



Avis n° 14/2008 du 2 avril 2008

Objet : avis à la demande de la Ministre des Affaires sociales et de la Santé publique et de la Ministre de la Fonction publique et des Entreprises publiques concernant un projet de loi portant institution et organisation de la plate-forme eHealth (A/2008/016)

La Commission de la protection de la vie privée ;

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* (ci-après la "LVP"), en particulier l'article 29 ;

Vu 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* (ci-après l'"A.R. du 13 février 2001") ;

Vu la demande d'avis de Madame ONKELINX, Ministre des Affaires sociales et de la Santé publique, et de Madame VERVOTTE, Ministre de la Fonction publique et des Entreprises publiques, reçue le 17/03/2008 ;

Vu le rapport du Président, Monsieur Willem DEBEUCKELAERE ;

Émet, le 02/04/2008, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1.1. Généralités

1. Le projet de loi soumis à l'avis de la Commission de la protection de la vie privée par la Ministre des Affaires sociales et de la Santé publique et la Ministre de la Fonction publique et des Entreprises publiques a d'abord pour but de créer au sein de la Banque-carrefour de la Sécurité sociale une nouvelle institution publique dotée de la personnalité juridique : la plate-forme eHealth.

2. Parallèlement à la création de la plate-forme eHealth, qui doit devenir la colonne vertébrale technique d'un échange sécurisé de données, le projet consacre également une attention particulière à la gestion organisationnelle de certains flux de données de santé. Il instaure notamment la possibilité de créer à cet effet une association sans but lucratif¹.

1.2. La plate-forme eHealth

3. La plate-forme eHealth assurera la gestion d'un réseau de services de base, auquel tous les acteurs des soins de santé seront progressivement raccordés et à l'aide duquel l'échange électronique mutuel de données à caractère personnel sera organisé, d'une manière dûment sécurisée et dans le respect de la vie privée. La plate-forme eHealth n'enregistrera pas elle-même des données à caractère personnel de contenu de façon centralisée mais permettra et stimulera par contre un échange électronique dûment sécurisé de données à caractère personnel entre tous les acteurs concernés des soins de santé².

1.2.1. Finalité

4. L'échange électronique sécurisé de données à caractère personnel via la plate-forme eHealth poursuit trois objectifs. Premièrement, il s'agit d'optimiser la qualité des soins de santé et la sécurité du patient, au moyen d'un échange électronique mutuel bien organisé de données à caractère personnel significatives relatives au patient et à son état de santé, aux soins administrés et aux résultats des soins administrés, entre les différents prestataires de soins et les établissements de soins concernés. De plus, la plate-forme eHealth contribuera à une simplification des formalités administratives pour toutes les parties concernées par les soins de santé, et ce grâce à l'instauration de processus électroniques bien organisés et à l'accès à certaines banques de données. Enfin, la plate-forme eHealth permettra également un meilleur appui de la politique des soins de santé, étant

¹ Voir page 5 de l'exposé des motifs.

² Voir pages 1 et 2 de l'exposé des motifs.

donné qu'elle peut fonctionner en tant qu'organisation intermédiaire et ainsi convertir des données à caractère personnel en données anonymes ou codées qui peuvent alors être mises à la disposition des acteurs des soins de santé, des décideurs politiques et des chercheurs³.

1.2.2. Tâches de la plate-forme eHealth⁴

5. La plate-forme eHealth a notamment pour mission de concevoir, gérer et développer au profit des acteurs des soins de santé des services électroniques, tels que d'une part, une plate-forme de collaboration pour l'échange mutuel électronique et sécurisé de données à caractère personnel et d'autre part, les services de base utiles à l'appui de cet échange électronique de données à caractère personnel. À cet égard, il faut accorder une attention particulière au système de gestion des utilisateurs et des accès (*contrôle ex ante*) et de logging (*contrôle ex post*) qu'il faut mettre en place. La plate-forme eHealth peut également, moyennant l'accord des patients concernés, tenir à jour dans ce qu'on appelle un "*répertoire des références*" quels acteurs des soins de santé conservent quels types de données à caractère personnel les concernant, sans toutefois enregistrer les données concernées elles-mêmes.

6. Une autre mission de la plate-forme eHealth consiste, en tant qu'organisation intermédiaire, à recueillir, agréger, coder ou dépersonnaliser et mettre à la disposition des données à caractère personnel utiles à la connaissance, à la conception, à la gestion et à la prestation des soins de santé. La plate-forme eHealth ne peut toutefois en principe pas enregistrer elle-même les données à caractère personnel en question.

