préciser le contexte :

[4] Oncologie médicale, médecine d'urgence (MBS144), médecine aigue, gériatrie, médecine générale, anesthésie-réanimation, chirurgie, neurochirurgie, chirurgie plastique, neurologie, gynécologie-obstétrique, ophtalmologie, oto-rhino-laryngologie, urologie, orthopédie, stomatologie, dermato-vénéréologie, médecine interne, pneumologie, gastro-entérologie, pédiatrie, cardiologie, neuropsychiatrie, rhumatologie, médecine physique et réadaptation, radiothérapie, médecine nucléaire, réadaptation fonctionnelle et professionnelle des handicapés, médecine d'urgence (MPC22), endocrino-diabétologie, néonatologie, oncologie, gériatrie, chirurgie orale et maxillo-faciale, hématologie et oncologie pédiatrique, soins intensifs, neurologie pédiatrique, néphrologie.

[5] Dans le cadre du projet pilote, le nombre d'hôpitaux (notamment le CHU Charleroi et l'UZ Leuven) ainsi que le nombre de prestataire de soins extramuraux qui consulteront et enregistreront les données, est limité.



7. L'accès aux données non codées des notifications dans le Registre central de traçabilité est régi comme suit:

- un prestataire de soins en relation thérapeutique avec le patient concerné a accès aux données des notifications relatives à ce patient.

- le prestataire de soins qui a enregistré une notification peut, à tout moment, consulter les données de cette notification.

8. Suite à une notification, le registre génère une "carte implant" sous format pdf qui mentionne les données de la notification. Le prestataire de soins concerné est en mesure d'imprimer cette "carte implant" pour la remettre au patient. Cette "carte implant" est enregistrée sous formée chiffrée dans le registre.[6] En ce qui concerne l'accès à la "carte implant" déchiffrée, les mêmes règles que celles valables pour l'accès aux données non codées de la notification s'appliquent.

9. L'AFMPS a accès aux données des notifications dans le registre, mais non au NISS du patient. Grâce au numéro de référence d'un implant (et éventuellement du numéro de lot), l'AFMPS est en mesure d'établir une liste de toutes les notifications, de tous les implantateurs, distributeurs, prescripteurs et établissements de soins, etc., concernés par l'implant en question.

10. Lorsqu'un implant constitue un grave danger pour la santé publique ou lorsque le risque existe que ce type de dispositif médical ait entraîné ou puisse entraîner la mort d'un patient, d'un utilisateur ou d'un tiers ou gravement compromettre leur santé, et lorsque le seul moyen raisonnable pour y faire face est l'identification d'une ou de plusieurs personnes,

[6] La clé de chiffrement est, à son tour, chiffrée par la Plate-forme eHealth. Par ailleurs, un déchiffrement n'est possible qu'à la demande d'un utilisateur mandaté (prestataire de soins en relation thérapeutique avec le patient).

alors l'AFMPS peut procéder à l'identification de la personne ou des personnes concernées. La loi du 15 décembre 2013 prévoit que l'AFMPS doit, dans ce cas, en faire une déclaration motivée auprès du Conseil national de l'Ordre des médecins. Le Conseil peut déléguer un médecin afin de surveiller l'identification. Seul un médecin peut prendre contact avec la personne concernée, et lui communiquer les informations requises dans le respect du secret médical. La loi précise que le Roi détermine les modalités selon lesquelles cette identification peut avoir lieu, les moyens de communications qui peuvent être utilisés à cette occasion, et les procédés qui, compte tenu de la situation et de l'urgence éventuelle, sont préalablement mis en œuvre pour remédier à la situation et procéder à cette identification.

Vu les modalités limitées du projet pilote, il est prévu qu'en cas de crise grave, l'accès de l'AFMPS aux données à caractère personnel non codées doit faire l'objet d'une approbation spécifique et préalable du Comité sectoriel.

