Comité sectoriel de la sécurité sociale et de la santé
Section « Santé »

CSSSS/11/049

DÉLIBÉRATION N° 11/014 DU 15 FÉVRIER 2011, MODIFIÉE POUR LA DERNIÈRE FOIS LE 20 MARS 2012, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ DANS LE CADRE DE L'APPLICATION WEB 'WEBWACHTMAILER'

La section santé du Comité sectoriel de la sécurité sociale et de la santé (*dénommée ci-après* : "*le Comité sectoriel*"),

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

Vu l'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*;

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 délibération du Comité sectoriel du 15 février 2011, modifiée le 22 novembre 2011;

Vu la demande de modification de la délibération précitée, reçue le 6 février 2012;

Vu le rapport d'auditorat de la plate-forme eHealth du 12 mars 2012;

Vu le rapport de monsieur Yves Roger,

Émet, après délibération, la décision suivante, le 20 mars 2012 :

I. OBJET DE LA DEMANDE

1. L'asbl Hermes met à disposition une application web grâce à laquelle un médecin de garde peut rédiger un rapport de garde dans le cadre du service de garde des médecins généralistes. L'objectif de cette application web est double:

   - garantir la continuité des soins grâce à la rédaction et à la transmission du rapport de garde par le médecin de garde au médecin généraliste du patient concerné;
   - communiquer une sélection de données à caractère personnel codées contenues dans ces rapports de garde au coordinateur de chaque cercle de garde, en vue de la rédaction du rapport annuel obligatoire sur le fonctionnement des services de garde à l'attention du SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement. Ce rapport contient exclusivement des données agrégées et anonymisées.

2. En fonction de la présence ou non d'une fonction de réceptionniste dans le poste de garde du cercle concerné, une procédure différente est appliquée pour la création d'un rapport de garde. Si un réceptionniste est présent, celui-ci enregistre d'abord un nombre limité de données à caractère personnel relatives au patient. Ces données sont enregistrées dans une 'liste salle d'attente'. Si le médecin de garde concerné rédige ensuite le rapport de garde, les données à caractère personnel provenant de la liste salle d'attente sont remplies automatiquement dans le rapport de garde, qui est complété par le médecin de garde. Si la fonction de réceptionniste n'est pas prévue, il n'y a pas de liste salle d'attente et le médecin de garde concerné doit remplir lui-même toutes les données à caractère personnel requises.

3. Si la fonction de réceptionniste est prévue dans le poste de garde du cercle concerné, le réceptionniste se connecte au moyen de sa carte eID[1]. La gestion des utilisateurs et des accès de la plate-forme eHealth identifie et authentifie, sur la base des données de l'eID, la personne concernée et transmet les données d'identification de la personne concernée à l''Access Control List' de l'application web. Cet Access Control List contient les droits d'accès des utilisateurs de l'application web. Les droits d'accès dans l'Access Control List sont déterminés par le coordinateur de chaque cercle de médecins généralistes, en ce qui concerne les utilisateurs de son cercle de médecins généralistes (réceptionnistes et médecins de garde). Toute modification de cette liste de contrôle d'accès fait l'objet d'une journalisation. Si le réceptionniste peut faire valoir des droits d'accès conformément à l'Access Control List, l'accès lui est accordé. Si le réceptionniste ne reçoit pas d'accès de l'Access Control List, une page contenant un message erreur s'affiche.

4. Si le réceptionniste autorisé s'est identifié et authentifié correctement, il peut ensuite enregistrer les données suivantes relatives au patient:
   - numéro d'identification de la sécurité sociale (soit le numéro d'identification du Registre national ou le numéro d'identification attribué par la Banque Carrefour de la sécurité sociale)
   - nom, prénom
   - date de naissance
   - sexe:

[1] Comme back-up, il est prévu que la connexion peut également se faire au moyen du token citoyen.

- rue, numéro maison, code postal et domicile
- données de communication (téléphone, GSM, …)

- la raison de l'appel en texte libre
- le moment de l'appel
- le type de contact:
  - visite à domicile
  - téléphonique
  - consultation
- le degré d'urgence (salle d'attente):
  - pas urgent
  - urgent
  - extrêmement urgent
- médecin généraliste du patient (liste de choix): derrière la liste de choix (nom, prénom) se trouvent les données suivantes du médecin:
  - adresse: rue, n° de la maison, code postal, domicile
  - numéro INAMI
  - détenteur d'un compte medibridge (O/N)
  - détenteur d'un compte eHealthbox (O/N)

5. Ces données constituent donc la 'liste salle d'attente' et sont uniquement visibles pour la réception et le médecin de garde. Lors de la rédaction du rapport de garde par le médecin de garde, ces données sont automatiquement intégrées dans ce rapport et - si nécessaire - corrigées par le médecin de garde. Les données sont ensuite définitivement supprimées de la liste salle d'attente.