7. Ensuite, des accords peuvent être conclus au sein de la plate-forme eHealth sur la répartition des tâches en ce qui concerne la collecte, la validation, l'enregistrement et la mise à disposition des données à caractère personnel qui seront échangées au moyen de la plate-forme de collaboration. Il ne s'agit donc pas d'un enregistrement centralisé de données à caractère personnel au sein de la plate-forme eHealth elle-même.

1.2.3. Accès au Registre national et utilisation du numéro d'identification du Registre national

8. Pour l'exécution de ses missions, la plate-forme eHealth a accès au Registre national des personnes physiques. Elle a également le droit d'utiliser le numéro d'identification de ce registre. Lors de l'échange de données à caractère personnel non codées par l'intermédiaire de la plate-forme eHealth, on utilise d'ailleurs exclusivement le numéro d'identification du Registre national des

³ Voir pages 2, 3 et 4 de l'exposé des motifs.

⁴ Voir article X+3 du projet et pages 8 à 12 de l'exposé des motifs.

personnes physiques ou le numéro d'identification attribué par la Banque-carrefour de la Sécurité sociale (ci-après appelés tous deux le "numéro d'identification de la sécurité sociale" et, en abrégé, le NISS)⁵.

1.2.4. Désignation d'un conseiller en sécurité de l'information et d'un médecin

9. En outre, la plate-forme eHealth doit désigner, parmi les membres de son personnel et après avis de la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé, aussi bien un conseiller en sécurité de l'information qu'un médecin sous la surveillance et la responsabilité duquel s'effectue le traitement de données à caractère personnel relatives à la santé⁶.

1.2.5. Autorisation du comité sectoriel

10. 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, institué au sein de la Commission de la protection de la vie privée, sauf dans quelques cas exceptionnels⁷.

1.3. Création d'une association sans but lucratif

11. Outre la création de la plate-forme eHealth, le projet de loi souhaite également offrir la possibilité à l'État – plus précisément au Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement et aux Régions et Communautés – ainsi qu'à l'Institut national d'assurance maladie-invalidité de fonder, en collaboration avec les mutualités et les associations scientifiques de prestataires de soins, une association sans but lucratif pour promouvoir la qualité de la pratique médicale par l'échange de données cliniques à caractère personnel. L'exposé des motifs⁸ du projet définit les tâches de cette ASBL comme suit :

"Cette ASBL décidera du contenu des flux de données à organiser, définira les droits d'accès des différentes parties et se prononcera sur la mise à disposition de données anonymes ou codées, dans le cadre du support stratégique ou de la recherche scientifique, tout en observant les dispositions en matière de respect de la vie privée et sous la surveillance du

⁵ Voir articles X+4 et X+5 du projet et pages 12 à 14 de l'exposé des motifs.

⁶ Voir articles X+6 et X+7 du projet et pages 14 et 15 de l'exposé des motifs.

⁷ Voir article X+8 du projet et pages 15 à 18 de l'exposé des motifs.

⁸ Pages 5 et 6 de l'exposé des motifs.

comité sectoriel compétent de la CPVP. Une large participation des représentants des différents domaines cliniques sera garantie.

L'ASBL concernée remplit par conséquent une fonction de "régisseur" et désigne, en fonction de la matière en question, un des membres de la plateforme E-health pour le développement et la mise en œuvre opérationnels des flux de données concernés. Ainsi, on assurera que seules de nouvelles configurations soient développées où cela s'avère nécessaire et on pourra assurer l'utilisation optimale des configurations existantes (par exemple Carenet).

Cette ASBL n'a bien sûr pas pour mission de procéder à une analyse des données ou de se prononcer sur la qualité des soins. L'ASBL concernée ne porte dès lors en rien préjudice aux compétences des organes existants mais comble un vide afin d'organiser des flux de données spécifiques dans le secteur des soins de santé, de manière transparente, sécurisée et non commerciale."

II. CONTEXTE DE LA DEMANDE D'AVIS

12. Le présent projet de loi comporte une révision complète de l'article 4 de la loi du 27 décembre 2006 *portant des dispositions diverses (I)* qui prévoyait la création du Service d'État "Be Health" et de l'arrêté royal du 3 mai 1999 *portant création d'une Commission "Normes en matière de télématique au service du secteur des soins de santé"*. Ces règles sont dès lors abrogées par le présent projet⁹.