11. A l'occasion de l'enregistrement et de la consultation des données, plusieurs sources authentiques sont consultées:

- le registre national des personnes physiques : y sont consultés le nom, le prénom, le sexe, l'année de naissance de la personne concernée, le domicile principal et la date de décès. Les données s'affichent à l'écran de la personne qui enregistre les données, et ce pour éviter toute erreur. Ensuite, seuls le sexe, l'année de naissance, la date de décès et le code postal du domicile principal sont enregistrés dans le registre[7]. Afin de garantir la qualité des données du Registre central de traçabilité, le registre national doit communiquer automatiquement les modifications éventuelles relatives au numéro du registre national, à la date de naissance, au sexe, au décès et au code postal au RCT.

- CoBRHA[8]: cette source authentique est consultée pour valider l'identité des prestataires de soins et établissements de soins concernés. Le nom et le prénom des prestataires de soins ainsi que le nom de l'établissement de soins s'affichent à l'écran de l'utilisateur qui introduit les données, et ce pour éviter toute erreur.

- SADNDMI[9]: cette source authentique est consultée pour valider les implants et ajouter des données supplémentaires par implant (producteur, distributeur, marque, ...).

- banque de données des relations thérapeutiques: cette banque de données est tenue à jour par le Collège intermutualiste national (CIN). Elle contient les preuves électroniques d'une relation thérapeutique.

12. En vue du traitement des données à caractère personnel pseudonymisées à des fins statistiques et de rapportage, les données à caractère personnel pseudonymisées sont également communiquées à un datawarehouse de l'AFMPS. Ces données permettront de

[7] La consultation des données du registre national a été autorisée par la délibération n° 25/2014 du 24 mars 2014.
[8] CoBRHA est un fichier de données contenant les données d'identification de base des prestataires de soins agréés et des établissements de soins agréés. Il est tenu à jour par la Plate-forme eHealth et il est alimenté par l'ensemble des pouvoirs publics belges qui procèdent à l'agréation des prestataires de soins ou des établissements de soins.
[9] Sources Authentiques des Distributeurs Notifiés et des Dispositifs Médicaux Implantables (SADNDMI). Il s'agit de la banque de données qui, en vertu de la loi du 15 décembre 2013, doit être alimentée par les distributeurs d'implants.

calculer des statistiques sur les types d'implant par catégorie de personne concernée (critères : type, homme/femme, catégorie d'âge, …) ainsi qu'en cas d'incidents (recall) relatifs à un implant (critères : nombre de placements, catégories d'âge, …). En cas d'incident, le rapportage requis à des fins d'usage interne et/ou pour l'aide à la prise de décision politique, sera réalisé. L'accès aux données à caractère personnel enregistrées dans le datawarehouse se limite aux agents du service concerné de l'AFMPS.

II. COMPÉTENCE

13. Conformément à l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, toute communication de données à caractère personnel relatives à la santé, sauf exceptions prévues, requiert une autorisation de principe de la chambre sécurité sociale et santé du comité de sécurité de l'information.

14. Etant donné que les dispositions concernées de la loi du 15 décembre 2013 ne sont pas encore entrées en vigueur et que les modalités concrètes du traitement de données doivent encore être précisées par arrêté royal, le Comité est compétent pour se prononcer sur la communication de données à caractère personnel relatives à la santé dans le cadre du Registre central de traçabilité.

15. Le Comité souligne que l'utilisation du numéro de registre national et l'accès aux données du Registre national requièrent l'autorisation du Ministre de l'Intérieur, sauf s'il existe un fondement légal ou que la communication a fait l'objet d'une délibération du Comité sectoriel du Registre national. Le Comité constate que le Comité sectoriel du Registre national s'est prononcé sur cette communication dans la délibération RN n° 25/2014 du 24 mars 2014[10]. Le Comité doit par conséquent exprimer une réserve sur ce point.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

16. Le traitement de données à caractère personnel relatives à la santé est en principe interdit, et ce conformément au prescrit de l'article 9, §1er du RGPD.