6. Le médecin de garde qui souhaite rédiger un rapport de garde se connecte également au moyen de sa carte eID[2]. La gestion des utilisateurs et des accès de la plate-forme eHealth identifie et authentifie la personne concernée au moyen des données de sa carte eID et vérifie au moyen des données contenues dans la banque de données fédérale des professionnels des soins de santé si la personne concernée est effectivement un médecin. Dans l'affirmative, la gestion des utilisateurs et des accès de la plate-forme eHealth transmet ensuite les données d'identification à l'Access Control List de l'application web. L'Access Control List vérifie si le médecin de garde peut faire valoir des droits d'accès. Dans l'affirmative, le médecin de garde se voit accorder l'accès à l'application.

7. S'il s'est connecté avec succès, le médecin de garde ouvre un nouveau rapport de garde. Si la fonction de réceptionniste est prévue et que celui-ci a rempli les données du patient concerné dans la liste salle d'attente, les données enregistrées dans la liste salle d'attente sont automatiquement préremplies dans le rapport de garde. En l'absence d'un réceptionniste, le médecin de garde doit remplir lui-même l'ensemble des données énumérées ci-après.

8. S'il s'est identifié et authentifié correctement, le médecin de garde autorisé peut enregistrer les données suivantes dans le rapport de garde:
   - le nom/prénom/domicile du médecin généraliste personnel (destinataire du rapport) est sélectionné dans une liste de choix, derrière laquelle se trouvent les données suivantes par médecin
     - adresse: rue, n°, code postal, domicile
     - numéro INAMI

[2] Comme back-up, il est prévu que la connexion peut également se faire au moyen du token citoyen.

- détenteur d'un compte medibridge (oui/non)
- détenteur d'un compte eHealthbox (oui/non)

- données du patient
  - numéro d'identification de la sécurité sociale (soit le numéro d'identification du Registre national ou le numéro d'identification attribué par la Banque Carrefour de la sécurité sociale)
  - nom, prénom
  - date de naissance
  - sexe:
  - rue, n°, code postal, domicile
  - données de communication (téléphone, GSM, …)
- données de contact
  - type de contact (visite à domicile/consultation/contact téléphonique)
  - moment de l'appel
  - moment du contact avec le médecin
  - degré d'urgence (peut attendre jusqu'après la garde/utilisation normale des services de garde/urgent/extrêmement urgent)
- données médicales
  - plaintes subjectives (= plaintes communiquées lors de l'appel)
    - classification IBUI[3]
    - texte libre
  - constatations objectives
    - texte libre
  - évaluation par médecin (= diagnostic)
    - classification IBUI
    - texte libre
  - planning par médecin
    - médication
      - code CNK[4]
      - nombre de conditionnements
      - instructions
    - actes
      - classe ICPC2
      - type: renvoi, vaccination, suture, ...
      - texte libre
    - attestation d'absence
      - date de début
      - date de fin
      - prolongation (oui/non)
      - cause (accident/maladie)
      - type (travail/école/sport)
    - texte libre
- refus du patient de donner accès au rapport de garde pendant le service de garde[5]

---

[3] Identificateur unique belge, numéro d'un terme de thésaurus médical, lié à un code ICP2-code et un code ICD10.

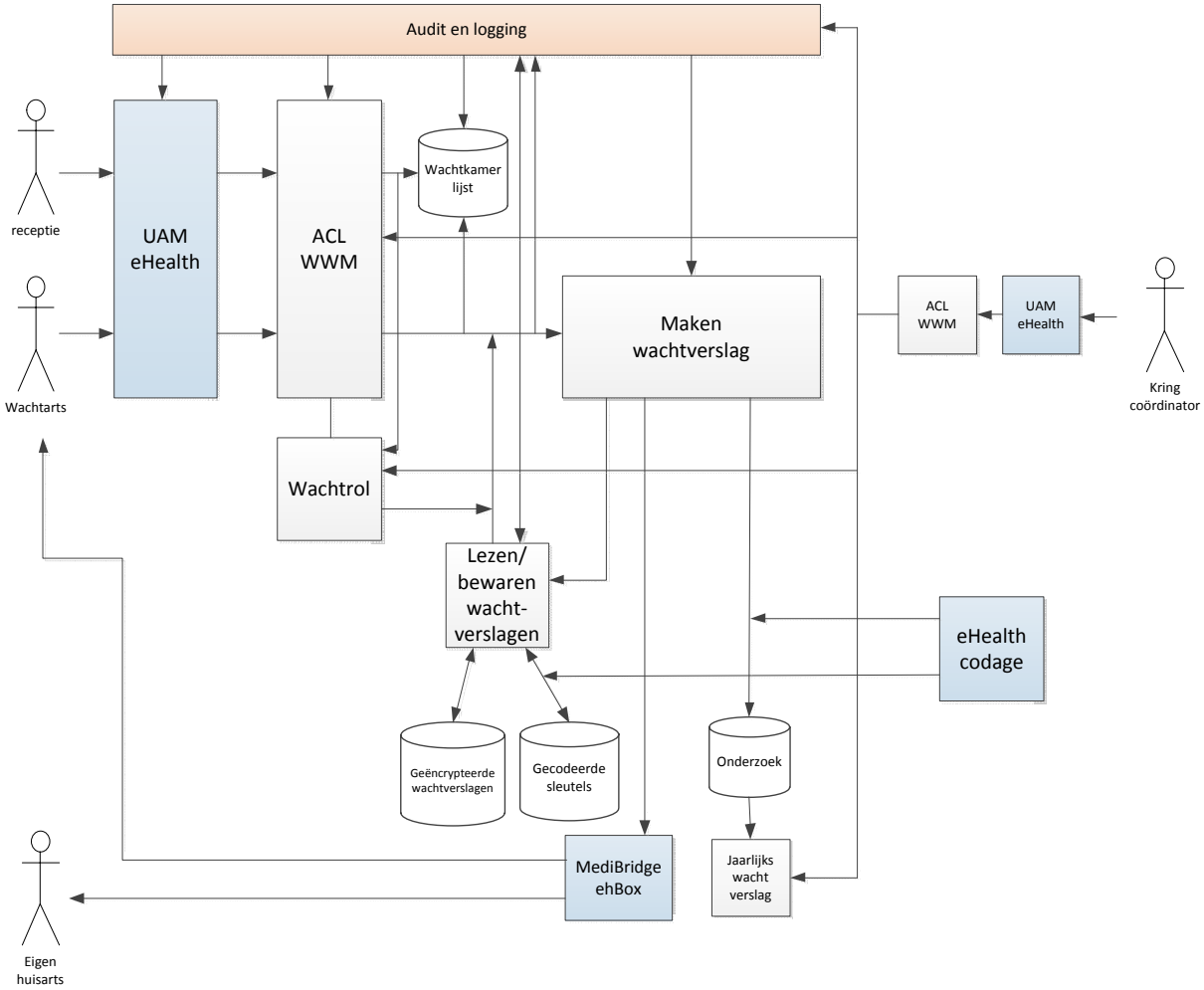
[4] Système de codage belge des médicaments.