13. L'institution et l'organisation de la plate-forme eHealth ont également certaines conséquences pour le Comité sectoriel de la Sécurité Sociale et de la Santé. Le projet de loi prévoit en effet une modification de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* en ce sens que les trois membres externes du Comité sectoriel de la Sécurité Sociale et de la Santé, ayant la qualité de médecin, expert en matière de gestion de données relatives à la santé, doivent être indépendants de la plate-forme eHealth, que la rédaction d'un avis juridique et technique relatif aux dossiers de la section santé du Comité sectoriel est confiée à la plate-forme eHealth, que la présidence du Comité sectoriel est dorénavant définie comme une mission à temps partiel à raison de 50 % (avec une indemnité dont le montant est égal à 50 % du traitement et autres avantages que l'intéressé recevrait s'il était conseiller auprès de la

⁹ Voir articles X+30 et X+31 du projet.

Cour d'appel) et que le fonctionnaire dirigeant de la plate-forme eHealth assiste aux réunions de la section santé avec voix consultative¹⁰.

III. EXAMEN DE LA DEMANDE D'AVIS

3.1. Considérations générales

14. La Commission souscrit à la finalité générale du projet : créer, pour l'ensemble du monde des soins de santé, une plate-forme TIC qui comble clairement une lacune et est ouverte à tous les acteurs des soins de santé.

15. Il est clair que les soins de santé sont devenus une tâche et une activité dans le cadre de laquelle de nombreux acteurs différents méritent de l'attention, une place et une contribution : les patients, les professionnels, les médecins, les associations et les instituts de soins et de prévention, les administrations et les associations de membres, les entreprises, l'enseignement et la formation, la recherche et le développement. Les flux mutuels d'informations et la gestion des informations nécessaires ont dès lors commencé depuis longtemps. Ces flux d'informations augmentent en volume, en quantité et en rapidité.

16. Les TIC constituent un élément important dans l'ensemble de ce traitement d'informations. Il est dès lors évident qu'aujourd'hui déjà, de nombreux processus sont déjà complètement ou partiellement informatisés, ou sur le point de l'être, dans le cadre de ce traitement d'informations.

17. La Commission constate que le présent projet opte pour le stockage décentralisé de données médicales électroniques. Dans un tel système, la structure documentaire existant chez les différents prestataires de soins de santé reste inchangée et chaque prestataire ou établissement de soins de santé reste également entièrement responsable (de la partie) du dossier médical qu'il a créé(e). Dans le contexte de l'échange électronique de données de santé, ce modèle est avancé par le Groupe 29¹¹ comme l'un des systèmes recommandés.

¹⁰ Voir articles X+26, X+27 et X+28 du projet ainsi que les pages 27 à 29 de l'exposé des motifs.

¹¹ "Dans le cas du modèle de stockage "décentralisé", qui ne devient un "système" que par la création de chemins de recherche correspondants, la structure de documentation des données relatives à la santé chez les prestataires de soins de santé resterait inchangée. La facilité de localisation des données d'un patient dans ce système dépend de la qualité du système de recherche.

Dans ce modèle organisationnel, le professionnel de santé/l'établissement de soins de santé reste le "responsable" du fichier (plus précisément de la partie du DME qu'il a créée). Vu l'architecture complexe de ce modèle, il pourrait se révéler nécessaire de désigner un organe central chargé de gérer et de contrôler l'ensemble du système et d'en assurer la compatibilité avec la protection des données."

18. Afin que les acteurs principaux puissent communiquer entre eux d'une manière valable et sûre, il est nécessaire d'offrir une plate-forme universelle qui permette que l'exécution de cet échange d'informations soit de qualité.

19. Outre la sécurité relative au contenu, l'exactitude et la précision, la rapidité, la fiabilité et l'actualité, l'attention consacrée à la vie privée des personnes concernées dans le cadre des soins de santé est primordiale aux yeux de la Commission de la protection de la vie privée.

20. La Commission accueille donc positivement le présent projet et souscrit à sa philosophie de base. Dans ce cadre, plusieurs éléments sont importants :

- en tant que fournisseur de services, la plate-forme eHealth est ouverte à l'ensemble des parties concernées actives dans les soins de santé ;
- la plate-forme eHealth propose, en tant que service public, un réseau d'information qui peut aussi bien représenter une alternative qu'un point de départ pour les nombreuses communications d'informations existantes ou en devenir concernant les soins de santé ;
- la plate-forme eHealth propose un service complet en tant qu'intégrateur de services dans lequel l'aspect protection de la vie privée et secret médical constitue un élément essentiel du service et représente une condition d'autorisation nécessaire ;
- la protection de la vie privée et le secret médical sont notamment garantis dans cette plate-forme par la procédure d'autorisation auprès du Comité sectoriel de la Sécurité Sociale et de la Santé
 - sous la tutelle de la Commission de la protection de la vie privée
 - dans le cadre d'un suivi permanent en interne par le conseiller en sécurité de l'information
 - ainsi que par le médecin responsable.