17. Dans l'attente de l'entrée en vigueur des dispositions concernées de la loi du 15 décembre 2013 et de la rédaction des arrêtés d'exécution, il peut être constaté que le traitement peut, en l'occurrence, être estimé nécessaire pour la gestion des système et des services de soins de santé ou de protection sociale sur la base du droit de l'Union[11] (pour autant que les données soient traitées sous la surveillance d'un professionnel des soins de santé)[12].

18. Le Comité estime par conséquent qu'il existe un motif d'admissibilité valable pour le traitement des données à caractère personnel relatives à la santé envisagé.

---

[10] Délibération RN n°25/2014 du 24 mars 2014 demande d'autorisation formulée par l'Agence Fédérale des Médicaments et des Produits de Santé afin d'utiliser le Registre national dans le cadre d'un projet pilote relatif au Registre central de traçabilité (RN-MA-2014-021).
[11] Art 9, §2, h) du RGDP.
[12] Art. 9, §3 du RGPD.

B. FINALITÉ

19. 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.

20. Le Comité constate que la création du registre sous la responsabilité de l'AFMPS vise à développer un système d'enregistrement permettant de tracer les dispositifs médicaux implantés. Le système d'enregistrement a été mis au point pour les besoins des prestataires de soins concernés par le traitement du patient et de l'AFMPS qui peut ainsi surveiller l'utilisation et la distribution des implants et, dans des situations exceptionnelles, peut utiliser les données du registre pour prendre les mesures appropriées à l'égard des patients concernés.

21. La loi du 15 décembre 2013 décrit les finalités du registre comme suit:
- recueillir les informations nécessaires afin de permettre aux autorités et professionnels concernés d'accomplir leurs tâches en matière de matériovigilance, notamment identifier les incidents, et y apporter le suivi adéquat en vue de protéger la santé publique;
- recueillir les informations nécessaires à l'exécution par les autorités compétentes de leurs missions telles que décrites dans la loi du 15 décembre 2013;
- permettre aux patients et aux prestataires de soins en relation thérapeutique avec le patient de disposer de l'information la plus exacte possible sur la nature du dispositif médical implantable qui a été implanté chez la personne concernée;
- recueillir les informations nécessaires afin de permettre aux autorités compétentes d'exécuter leurs missions de protection de la santé publique, et notamment permettre de disposer et de communiquer des informations générales sur l'exposition de la population à un risque de matériovigilance;
- permettre de mieux connaître l'utilisation des dispositifs médicaux implantables;
- conserver les données qui pourraient servir de preuve dans le cadre d'une procédure judiciaire, administrative ou disciplinaire.

22. Conformément à sa mission légale, l'AFMPS s'assure de la qualité, de la sécurité et de l'efficacité des médicaments à usage humain (y compris des médicaments homéopathiques et des médicaments à base de plantes, des préparations magistrales et officinales), des médicaments à usage vétérinaire ainsi que des dispositifs médicaux et accessoires, de leur conception à leur utilisation. L'AFMPS veille également au bon déroulement de toutes les opérations effectuées avec le sang, les cellules et les tissus, de leur prélèvement à leur utilisation. Les domaines de compétence de l'AFMPS sont la recherche et le développement; l'enregistrement et l'autorisation de mise sur le marché de médicaments et de produits de santé; la vigilance; le contrôle de la production et de la distribution de médicaments et de produits de santé; et le bon usage de ces médicaments et produits.

23. Le Comité constate que le traitement envisagé poursuit des finalités déterminées, explicites et légitimes.

C. PROPORTIONNALITÉ

24. 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

25. Le Comité prend acte du fait que le nombre de catégories de données à caractère personnel qui sont enregistrées, est pertinent, bien qu'il soit limité, et que l'enregistrement a pour finalité la traçabilité des implants, tant dans le chef des prestataires de soins concernés que dans le chef de l'AFMPS, dans des situations exceptionnelles.