[5] L'application prévoit la possibilité pour un médecin de garde de lire le rapport de garde rédigé par un autre médecin de garde dans le mois de la création du rapport de garde (cf. infra). Le patient peut cependant s'y opposer explicitement.

9. Est ajouté au rapport de garde, l'identification de l'auteur du rapport de garde (le médecin de garde), l'identification du cercle de garde concerné ainsi qu'un numéro unique.

10. Les parties suivantes de l'application web sont ensuite activées:
- transmission rapport de garde au médecin généraliste personnel;
- transmission copie personnelle rapport de garde au médecin de garde;
- codage, agrégation et transmission des données vers la banque de données de recherche codées en vue de la rédaction du rapport de garde annuel,
- chiffrement et enregistrement du rapport de garde en vue de son utilisation ultérieure (cf. infra).

D'un point de vue schématique, ceci peut être présenté comme suit :



11. Après que le médecin de garde a confirmé le rapport, il est envoyé au médecin généraliste personnel du patient via les services d'un développeur logiciel[6].

12. Après confirmation du rapport, le module de rapport de garde convertit les données dans un format spécifique. Le demandeur déclare que tout logiciel de gestion du dossier médical électronique par les médecins généralistes est capable d'intégrer ce format.

[6] Medibridge.

13. Le rapport est ensuite chiffré de manière asymétrique au moyen du service de chiffrement du développeur logiciel précité et est envoyé au médecin généraliste personnel du patient à l'aide du numéro INAMI. Le message est déchiffré chez le médecin généraliste par son propre programme. Il est ensuite intégré automatiquement dans le dossier médical électronique du patient concerné.

14. Si le médecin généraliste personnel n'utilise pas les services du développeur logiciel précité, le rapport est imprimé chez le médecin de garde. Celui-ci envoie ensuite le rapport par la poste au médecin généraliste personnel ou le remet au patient.

15. Étant donné que le médecin de garde doit conserver une copie de son propre rapport de garde, il est nécessaire qu'il reçoit également ce rapport. Le mode d'envoi est identique au mode d'envoi au médecin généraliste.

16. Dans une phase ultérieure, l'application web communiquera les rapports de garde au médecin généraliste et au médecin de garde concerné au moyen de la boîte aux lettres électronique sécurisée de la plate-forme eHealth, l'eHealth-box.

17. Une sélection des données du rapport de garde est communiquée à une banque centrale de données de recherche. Celle-ci est uniquement accessible aux coordinateurs des cercles de médecins généralistes en vue de la rédaction du rapport de garde annuel et les coordinateurs concernés ne peuvent consulter que les seuls rapports de garde de leur propre cercle de médecins généralistes. Conformément à l'article 7 de l'arrêté royal du 8 juillet 2002 *fixant les missions confiées aux cercles de médecins généralistes,* tout cercle de médecins généralistes agréé est, en effet, obligé d'organiser, dans le cadre de l'organisation de service de garde, l'enregistrement des données suivantes: *épidémiologie, problèmes de sécurité, plaintes de patients, plaintes à propos des services.* Ce rapport qui contient uniquement des données anonymes et agrégées est ensuite envoyé par tout coordinateur de cercle au service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement.

18. Avant de transmettre la sélection de données à la banque de données de recherche, le numéro d'identification de la sécurité sociale (NISS) de la personne concernée est codé au moyen du service de base 'codage et anonymisation' de la plate-forme eHealth. La plate-forme eHealth conserve le lien entre le NISS et le numéro codé à des fins d'études longitudinales; toutefois, aucune possibilité de décodage n'est prévue.