21. La Commission observe néanmoins que les données relatives à la santé doivent être considérées comme sensibles, non seulement au regard de la LVP, mais aussi dans la conception que s'en font les usagers des services de santé. L'efficacité d'une plate-forme d'échange de données de santé telle qu'eHealth est donc étroitement liée à la confiance placée par les usagers dans cette plate-forme,

(Voir document de travail 131 du Groupe 29 *sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, page 19.

(http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf).

Le 12 février 2008, il a été décidé au sein du sous-groupe "Medical data" du Groupe 29 de ne rien changer à ce document de travail 131, qui date déjà du 15 février 2007 et qui a entre-temps fait l'objet d'une "public consultation". Il s'agit donc d'un document officiel et définitif du Groupe 29.)

tant en ce qui concerne le respect du secret médical et de la confidentialité des données de santé, qu'en ce qui concerne la sécurité des flux de données.

22. De ce point de vue, la Commission insiste pour que le projet de loi reprenne une disposition qui stipule que le projet ne porte en rien préjudice à la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, à la loi du 22 août 2002 *relative aux droits du patient*, ni aux règles légales concernant l'exercice des professions des soins de santé.

3.2. La plate-forme eHealth en tant qu'intégrateur de services

23. La Commission constate qu'en principe, la plate-forme eHealth n'enregistre pas elle-même des données à caractère personnel¹², mais fonctionne uniquement comme une plate-forme par l'intermédiaire de laquelle l'échange électronique de données à caractère personnel sera organisé.

24. La Commission en conclut que la plate-forme eHealth est créée en tant qu'intégrateur de services et non en tant qu'intégrateur de données. Il faut donc vérifier dans quelle mesure sa création et son fonctionnement sont conformes à la LVP.

25. À l'occasion d'une discussion interne sur la problématique de l'intégration qui a eu lieu au sein de la Commission le 28 novembre 2007, un certain nombre de principes à respecter en cas d'intégration de services ont été avancés. La Commission constate que la plate-forme eHealth, telle que régie dans le projet, répond aux préoccupations de la Commission en la matière. On peut notamment souligner les points suivants :

- Loyauté, licéité et finalité

26. La plate-forme eHealth est chargée légalement d'un certain nombre de missions clairement définies, les services qui peuvent être fournis étant clairement mentionnés. Il est clairement indiqué qui sera le responsable du traitement pour la plate-forme, auprès duquel on peut exercer son droit d'accès, de rectification et de suppression.

¹² Les seules banques de données où figurent des données à caractère personnel qui seront tenues à jour par la plate-forme concernent d'une part le répertoire des références (voir les points 31 et suivants ci-dessous) et d'autre part, le logging (où il est mentionné que le docteur X a réclamé certaines données auprès du prestataire de soins Y concernant un patient Z (sans préciser quelles sont ces données)).

Par souci d'exhaustivité, on peut également faire référence ici aux données à caractère personnel que la plate-forme eHealth enregistrera dans les tableaux de concordance qu'elle tiendra à jour dans le cadre de son rôle d'organisation intermédiaire (voir les points 66 et suivants ci-dessous).

➤ Proportionnalité

27. Le champ d'action de la plate-forme eHealth est homogène et bien délimité. L'échange des données via cette plate-forme est soumis à des autorisations des comités sectoriels, ce qui constitue une garantie que l'on n'échangera pas plus de données à caractère personnel que celles qui sont pertinentes à la lumière de la finalité visée. Une répartition des tâches est prévue en matière de collecte, de validation, d'enregistrement et de mise à disposition des données qui sont échangées via la plate-forme.

➤ Précision et exactitude

28. Il est stipulé que des conventions seront établies au sujet des normes de qualité auxquelles les données doivent répondre ainsi que de la manière dont le respect de ces normes sera contrôlé.

➤ Transparence

29. La gestion de la plate-forme eHealth est confiée à un Comité de gestion au sein duquel les titulaires des données ont voix au chapitre. La création d'un Comité de concertation où les principales parties concernées sont représentées est également prévue.

