



**Comité sectoriel de la sécurité sociale et de la santé
Section "Santé"**

CSSSS/14/113

**DÉLIBÉRATION N° 14/011 DU 21 JANVIER 2014, MODIFIÉE LE 15 JUILLET 2014,
PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL
CODÉES RELATIVES À LA SANTÉ À L'AGENCE FÉDÉRALE DES MÉDICAMENTS
ET DES PRODUITS DE SANTÉ DANS LE CADRE DU REGISTRE CENTRAL DE
TRAÇABILITÉ**

La section santé du Comité sectoriel de la sécurité sociale et de la santé (dénommée ci-après « le Comité sectoriel »);

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;

Vu la loi du 13 décembre 2006 portant dispositions diverses;

Vu la délibération n° 14/011 du 21 janvier 2014;

Vu la demande de modification;

Vu le rapport d'auditorat de la Plate-forme eHealth du 30 juin 2014;

Vu le rapport de monsieur Yves Roger;

Émet, après délibération, la décision suivante, le 15 juillet 2014:

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 sectoriel, 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 codé² (NISS), sexe et année de naissance.
 - 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.
6. Le Registre central de traçabilité est alimenté comme suit:

¹ Art. 50 et suivants.

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 registre peut être alimenté par certaines catégories de médecins⁴ 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 prestataires de soins sont actuellement déjà obligés de communiquer des données relatives aux implants posés à l'INAMI, plus précisément dans le cadre des applications Orthoprïde⁶ et Qermid (tuteurs coronaires⁷; endoprothèses⁸; et pacemakers et défibrillateurs⁹). Pour éviter que les prestataires de soins ne doivent communiquer plusieurs fois les mêmes données à différentes banques de données, il est prévu que les données à caractère personnel concernées qui sont déjà enregistrées dans les applications Orthoprïde et Qermid soient communiquées au Registre central de traçabilité.
7. Avant que les données de la notification ne puissent être enregistrées dans le Registre central de traçabilité, le NISS du patient est codé au moyen du service de base concerné de la Plate-forme eHealth. La Plate-forme eHealth conserve le lien entre le numéro codé et le numéro d'identification réel, de sorte que le même numéro codé soit toujours attribué à la personne concernée. Les données à caractère personnel codées ne peuvent cependant être décodées que dans les cas décrits ci-dessous.
 8. 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.
 9. 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

⁴ Oncologie médicale, médecine d'urgence (MBS144), médecine aiguë, gériatrie, médecine générale, anesthésie-réanimation, chirurgie, neurochirurgie, chirurgie plastique, neurologie, gynécologie-obstétrique, ophtalmologie, oto-rhino-laryngologie, urologie, orthopédie, stomatologie, dermato-vénérologie, 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, néonatalogie, 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 extramurales qui consulteront et enregistreront les données, est limité.

⁶ Délibération n° 08/048 du 2/09/2008, dernièrement modifiée le 17 juillet 2012.

⁷ Délibération n° 11/053 du 19 juillet 2011, dernièrement modifiée le 17 juillet 2012.

⁸ Délibération n° 11/015 du 15 février 2011, modifiée le 19 juin 2012.

⁹ Délibération n° 09/073 du 15 décembre 2009, dernièrement modifiée le 18 octobre 2011 (défibrillateurs et pacemakers).

enregistrée sous formée chiffrée dans le registre.¹⁰ 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.

10. 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.
11. 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, 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.

12. 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 registre¹¹. 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 nationale, à la date de naissance, au sexe, au décès et au code postal au RCT.

¹⁰ 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).

¹¹ La consultation des données du registre national a été autorisée par la délibération n° 25/2014 du 24 mars 2014.