26. Le Comité constate en outre que les données à caractère personnel sont enregistrées sous forme pseudonymisée et qu'il est à cet égard fait appel aux services de base de la Plate-forme eHealth. Les "cartes implant" sous format pdf (contenant des données à caractère personnel non pseudonymisées) sont conservées sous forme chiffrée et peuvent uniquement être déchiffrées par des prestataires de soins en relation thérapeutique avec la personne concernée (et par le prestataire de soins qui a réalisé la notification en question). La clé de chiffrement est, à son tour, codée par la Plate-forme eHealth. Par ailleurs, un déchiffrement n'est possible qu'à la demande d'un utilisateur mandaté.

27. Les données à caractère personnel pseudonymisées sont utilisées par l'AFMPS pour réaliser des recherches relatives à certains implants, à la lumière des finalités précitées. Les données à caractère personnel pseudonymisées seront également traitées, afin de pouvoir réaliser les statistiques et le rapportage utiles à la lumière de la finalité spécifique du registre[13].

28. Seuls les prestataires de soins (médecins et dentistes) en relation thérapeutique avec la personne concernée peuvent enregistrer les notifications et consulter les données à caractère personnel non codées. Par dérogation à ce qui précède, les prestataires de soins qui ont enregistré des notifications peuvent toujours consulter leurs propres notifications.

29. Le Comité constate que L'AFMPS n'aura accès à des données à caractère personnel non pseudonymisées (identité de la personne concernée) que dans des cas exceptionnels visés par l'article 51, §§ 6 et 8 de la loi du 15 décembre 2013 en matière de dispositifs médicaux. Sans préjudice des dispositions légales applicables, le Comité estime que le responsable du traitement des données doit mettre en œuvre des mesures afin de garantir que seul les acteurs autorisés légalement puissent accéder à la banque de données et à identifier la personne concernée. Cependant, vu la phase pilote, cet accès devra toujours faire l'objet d'une autorisation spécifique complémentaire du Comité de sécurité de l'information.

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

31. Conformément à l'article 5 du RGPD, les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que

[13] Article 51, § 3 de la loi du 15 décembre 2013 en matière de dispositifs médicaux.

pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. La loi du 15 décembre 2013 précise que les données à caractère personnel seront conservées pendant une période de 30 ans après le décès de la personne concernée ou pendant une période de 30 ans après le moment auquel le dispositif médical implanté est définitivement explanté. Etant donné qu'il s'agit d'un projet pilote, le Comité estime que les données à caractère personnel doivent être détruites à l'issue du projet pilote, sauf s'il y a un déploiement général du registre dans le cadre de la loi du 15 décembre 2013 et de ses arrêtés d'exécution. Le Comité estime que, dans ce cas, il est acceptable que les données à caractère personnel déjà enregistrées dans le Registre central de traçabilité soient conservées conformément aux modalités prévues dans la loi précitée.

32. Le Comité prend acte du fait que la Plate-forme eHealth interviendra, conformément à l'article 5, 8° de la loi du 21 août 2008 relative à l'institution et à l'organisation de la Plate-forme eHealth, lors du codage des numéros d'identification des personnes concernées. Le lien entre le numéro codé et le numéro d'identification réel doit être conservé pendant une période identique à celle prévue pour les données enregistrées dans le Registre central de traçabilité. Par ailleurs, la possibilité de décodage est indispensable dans les cas suivants:
- consultation des notifications par les prestataires de soins en relation thérapeutique avec un patient (dans un ou en dehors d'un établissement de soins);
- consultation des notifications par l'AFMPS dans des situations de crise (après autorisation spécifique complémentaire du Comité).

D. TRANSPARENCE

33. Lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement doit fournir plusieurs informations à la personne concernée.[14] Cette disposition ne s'applique pas, notamment, lorsque la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés. En pareil cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.