➤ Sécurité

30. Un conseiller en sécurité sera spécifiquement désigné pour la plate-forme¹³. La Commission souligne la nécessité d'une politique de sécurité bien conçue et renvoie à ce sujet, à titre de référence, aux principes élaborés par la Banque-carrefour de la Sécurité sociale¹⁴. En vue de la création de systèmes performants pour la protection des données en général et de mécanismes d'identification, d'authentification et de droits d'accès en particulier, la Commission souhaite souligner dans ce contexte les lignes directrices qui sont prévues à ce sujet dans le document du Groupe 29 évoqué précédemment¹⁵.

¹³ Voir les points 78 et suivants.

¹⁴ Voir notamment les documents suivants : Politique de sécurité de l'information (http://www.bcsc.fgov.be/Fr/securete/securete_10.htm) ; Directives en matière de sécurité au niveau des institutions qui font partie du réseau géré par la Banque-carrefour de la Sécurité sociale (Banque-carrefour) ; Normes minimales de sécurité à respecter par les institutions sociales en vue de leur connexion au réseau de la Banque-carrefour de la Sécurité sociale (http://www.bcsc.fgov.be/Fr/documentation/document_2.htm)

¹⁵ Voir le document de travail 131 du Groupe 29 *sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, pp. 23-24 et 25-26 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf).

3.3. Le répertoire des références géré par la plate-forme eHealth

31. La Commission constate que la plate-forme eHealth – par analogie avec la Banque-carrefour de la Sécurité sociale¹⁶ – peut disposer d'un répertoire des références qui reprend, exclusivement pour les patients qui y consentent, chez quels acteurs des soins de santé quels types de données à caractère personnel les concernant sont conservées, sans que les données à caractère personnel de contenu elles-mêmes ne soient enregistrées dans la plate-forme eHealth. Ce répertoire des références peut alors notamment être utilisé en vue de canaliser une demande de données à caractère personnel vers l'endroit où celles-ci sont disponibles¹⁷ en vertu du répertoire des références et en vue d'un contrôle d'accès préventif¹⁸.

32. Il faut souligner que le répertoire des références de la plate-forme eHealth n'est pas une banque de données à caractère personnel contenant des données à caractère personnel de contenu. Il contient uniquement des références, par patient, relatives aux acteurs des soins de santé qui conservent un dossier concernant ce patient.

33. La Commission estime qu'un rôle important est réservé au répertoire des références de la plate-forme eHealth. Elle insiste sur le modèle décentralisé de cette plate-forme et sur la fonction du répertoire des références en tant que filtre qui doit veiller à ce que ne soient communiquées que les données à caractère personnel autorisées et à ce que ces données ne parviennent qu'au(x) bon(s) destinataire(s).

34. Ensuite, la Commission prend acte du fait qu'un patient n'est repris dans le répertoire des références de la plate-forme eHealth que s'il a donné son consentement à cet effet. Il doit s'agir d'un consentement au sens de l'article 1, § 8 de la LVP, c'est-à-dire une manifestation de volonté, libre, spécifique et informée par laquelle on accepte que des données à caractère personnel relatives à la personne concernée fassent l'objet d'un traitement.

¹⁶ Voir article 6 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.

¹⁷ Si, pour réaliser ses missions, un acteur des soins de santé a besoin de certaines données à caractère personnel déjà disponibles chez un autre acteur des soins de santé, il peut, le cas échéant, réclamer ces données à ce dernier moyennant le respect des dispositions légales et réglementaires relatives à la protection de la vie privée.

¹⁸ On peut vérifier si l'acteur des soins de santé qui demande la communication de données à caractère personnel gère effectivement un dossier concernant le patient en question.

35. La Commission souhaite souligner qu'à l'instar du Groupe 29¹⁹, elle considère l'autodétermination du patient comme essentielle. Le propre jugement du patient sur les cas où et la manière dont ses données sont utilisées doit toujours pouvoir jouer un rôle important. Obtenir le consentement du patient avant d'enregistrer ses données dans le répertoire des références est dès lors une règle qui s'inscrit tout à fait dans le cadre de cette perspective.

36. De ce point de vue, la Commission plaide également pour que, lors de l'élaboration du cadre (juridique) de la plate-forme eHealth, on prévoie de manière générale les mesures nécessaires pour que le système soit aussi suffisamment transparent sur d'autres points à l'égard du patient²⁰. Concrètement, cela implique notamment que le patient doit en principe avoir le droit de vérifier à quelles personnes/instances ses données sont transmises via la plate-forme eHealth ou qui consulte ses données²¹. À ce sujet, la Commission renvoie aux règles relatives au droit du patient quant à l'information ou à la consultation de ses données²².