19. La banque de données de recherche codées contient les données suivantes, par rapport de garde:
    - numéro d'identification de la sécurité sociale (soit le numéro d'identification du Registre national ou le numéro d'identification attribué par la Banque Carrefour de la sécurité sociale)
    - numéro d'identification du cercle de garde dont fait partie le médecin de garde émetteur
    - données du patient
        - sexe:
        - code postal:
        - classe d'âge ('0','1-4','5-9','10-14','15-19','20-24','25-29','30-34','35-39','40-44','45-49','50-54','55-59','60-64','65-69','70-74','75-79','80-84','85-89','90-94','95+','inconnu')
    - données de contact

- type de contact (visite à domicile/consultation/contact téléphonique)
- laps de temps entre l'appel et le contact avec le médecin
- moment agrégé du contact avec le médecin
    - année
    - numéro de la semaine
    - weekend ou période de lundi à vendredi
    - heure du contact
- degré d'urgence (peut attendre jusqu'après la garde/utilisation normale des services de garde/urgent/extrêmement urgent)

- données médicales
    - plaintes subjectives (= plaintes communiquées lors de l'appel): classification IBUI
    - évaluation par médecin (= diagnostic) : classification IBUI
- référence
    - numéro INAMI institution

20.1. Les données à caractère personnel codées ne sont conservées dans la banque de données que pour la durée de dix-huit mois, plus précisément le temps nécessaire à la rédaction du rapport de garde annuel.

20.2. L'application prévoit également que les rapports de garde sont conservés de manière chiffrée sur un serveur central pour deux finalités:

- le médecin de garde doit toujours disposer d'un rapport de la consultation qu'il a réalisé. Bien qu'il reçoive comme décrit ci-dessus une copie électronique, l'expérience a, selon le demandeur, montré que des rapports de garde se sont égarés suite à des problèmes techniques. C'est la raison pour laquelle les rapports de garde sont conservés sur un serveur pendant un an, ensuite, ils sont détruits définitivement. L'utilisateur qui est intervenu en tant que médecin de garde est averti à plusieurs reprises qu'il doit télécharger ces rapports. Seul l'auteur du rapport de garde peut télécharger le rapport de garde pour cette finalité.

- par ailleurs, en vue de la continuité des soins, il est indispensable qu'un médecin de garde puisse lire les rapports de garde d'un patient en cas de *nouvelle consultation*, par exemple dans les cas suivants:
  ° un patient palliatif auquel le médecin de garde rend visite éventuellement plusieurs fois par jour ;
  ° un patient qui demande des explications par téléphone concernant une consultation antérieure ;
  ° un patient qui informe le médecin de garde sur l'évolution de sa maladie ;
  ° une deuxième consultation au cours du weekend pour la même maladie.

  Etant donné que les rapports de garde n'ont pour cette finalité qu'une utilisation limitée dans le temps, il est seulement possible de demander leur affichage jusqu'à un mois à compter de la création du rapport de garde.

20.3. Les rapports sont enregistrés pour les finalités précitées, de manière chiffrée, sur un serveur central de sorte que seuls les utilisateurs autorisés puissent avoir accès au contenu des rapports (cf. infra). Etant donné que les rapports de garde sont conservés de manière chiffrée, les gestionnaires du serveur ne sont pas en mesure de prendre connaissance des rapports de garde.

II. COMPÉTENCE

21. L'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth* dispose que toute communication de données à caractère personnel par ou à la plate-forme eHealth requiert une autorisation de principe de la section Santé du Comité sectoriel de la sécurité sociale et de la santé, sauf dans quelques cas exceptionnels.

22. La communication de données à caractère personnel par ou à la plate-forme eHealth, dans le cadre du service de base 'gestion des utilisateurs et des accès', a fait l'objet d'une autorisation du Comité sectoriel par sa délibération n° 09/008 du 20 janvier 2009[7].

23. Conformément à l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, la section Santé du Comité sectoriel de la sécurité sociale et de la santé est compétente pour l'octroi d'une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé au sens 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*, dénommée ci-après : "la loi du 8 décembre 1992").

24. La communication de données à caractère personnel relatives à la santé ne doit cependant pas faire l'objet d'une autorisation lorsque la communication intervient entre professionnels des soins de santé qui sont soumis au secret professionnel et qui sont personnellement concernés par l'exécution d'actes de diagnostic, de prévention et de prestations de soins à l'égard d'un patient.

25. La communication de données à caractère personnel relatives à la santé entre le médecin de garde et le médecin généraliste du patient concerné sous la forme d'un rapport de garde ne doit par conséquent pas faire l'objet d'une autorisation du Comité sectoriel. L'examen par le Comité sectoriel se limite par conséquent au traitement de données à caractère personnel par l'application web WebWachtMailer et à la communication de données à caractère personnel – codées - relatives à la santé par cette application web à la banque de données de recherche, dans le cadre de la rédaction du rapport annuel par les coordinateurs de cercle.