- CoBRHA¹²: 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.
 - SADNDMI¹³: 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.
13. En vue du traitement des données à caractère personnel codées à des fins statistiques et de rapportage, les données à caractère personnel codées sont également communiquées à un datawarehouse de l'AFMPS. Ces données permettront de 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

14. 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 du Comité sectoriel.
15. Etant donné que la loi du 15 décembre 2013 n'est pas encore entrée en vigueur et que les modalités concrètes du traitement de données doivent encore être précisées par arrêté royal, le Comité sectoriel 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.
16. Le Comité sectoriel souligne que l'utilisation du numéro de registre national et l'accès aux données du Registre national requièrent l'autorisation du Comité sectoriel du Registre national, sauf s'il existe un fondement légal. Le Comité sectoriel doit par conséquent exprimer une réserve sur ce point.

¹² 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'agrégation des prestataires de soins ou des établissements de soins.

¹³ 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.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

17. Le traitement de données à caractère personnel relatives à la santé est en principe interdit¹⁴, sauf dans les exceptions prévues dans la loi relative à la vie privée.
18. Dans l'attente de l'entrée en vigueur 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 à la promotion et à la protection de la santé publique¹⁵ et à la gestion de services de santé agissant dans l'intérêt de la personne concernée (pour autant que les données soient traitées sous la surveillance d'un professionnel des soins de santé)¹⁶.
19. Le Comité sectoriel estime par conséquent qu'il existe un motif d'admissibilité valable pour le traitement des données à caractère personnel relatives à la santé envisagé.

B. FINALITÉ

20. L'article 4, § 1^{er}, 2^o, de la loi relative à la vie privée autorise le traitement de données à caractère personnel uniquement pour des finalités déterminées, explicites et légitimes.
21. Le Comité sectoriel 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.
22. 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;

¹⁴ Article 7, § 1^{er}, 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 (*M.B.* 18 mars 1993) (dénommée ci-après loi relative à la vie privée).

¹⁵ Art. 7, § 2, d) de la loi relative à la vie privée.

¹⁶ Art. 7, § 2, j) de la loi relative à la vie privée.

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

C. PROPORTIONNALITÉ

25. L'article 4, § 1^{er}, 3^o, de la loi relative à la vie privée dispose que 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.
26. Le Comité sectoriel 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.
27. Le Comité sectoriel constate en outre que les données à caractère personnel sont enregistrées sous forme codée 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 codées) 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.
28. Les données à caractère personnel codées sont utilisées par l'AFMPS pour réaliser des recherches relatives à certains implants, à la lumière des finalités précitées. Les données à caractère personnel codées seront également traitées, afin de pouvoir réaliser les statistiques et le rapportage utiles à la lumière de la finalité spécifique du registre.
29. 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.
30. L'AFMPS n'aura accès à des données à caractère personnel non codées que dans des cas exceptionnels. Cependant, vu la phase pilote, cet accès devra toujours faire l'objet d'une autorisation spécifique complémentaire du Comité sectoriel.
31. Compte tenu de l'objectif de traçabilité, le Comité sectoriel estime que le traitement de ces données à caractère est en principe adéquat, pertinent et non excessif.
32. Conformément à l'article 4, § 1^{er}, 5^o, de la loi relative à la vie privée, les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. 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 sectoriel 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 sectoriel 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.

33. Le Comité sectoriel 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 sectoriel).

D. TRANSPARANCE

34. Lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement doit, dès l'enregistrement des données à caractère personnel, ou si une communication de données à caractère personnel à un tiers est envisagée, au plus tard au moment de la première communication des données à caractère personnel, fournir plusieurs informations.¹⁷ Le responsable du traitement est dispensé de cette notification lorsque pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés, et lorsque l'enregistrement est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.
35. Par ailleurs, le responsable du traitement de données à caractère personnel, collectées pour des fins déterminées, explicites et légitimes et l'organisation intermédiaire ne doivent pas respecter l'obligation d'information dans le cadre du traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques lorsque l'organisation intermédiaire est une autorité administrative chargée explicitement, par ou en vertu de la loi, de rassembler et de coder des données à caractère personnel et soumise, à cet égard, à des mesures spécifiques visant à protéger la vie privée. En l'occurrence, la Plate-forme eHealth intervient pour le codage des données à caractère personnel, avant leur transmission au Registre central de traçabilité.
36. Compte tenu de ce qui précède, le Comité sectoriel estime que tant les prestataires de soins concernés, les gestionnaires des registres Orthoprive et Qermid que l'AFMPS sont dispensés de la notification à la personne concernée.