37. À titre d'exemple, la Commission renvoie à cet égard à l'article 6, § 3, deuxième alinéa, 3° de la loi du 19 juillet 1991 *relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques*²³.

¹⁹ Voir document de travail 131 du Groupe 29 *sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, p. 15 à 17

(http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf).

²⁰ Voir également le document de travail 131 du Groupe 29 *sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, p. 22 et 23

(http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf).

²¹ Voir également le document de travail 131 du Groupe 29 *sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, p. 24

(http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf).

²² Voir respectivement l'article 9 de la LVP et l'article 9, § 2 de la loi du 22 août 2002 *relative aux droits du patient*.

²³ "§ 3. Le titulaire de la carte peut à tout moment demander, au moyen de cette carte ou auprès de la commune dans laquelle il est inscrit aux registres de la population, de consulter les données électroniques qui sont enregistrées sur la carte ou sont accessibles au moyen de celle-ci, et a le droit de demander la rectification de ses données à caractère personnel qui ne seraient pas reprises de manière précise, complète et exacte sur la carte.

Le titulaire de la carte a le droit de demander, au moyen de cette carte ou auprès de la commune dans laquelle il est inscrit aux registres de la population :

1° de consulter des informations le concernant qui sont reprises au registre de la population ou au Registre national des personnes physiques ;

2° de procéder à la rectification de ces données si elles ne sont pas reprises de manière précise, complète et exacte ;

3° de connaître toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consulté ou mis à jour ses données au registre de la population ou au Registre national des personnes physiques, à l'exception des autorités administratives et judiciaires chargées de la recherche et de la répression des délits (ainsi que de la Sûreté de l'Etat et du Service général du renseignement et de la sécurité des Forces armées)."

3.4. Accès au Registre national des personnes physiques et utilisation du numéro de ce registre et du numéro d'identification de la sécurité sociale

3.4.1. Numéro de Registre national ou numéro d'identification de la sécurité sociale et demande d'un identifiant sectoriel

38. Le projet de loi soumis à l'avis de la Commission prévoit que, pour exécuter ses missions, la plate-forme eHealth ait accès aux données à caractère personnel enregistrées dans le Registre national des personnes physiques et puisse également utiliser le numéro d'identification de ce registre.

39. La plate-forme eHealth peut en outre également utiliser le numéro d'identification attribué par la Banque-carrefour de la Sécurité sociale, en application de l'article 8, § 1, 2° de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*. Il s'agit d'un numéro d'identification attribué à des personnes physiques qui doivent être identifiées de manière univoque mais qui ne disposent pas (encore) d'un numéro d'identification du Registre national des personnes physiques. L'utilisation de ce numéro d'identification attribué par la Banque-carrefour de la Sécurité sociale est libre, conformément à l'article 8, § 2 de la loi précitée du 15 janvier 1990, et ne doit dès lors pas être explicitement prévue dans le présent projet de loi.

40. L'utilisation aussi bien du numéro de Registre national que du numéro d'identification de la sécurité sociale est obligatoire, selon l'article X+5 : "*Lors de la communication de données à caractère personnel non codées à ou par la plate-forme eHealth, seuls les numéros d'identification visés à l'article 8 de la loi relative à la Banque Carrefour de la sécurité sociale sont utilisés.*"

41. Le projet opte donc pour l'utilisation d'une clé d'identification unique existante lors de l'échange de données à caractère personnel via la plate-forme eHealth et non pour l'utilisation d'un numéro d'identification sectorielle spécifique pour le secteur des soins de santé.

42. Cette obligation vaut uniquement pour l'échange de données via la plate-forme. L'exposé des motifs précise que les acteurs des soins de santé "[peuvent donc] *continuer à utiliser leur propre système d'identification pour d'autres finalités (internes)*". Le projet laisse donc à l'ensemble du secteur des soins de santé la liberté d'utiliser des identifiants spécifiques.

43. Toutefois, il est assez clair que, si la plate-forme eHealth est une réussite, la "norme" choisie dans la plate-forme eHealth pour communiquer avec et sur des "personnes" deviendra également la norme générale pour l'ensemble du monde des soins de santé. Depuis 1986, c'est d'ailleurs déjà le

cas pour tous les échanges de données à caractère personnel entre les prestataires de soins de santé d'une part et l'Institut national d'assurance maladie-invalidité et les mutualités d'autre part, pour lesquels, en exécution de l'arrêté royal du 5 décembre 1986²⁴, le numéro de Registre national doit également être utilisé.