26.1. Bien que la communication du rapport de garde entre le médecin de garde et le médecin généraliste ne fait pas partie de ses domaines de compétence, le Comité sectoriel attire l'attention sur le fait que tout médecin de garde doit, en toute hypothèse, tenir compte de la législation applicable relative à la légitimité de la communication du rapport de garde au médecin généraliste. A cet égard, il renvoie explicitement à la loi du 22 août 2002 relative aux droits du patient, au code de déontologie médicale de l'Ordre national des médecins et, de toute évidence, à la loi du 8 décembre 1992.

26.2. La plate-forme eHealth est finalement chargée du codage du numéro d'identification de la sécurité sociale ; à cet égard, est conservé le lien entre ce numéro et le numéro codé. Conformément à l'article 5, 8°, de la loi du 21 août 2008 realtive à l'institution et à l'organisation de la plate-forme eHealth, la plate-forme eHealth peut cependant

[7] Délibération n° 09/008 du 20 janvier 2009, modifiée le 16 mars 2010 et le 15 juin 2010, du Comité sectoriel de la sécurité sociale et de la santé relative à l'application de la gestion intégrée des utilisateurs et des accès par la plate-forme eHealth, lors de l'échange de données à caractère personnel.

conserver le lien entre le numéro d'identification réel d'une personne concernée et le numéro d'identification codé qui lui a été attribué, si le destinataire des données à caractère personnel codées en fait la demande d'une façon motivée, moyennant autorisation de la section Santé du Comité sectoriel de la sécurité sociale et de la santé.

III. TRAITEMENT

A. FINALITÉ

27. L'article 4, § 1, 1°, de la loi du 8 décembre 1992 dispose que tout traitement de données à caractère personnel doit être loyal et licite. Par ailleurs, l'article 4, § 1er, 2°, de la loi du 8 décembre 1992 n'autorise le traitement que pour des finalités déterminées, explicites et légitimes.

28. L'asbl Hermes qui intervient comme responsable du traitement a, conformément à ses statuts, pour objectif :
- initier des études relatives à la problématique de l'exercice de la profession de médecin généraliste ou y collaborer ;
- collaborer à des formations scientifiques universitaires et postuniversitaires pour médecins généralistes ;
- promouvoir la recherche scientifique par les médecins généralistes ;
- soutenir l'exercice de la profession de médecin généraliste.

29. A cet égard, l'association peut organiser tout type d'activités ou y participer dans la mesure où ces activités permettent d'atteindre les objectifs de l'asbl.

30. L'application web mise à disposition par l'asbl Hermes vise, dans un premier temps, dans le cadre des services de garde à organiser obligatoirement par les cercles de médecins généralistes[8], à rédiger un rapport de garde en ligne et à transmettre ce rapport de garde (par la voie électronique ou sur support papier) au médecin généraliste du patient concerné, d'une part, et au médecin de garde même, d'autre part.

31. Par ailleurs, l'application web a pour objectif d'enregistrer une sélection de données provenant du rapport de garde créé à l'aide de l'application web, dans une banque de données qui peut uniquement être consultée par les coordinateurs des cercles de médecins généralistes, dans le cadre du rapport annuel obligatoire au service public fédéral Santé publique.
32. Le Comité sectoriel estime par conséquent que la finalité du traitement envisagée par le demandeur est une finalité déterminée, explicite et légitime.

B. PROPORTIONNALITÉ

33. L'article 4, § 1er, de la loi du 8 décembre 1992 dispose que les données à caractère personnel traitées doivent être adéquates, pertinentes ou non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement. Par ailleurs, elles doivent être exactes et, si nécessaire, mises à jour.

[8] Section II, arrêté royal du 8 juillet 2002 fixant les missions confiées aux cercles de médecins généralistes.

Toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

34. En ce qui concerne la communication de données à caractère personnel relatives à la santé à la banque de données de recherche, le demandeur motive que les données à caractère personnel envisagées sont nécessaires à la rédaction du rapport annuel par les coordinateurs de cercle. Ces derniers doivent notamment pouvoir intégrer les éléments suivants dans le rapport:
    - région de provenance du patient (cercle de garde propre ou cercle de garde voisin);
    - pyramide d'âge par sexe;
    - nécessité réelle d'utiliser le service de garde (par groupe d'âge);
    - nombre de visites à domicile/consultations/consultations téléphoniques réparties par région du patient;
    - incidence des pathologies pour lesquelles le patient se présente, par groupe d'âge;
    - incidence des pathologies diagnostiquées par le médecin, par groupe d'âge;
    - délai d'attente du patient (temps s'écoulant entre l'appel et le contact), réparti par degré d'urgence;
    - fréquence d'utilisation du service de garde, répartie:
        - partie de la semaine du lundi ou vendredi et weekend;
        - semaine de l'année;
        - heure de la journée.

35.1. En ce qui concerne le délai de conservation des données, les données dans la banque de données de recherche sont conservées pendant dix-huit mois au maximum, à savoir le temps nécessaire à la rédaction du rapport annuel.