¹⁷ Article 9 de la loi relative à la vie privée.

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

37. Le responsable du traitement est tenu, avant de mettre en œuvre un traitement entièrement ou partiellement automatisé, de faire une déclaration à la Commission de la protection de la vie privée. L'AFMPS devra donc s'en charger.¹⁸

F. MESURES DE SÉCURITÉ

38. Les données à caractère personnel relatives à la santé peuvent uniquement être traitées sous la surveillance et la responsabilité d'un professionnel des soins de santé. Même si cela n'est pas strictement requis dans la loi relative à la vie privée, le Comité sectoriel estime qu'il est préférable de traiter de telles données sous la responsabilité d'un médecin.¹⁹ Le Comité sectoriel rappelle que lors du traitement de données à caractère personnel, le professionnel des soins de santé ainsi que ses préposés ou mandataires sont soumis au secret²⁰. Le Comité sectoriel 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.
39. Conformément à l'article 16, § 4, de la loi relative à la vie privée, les demandeurs doivent prendre toutes les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel. Ces mesures devront assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraînent l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.
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 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, ...); documentation²¹. Le Comité sectoriel prend acte du fait que l'AFMPS confirme qu'elle prévoit toutes les mesures de sécurité applicables requises.
41. En ce qui concerne la protection de l'application web, le Comité sectoriel prend acte du fait que l'application est accessible via le portail web sécurisé de la Plate-forme eHealth et

¹⁸ Article 17 de la loi relative à la vie privée.

¹⁹ Art. 7, § 4, de la loi relative à la vie privée.

²⁰ Art. 7, § 4, de la loi relative à la vie privée.

²¹ « 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

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

42. Le Comité sectoriel rappelle qu'il est interdit, conformément à l'article 6 de l'arrêté royal du 13 février 2001 portant exécution 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, d'entreprendre toute action visant à convertir les données à caractère personnel codées qui ont été communiquées en données à caractère personnel non codées. Le non-respect de cette interdiction peut donner lieu à une amende en vertu de l'article 39, 1°, de la loi relative à la vie privée. Le Comité sectoriel rappelle également qu'en cas de condamnation du chef d'infraction à l'article 39, le juge peut prononcer la confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction (fichiers manuels, disques et bandes magnétiques, ...) ou ordonner l'effacement de ces données. Le juge peut également interdire de gérer, personnellement ou par personne interposée, et pour deux ans au maximum, tout traitement de données à caractère personnel²².

²² Article 41 de la loi relative à la vie privée.

Par ces motifs,

la section Santé du Comité sectoriel de la sécurité sociale et de la santé

sous réserve de l'obtention de l'autorisation du Comité sectoriel du Registre national pour l'utilisation du numéro de registre national et l'accès aux données du Registre national,

autorise, aux modalités de la présente délibération, la communication de données à caractère personnel codées relatives à la santé à l'Agence fédérale des médicaments et des produits de santé dans le cadre du Registre central de traçabilité, et ce à l'intervention de la Plate-forme eHealth en vue du codage des données à caractère personnel.

La Plate-forme eHealth est autorisée à conserver le lien entre le numéro d'identification réel et le numéro codé pendant une période identique à celle prévue pour les données à caractère personnel du Registre central de traçabilité, comme prévu au point 32

La Plate-forme eHealth est autorisée à procéder au décodage des données à caractère personnel codées dans les cas prévus sous le point 33. Tout accès de l'AFMPS à des données à caractère personnel non codées requiert une autorisation explicite complémentaire du Comité sectoriel.

Yves ROGER
Président

| |
|--|
| Le siège du comité sectoriel de la sécurité sociale et de la santé est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles. |
|--|