3.4.2. Le codage de données à caractère personnel – éléments en faveur du choix d'une clé d'identification unique plutôt que d'un code d'identification sectorielle spécifique

44. Il existe plusieurs méthodes pour parvenir à une protection efficace et performante de la vie privée. Grosso modo, on connaît d'une part les méthodes légales (législation et réglementation qui sont imposées par les instruments de droit) et d'autre part, les possibilités techniques (barrières matérielles et technologiques). Un système de protection aura normalement recours à ces deux modes.

45. La question se pose de savoir dans quelle mesure il est ou non utile ou nécessaire d'utiliser une identification sectorielle spécifique (plutôt qu'une identification générale comme le numéro d'identification de la sécurité sociale) lors du traitement de données à caractère personnel relatives à la santé. Une identification sectorielle spécifique consisterait alors en un code ou en un numéro qui serait déduit du numéro d'identification de la sécurité sociale et qui pourrait ou devrait uniquement être utilisé pour certains traitements ou certaines finalités. Cette identification spécifique serait alors le code spécifique pour le secteur "soins de santé", limité ou non aux traitements dans le cadre des prestations curatives, strictement médicales ou élargies à l'ensemble des traitements sur le plan médical et paramédical, ou dans le domaine de la prévention, des mutualités, des obligations de droit social, de l'administration, etc.

46. Il est évident que le choix d'un identifiant sectoriel n'est utile que lorsque les instances qui doivent s'échanger des données à caractère personnel recourent à un même identifiant lors de ces échanges et donc, qu'un même algorithme est utilisé par tous pour déduire l'identifiant sectoriel du numéro d'identification de la sécurité sociale. La définition d'un tel algorithme pourrait être assumée par la plate-forme eHealth en tant qu'élément de son ensemble de tâches. Cette spécialisation de l'identifiant pourrait en outre encore être ventilée par exemple selon le type de prestataire de soins (un médecin généraliste, un hôpital, un laboratoire, une mutualité qui attribue un numéro unique par patient). On peut encore aller plus loin en codant de manière unique chaque prestation et chaque acte médical. Techniquement, tout cela est possible.

²⁴ Arrêté royal du 5 décembre 1986 *organisant l'accès aux informations et l'usage du numéro d'identification du Registre national des personnes physiques dans le chef d'organismes qui remplissent des missions d'intérêt général dans le cadre de la législation relative à l'assurance maladie-invalidité.*

47. Il va de soi que la limitation de l'utilisation d'identifiants spécifiques à des secteurs d'application aussi restreints que possible peut rendre le "couplage" de données à caractère personnel plus difficile en dehors de ces secteurs d'application.

48. Il est toutefois tout aussi évident qu'un tel codage doit toujours être suivi d'un déchiffrement ou décodage. Il s'agit en effet (presque) toujours d'un genre de "chaîne" d'informations qui doivent être couplées les unes aux autres pour parvenir à certaines représentations, poser des actes, administrer une médication ou des soins, assurer le suivi et tenir à jour le dossier de suivi administratif. Un problème supplémentaire se pose à cet égard : il peut en effet également arriver que l'on doive pouvoir détecter non seulement la personne, mais aussi parfois certains éléments matériels comme des médicaments ou des prothèses, des implants, etc. Se pose en outre la problématique de la recherche scientifique.

49. Le décodage doit donc pouvoir se faire de manière rapide et sans erreur, et ce sans générer la moindre charge administrative. Dans cette optique, n'appliquer aucun codage (ni décodage) assurerait la plus grande certitude.

50. Le fait de travailler avec une clé d'identification unique constitue le "degré zéro" du codage : le numéro d'identification de la sécurité sociale a justement pour but d'éviter le moindre doute quant à l'identification précise d'une personne. Si notre "nom" était unique, il suffirait en tant qu'identifiant unique. Ce n'est pas le cas (et un numéro standardisé est également plus facile à utiliser dans les TIC).

3.4.3. Analyse et avis de la Commission.

51. Jusqu'à présent, la Commission a déjà souligné à plusieurs reprises la nécessité d'élaborer des numéros d'identification spécifiques à un secteur déterminé²⁵. À cet égard, elle a toujours attiré l'attention sur les dangers éventuels – notamment les couplages effrénés de données à caractère personnel – liés à un numéro d'identification qui est utilisé dans plusieurs secteurs. La Commission rappelle son inquiétude à ce sujet.