35.2. Le demandeur argumente que le numéro d'identification de la sécurité sociale codé doit également être enregistré dans la banque de données de recherche afin de pouvoir identifier les patients de manière unique et de pouvoir analyser sur cette base les données pathologiques et démographiques des patients qui reviennent régulièrement pendant les services de garde. Le Comité sectoriel estime qu'il est acceptable que les personnes concernées soient identifiées de manière unique – codée – pour cette finalité.

36. En conclusion, le Comité sectoriel estime que les données à caractère personnel qui sont traitées, sont adéquates, pertinentes et non excessives.

37. Pour rappel, la communication de données à caractère personnel relatives à la santé entre le médecin de garde et le médecin généraliste ne doit pas faire l'objet d'une autorisation. Néanmoins, il y a lieu d'examiner dans quelle mesure le traitement des données à caractère personnel, plus précisément l'enregistrement temporaire des rapports de garde chiffrés, par l'application web même satisfait au principe de proportionnalité.

38. Les données enregistrées par le réceptionniste, si présent, dans la liste salle d'attente ne sont conservées sur le serveur de l'application web que pendant le temps nécessaire à leur intégration dans le rapport de garde. Les données sont ensuite supprimées définitivement de la liste salle d'attente.

39.1. Le rapport de garde même est enregistré sur le serveur de l'application web. Le Comité sectoriel estime qu'il est acceptable que les rapports de garde soient conservés, pendant un an en vue de leur consultation par le médecin de garde même, respectivement pendant un mois par tout autre médecin de garde qui est en mesure de prouver qu'il a effectué une consultation du patient.

39.2. Les rapports de garde sont conservés de manière chiffrée. Le demandeur décrit la procédure comme suit :
- une clé aléatoire est d'abord créée ;
- cette clé chiffre le rapport de garde, le rapport de garde chiffré est conservé sur le serveur. Le chiffrement est réalisé à l'aide de l'algorithme AES256 ;
- la clé est envoyée au service « codage » de la plate-forme eHealth. Le service renvoie une clé codée. La clé codée est conservée sur le serveur. Cette clé codée ne permet pas de déchiffrer le rapport de garde ;
- la clé originale est détruite.

39.3. Afin de pouvoir consulter un rapport de garde pendant un service de garde, il y a lieu de satisfaire aux conditions suivantes :
- le médecin qui ouvre un rapport de garde doit être de garde conformément à la gestion des utilisateurs et des accès ;
- le médecin qui ouvre un rapport de garde doit avoir une relation thérapeutique avec l'intéressé. Ceci est contrôlé a posteriori en vérifiant qu'il a créé un rapport de garde;
- le rapport de garde ne peut pas être antérieur à un mois (les rapports de garde qui datent de plus d'un mois ne sont plus affichés dans les résultats de recherche) ;
- le patient ne peut pas avoir refusé que le rapport de garde soit réouvert par la suite (voir le point n°8).

39.4. D'un point de vue technique, le déchiffrement se déroule comme suit :
- le rapport de garde chiffré est extrait de la banque de données en même temps que sa clé codée;
- la clé codée est décodée par la plate-forme eHealth ;
- la clé décodée (= clé originale) est utilisée afin de déchiffrer (AES256) le rapport de garde et est ensuite détruite ;
- le rapport de garde déchiffré est ainsi disponible.

39.5. Le contrôle a posteriori permet de vérifier qu'un utilisateur possédait une relation thérapeutique au moment où il a ouvert un dossier d'un patient. Une relation thérapeutique est confirmée dans le cadre de cette application web au moyen de l'envoi d'un rapport de garde dans le chef du patient concerné suite à la consultation.
Le contrôle a posteriori vise à vérifier pour tout dossier d'un patient ouvert par un utilisateur, par la suite aussi par ce même utilisateur, si un rapport de garde a été envoyé pour ce patient. En ce qui concerne les utilisateurs qui ne l'auraient pas fait, le coordinateur du cercle est averti et informé de ce non-envoi.

D'un point de vue technique, tous les rapports de garde qui ne sont pas ouverts par l'auteur sont journalisés dans la « post-hoc controle database ».

Un processus batch vérifie pour chaque élément figurant dans cette « post-hoc controle database » si dans les 24 heures qui suivent, un rapport de garde a été créé pour ce

patient par le médecin de garde qui a ouvert le rapport. Si tel n'est pas le cas, le coordinateur du cercle en est averti par mail.

Ce processus batch est réalisé tous les jours ouvrables à 12 heures.

Le coordinateur du cercle est chargé d'analyser les rapports de garde ouverts irrégulièrement qui lui ont été rapportés et de les transmettre à la direction du cercle de garde de sorte qu'une sanction puisse être prise.

40. Vu ce qui précède, le Comité sectoriel estime, en ce qui concerne le traitement de données à caractère personnel dans le cadre de l'application web, que les données à caractère personnel qui sont traitées, sont adéquates, pertinentes et non excessives.

41. Les résultats des rapports annuels de garde ne peuvent pas être publiés sous une forme qui permet l'identification de la personne concernée. Les coordinateurs de cercle sont par conséquent tenus de supprimer, dans le rapport annuel, toutes les données susceptibles de donner lieu à une identification des personnes concernées.