34. Compte tenu de ce qui précède, le Comité estime que tant les prestataires de soins concernés, les gestionnaires des registres Orthopride et Qermid que l'AFMPS sont dispensés de la notification à la personne concernée.

E. MESURES DE SÉCURITÉ

35. Selon l'article 9, §3 du RGPD, les données à caractère personnel relatives à la santé peuvent faire l'objet d'un traitement prévu au §2, point h), si ces données sont traitées par un professionnel des soins de santé soumis à une obligation de secret professionnel conformément au droit de l'Union ou sous sa responsabilité ou par une autre personne également soumise à une obligation de secret. Même si cela n'est pas strictement requis par le RGPD, le Comité estime qu'il est préférable de traiter de telles données sous la

[14] Article 14 du RGPD.

responsabilité d'un médecin. 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. Le Comité prend acte du fait que le traitement des données à caractère personnel se fera effectivement sous la surveillance et la responsabilité d'un médecin de l'AFMPS.

36. Conformément au RGPD, le responsable du traitement doit prendre toutes les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel. Ces mesures doivent assurer 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.

37. Le Comité rappelle que compte tenu des dispositions de l'article 51 de la loi du 15 décembre 2013 en matière de dispositifs médicaux, l'AFMPS ne peut avoir accès à l'identité de la personne concernée que dans les cas mentionnés aux paragraphes 6 et 8 du même article. Par conséquent, le Comité exige qu'un filtre soit mis en place de sorte que l'AFMPS n'ait accès qu'à des données pseudonymisées afin de limiter le risque de réidentification de la personne concernée.

38. 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 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, …); documentation[15]. Le Comité prend acte du fait que l'AFMPS confirme qu'elle prévoit toutes les mesures de sécurité applicables requises.

39. En ce qui concerne la protection de l'application web, le Comité prend acte du fait que l'application est accessible via le portail web sécurisé de la Plate-forme eHealth et la gestion des utilisateurs et des accès de la Plate-forme eHealth. Les utilisateurs doivent s'identifier et s'authentifier au moyen de leur carte d'identité électronique. Leur qualité et leurs droits d'accès sont ensuite vérifiés dans les sources authentiques pertinentes. Le traitement de données à caractère personnel dans le cadre de la gestion des utilisateurs et des accès de la Plate-forme eHealth a été autorisé par la délibération n° 09/008 du Comité sectoriel. Dans le cadre du service web et pour la protection de l'échange de données, il est fait appel au service de base 'end-to-end encryption' de la Plate-forme eHealth. En outre, les notifications font l'objet d'un horodatage pour lequel il est également fait appel au service

[15] « Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel », document rédigé par la Commission de la protection de la vie privée disponible à l'adresse: http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf

de base concerné de la Plate-forme eHealth. Enfin, tous les enregistrements et consultations de données feront l'objet de loggings de sécurité.

40. Le Comité rappelle qu'il est interdit d'entreprendre toute action visant à convertir les données à caractère personnel pseudonymisées qui ont été communiquées en données à caractère personnel non pseudonymisées.

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 supplémentaires 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.

Par ces motifs,

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

sous réserve de l'autorisation Ministre de l'Intérieur en ce qui concerne l'accès au Registre national et sous réserve de l'autorisation de Comité de sécurité de l'information en ce qui concerne l'accès aux données des registres de la Banque Carrefour de la sécurité sociale ;

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 d'identification réel et le numéro pseudonymisé pendant une période identique à celle prévue pour les données à caractère personnel du Registre central de traçabilité comme prévu au point 31.

La Plate-forme eHealth est autorisée à procéder au décodage des données à caractère personnel pseudonymisées dans les cas prévus sous le point 32. Tout accès de l'AFMPS à des données à caractère personnel non codées requiert une autorisation explicite complémentaire du Comité sectoriel.

Bart VIAENE