42. Conformément à l'article 7 de la loi du 8 décembre 1992, le traitement de données à caractère personnel relatives à la santé est en principe interdit. Cette interdiction ne s'applique cependant pas, e.a.:
- lorsque le traitement est rendu obligatoire par ou en vertu d'une loi, d'un décret ou d'une ordonnance pour des motifs d'intérêt public importants, ce qui est le cas pour la rédaction du rapport de garde annuel;
- lorsque le traitement est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé, ce qui est le cas pour la rédaction et la transmission du rapport de garde au médecin généraliste;

43. En ce qui concerne la condition selon laquelle le traitement est réalisé sous la surveillance d'un professionnel des soins de santé, le Comité sectoriel prend acte du fait que le traitement de données à caractère personnel relatives à la santé dans le cadre de l'application web WebWachtMailer a lieu sous la responsabilité d'un médecin. La condition précitée est par conséquent respectée.

C. TRANSPARENCE

44. En ce qui concerne le traitement des données à caractère personnel dans le cadre de la banque de données de recherche, l'article 9 de la loi du 8 décembre 1992 prévoit une obligation d'information des personnes concernées concernant lesquelles des données à caractère personnel sont traitées.

45. Le responsable du traitement est dispensé de la communication lorsque l'enregistrement ou la communication des données à caractère personnel 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.

46. Étant donné que le traitement de données a lieu dans le cadre de la rédaction obligatoire du rapport de garde annuel, le Comité sectoriel considère que le responsable du traitement est dispensé d'informer l'intéressé.

D. MESURES DE SÉCURITÉ

47. Conformément à l'article 16 de la loi du 8 décembre 1992, le responsable du traitement de l'application web, à savoir l'asbl Hermes, 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.

48. Si le traitement est confié à un sous-traitant, le responsable doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle concernant le traitement à réaliser. Le responsable doit veiller au respect de ces mesures, à savoir en les fixant dans des dispositions contractuelles. Il doit déterminer contractuellement la responsabilité du sous-traitant vis-à-vis du responsable du traitement. Le responsable du traitement doit se mettre d'accord avec le sous-traitant - dans un écrit ou sur un support électronique – que le sous-traitant n'agit que sur la seule instruction du responsable du traitement et que le sous-traitant est tenu aux mêmes obligations que celles auxquelles le responsable du traitement est tenu en application de l'article 16, § 3, de la loi du 8 décembre 1992.

49. En ce qui concerne l'enregistrement temporaire des données de la liste salle d'attente, des rapports de garde et de la banque de données de recherche, l'asbl Hermes utilise un serveur qui est géré par l'Universitair Ziekenhuis Leuven (UZLeuven). L'asbl Hermes est par conséquent tenue, en tant que responsable du traitement, de conclure une convention écrite avec l'UZLeuven, qui reprend les éléments précités. Une copie de cette convention doit être tenue à la disposition du Comité sectoriel.

50. Le Comité sectoriel fait observer que tout un chacun qui agit sous l'autorité du responsable du traitement ou du sous-traitant ainsi que le sous-traitant même, qui a accès aux données à caractère personnel, ne peut les traiter que sur l'instruction du responsable du traitement, sauf en vertu d'une obligation prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

51. En ce qui concerne la mise en oeuvre des mesures techniques et organisationnelles adéquates, le Comité sectoriel renvoie aux mesures de références qui ont été rédigées par la Commission de la protection de la vie privée en vue de la protection de tout traitement de données à caractère personnel[9]. Il s'agit d'une liste de dix domaines d'action liées à la sécurité de l'information pour lesquels tout organisme - personne morale, entreprise ou administration - qui conserve, traite ou communique des données à caractère personnel doit prendre des mesures. Conformément à ces meures de références, l'organisme doit disposer d'une politique de sécurité écrite précisant les stratégies et les mesures retenues pour sécuriser ces données. Il y a lieu de désigner un conseiller en sécurité qui est responsable de l'exécution de la politique de sécurité.

[9] http://www.privacycommission.be/en/static/pdf/mesures-de-r-f-rence-vs-01.pdf

L'organisme doit définir clairement les responsabilités et processus de gestion en matière de sécurité des données à caractère personnel et les intégrer adéquatement dans son organisation générale et son fonctionnement. L'organisme doit prendre les mesures qui s'imposent pour garantir la protection physique des données à caractère personnel. L'organisme doit s'assurer que les réseaux auxquels sont connetés les équipements impliqués dans le traitement des données à caractère personnel garantissent la confidentialité et l'intégrité de celles-ci. L'organisme doit s'assurer que les données à caractère personnel ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation. L'organisme doit mettre en oeuvre des mécanismes de journalisation et de traçage. L'organisme doit s'assurer que les mesures de sécurité techniques ou organisationnelles sont validées et font l'objet de révisions régulières. L'organisme doit posséder un plan de gestion des incidents de sécurité. Enfin, l'organisme doit disposer d'une documentation complète et régulièrement mise à jour concernant la sécurité des informations.

52. En ce qui concerne le traitement par l'UZLeuven, le Comité sectoriel prend acte du fait que l'UZLeuven dispose également d'un conseiller en sécurité. En ce qui concerne la protection de réseaux auxquels sont connectés les équipements impliqués dans le traitement de données à caractère personnel, il est prévu qu'au travers du firewall de l'UZLeuven, seules les ports http et https seront accessibles à partir de l'Internet. Les facilités de remote access de l'UZLeuven permettent de garantir que seules les personnes autorisées puissent avoir accès à l'ensemble des ports réseau des équipements via un réseau privé virtuel (VPN). En ce qui concerne l'authentification, ces personnes doivent utiliser leur token personnel. A cet égard, l'UZLeuven garde une trace de qui établit ce type de connexion et à quel moment. Le hardware des serveurs est installé dans un centre de données qui est équipé d'installations d'extinction automatique d'incendies et de réseaux d'alimentation électrique de secours. L'accès à ce centre est réservé aux seules personnes compétentes. Le Comité prend finalement acte du fait que le personnel concerné de l'UZLeuven n'a pas accès aux données à caractère personnel contenues dans l'application web même.

53. Au niveau de l'application web même, il est prévu un système de journalisation spécifique qui enregistre quel utilisateur exécute quelle opération à quel moment.

54. En ce qui concerne l'accès aux données en fonction de leur classification, il est fait usage du service de base 'gestion des utilisateurs et des accès' de la plate-forme eHealth en vue de l'identification et de l'authentification des utilisateurs à l'aide de leur eID et en vue de la vérification de la qualité de médecin dans la banque de données fédérale des professionnels des soins de santé. L'identification et l'authentification sont suivies par une vérification à l'aide de l'Access Control List qui fixe les droits d'accès du coordinateur de cercle, des médecins de garde et des réceptionnistes. Ce n'est qu'ensuite que les personnes concernées peuvent consulter les données en question.

55. Le coordinateur de cercle gère l'accès des membres de son cercle de médecins généralistes (réception et médecin de garde) au moyen de la liste de contrôle d'accès (Access Control List). Il gère les droits d'accès: il ajoute de nouveaux utilisateurs ou les supprime si nécessaire. Il supprime également les utilisateurs à la demande du cercle de médecins généralistes, de l'asbl Hermes ou de sa propre initiative en cas d'usage illicite par l'utilisateur concerné. Toute modification de la liste de contrôle d'accès fait également l'objet d'une journalisation.

56. Seuls le réceptionniste et le médecin de garde ont accès à la liste salle d'attente de leurs patients. Le médecin de garde et le réceptionniste ont, par ailleurs, aussi accès au fichier log de leurs actions respectives. En vertu des règles décrites ci-dessus, un médecin de garde a accès aux rapports de garde. Le coordinateur de cercle a enfin accès au fichier de log des utilisateurs de son cercle et a accès à la banque de données de recherche en ce qui concerne les rapports de garde rédigés par des médecins de garde de son cercle.

57. Le Comité sectoriel constate que Hermes conclut une convention relative à l'utilisation de l'application web, tant avec tout cercle de garde (obligatoirement créé sous la forme d'une association sans but lucratif) qu'avec tout coordinateur de cercle et utilisateur. Le Comité sectoriel a reçu une copie des modèles des conventions précitées.

58. Le Comité sectoriel fait observer que conformément à l'article 458 du Code pénal, toutes les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où elles sont appelées à rendre témoignage en justice ou devant une commission d'enquête parlementaire et celui où la loi les oblige à faire connaître ces secrets, les auront révélés, seront punies d'un emprisonnement de huit jours à six mois et d'une amende de cinq cents cinquante euros à deux mille sept cents cinquante euros. Par ailleurs, conformément à l'article 6 de l'arrêté royal du 13 février 2001 *portant exécution de la loi du 8 décembre 1992*, il est interdit d'entreprendre des actions visant à convertir les données à caractère personnel codées communiquées en données à caractère personnel non codées. Il y a lieu de souligner que le non-respect de cette interdiction est assorti d'une amende variant de cent à cent mille euros en vertu de l'article 39, 1°, de la loi du 8 décembre 1992. Le Comité sectoriel fait observer que conformément à l'article 5 du Code pénal, les personnes morales peuvent également être tenues pour pénalement responsables des infractions qui sont intrinsèquement liées à la réalisation de son objet ou à la défense de ses intérêts, ou de celles dont les faits concrets démontrent qu'elles ont été commises pour son compte.

59. Finalement, tant Hermes que l'UZLeuven sont tenus de bien informer les personnes agissant sous leur autorité sur les dispositions de la loi du 8 décembre 1992 et de ses arrêtés d'exécution ainsi que sur toute prescription pertinente relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel.

60. À condition qu'elles soient appliquées de manière correcte et intégrale, le Comité estime que les mesures de sécurité précitées sont suffisantes et permettent de garantir la confidentialité et la sécurité du traitement de données à la lumière des dispositions de l'article 16 de la loi du 8 décembre 1992.

Par ces motifs,

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

autorise, aux conditions prévues dans la présente délibération, le traitement des données à caractère personnel précitées, dans le cadre de l'application web WebWachtMailer.

Le Comité sectoriel autorise la plate-forme eHealth a conservé le lien entre le numéro d'identification réel des personnes concernées et les numéros d'identification codés qui leur ont été attribués.

Yves ROGER
Président