52. La Commission prend acte du fait que – contrairement à ce qui se fait dans d'autres États membres de l'Union européenne –, il n'y a pas d'enregistrement central de données dans la plate-forme eHealth. En prenant pour exemple la Banque-carrefour de la sécurité sociale, on a prévu

²⁵ Voir l'avis n° 14/2002 du 8 avril 2002, l'avis n° 19/2002 du 10 juin 2002, l'avis n° 30/2002 du 12 août 2002, l'avis n° 33/2002 du 22 août 2002, l'avis n° 10/2004 du 23 septembre 2004 et l'avis n° 01/2005 du 10 janvier 2005. Voir également notamment la délibération RN n° 20/2006 du 26 juillet 2006.

la création d'un répertoire des références qui doit permettre d'afficher à l'écran les données nécessaires par patient et ce, au moyen d'une connexion temporaire avec la base de données où sont enregistrées ces données spécifiques.

53. Un tel système ne permet pas en soi de traiter des données en créant des catégories sur la base du fait que la situation médicale de certaines personnes présente des caractéristiques communes, de rassembler toutes les données de santé relatives à une seule personne, ni d'effectuer des couplages non autorisés de données de santé avec d'autres données à caractère personnel (données sociales, fiscales, familiales, ...).

54. Comme mentionné ci-dessus, le projet opte *de facto* pour l'utilisation d'une clé d'identification unique générale : le numéro d'identification de la sécurité sociale, le cas échéant le numéro de Registre national.

55. Cette option est également fermement motivée dans l'exposé des motifs du projet : "*L'utilisation d'une clé d'identification unique offre des garanties pour une identification correcte des intéressés à chaque stade de l'échange de données à caractère personnel, c'est-à-dire tant pour l'émetteur que pour le destinataire des données à caractère personnel et pour les éventuels autres intervenants.*"²⁶

56. Un numéro d'identification spécifique pour les soins de santé ne sera, de par ce choix, pas appliqué en ce qui concerne l'échange de données à caractère personnel via la plate-forme eHealth.

57. Dans le prolongement de la jurisprudence citée, la Commission a examiné la question de savoir si l'utilisation du numéro d'identification du Registre national ou du numéro d'identification de la sécurité sociale comme identifiant unique au sein de la plate-forme eHealth était recommandée.

58. Vu qu'une identification correcte est d'une importance primordiale²⁷ d'une part, et qu'au stade actuel des choses, il n'y a pas d'argument suffisant qui s'y oppose d'autre part, il est recommandé de soutenir l'option d'un identifiant fort tel que le numéro d'identification de la sécurité sociale.

59. Un numéro de santé sectoriel général serait utilisé par un nombre si élevé de personnes qu'il n'offrirait peut-être pas une meilleure protection efficace et perceptible de la vie privée. L'utilisation

²⁶ Voir le commentaire des articles, article X+5.

²⁷ Voir également le document de travail 131 du Groupe 29 *sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, p. 16
(http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf).

d'un tel numéro sectoriel risque également de devenir une charge organisationnelle importante pour la plate-forme eHealth, ce qui pourrait donner lieu à une identification inefficace.

60. De plus, le développement d'un numéro de santé sectoriel occasionnerait également des problèmes spécifiques. Les méthodes qui entrent en ligne de compte pour l'élaboration d'un tel numéro présentent en effet d'importants inconvénients.

61. Les systèmes suivants sont envisageables en théorie : soit chaque acteur (médecin, hôpital, laboratoire médical, ...) attribue à ses patients un numéro propre (ce qui implique donc qu'un patient recevrait plusieurs numéros), soit chaque patient reçoit un seul numéro de santé et ce, au moyen d'un algorithme appliqué au numéro d'identification de la sécurité sociale²⁸. Les défauts de ces méthodes sont expliqués ci-après.

62. Dans l'hypothèse où un patient recevrait plusieurs numéros spécifiques (chez son médecin traitant, à l'hôpital, ...), il faudrait mettre au point des méthodes permettant aux systèmes informatiques des divers acteurs de toujours pouvoir identifier correctement le patient sur la base de ces différents numéros. Pour ce faire, deux solutions sont possibles :

- soit un logiciel spécial, conçu par eHealth et chargé des conversions nécessaires, est installé chez chaque acteur. Ceci impliquerait évidemment un défi organisationnel difficilement réalisable ;
- soit les conversions sont effectuées par la plate-forme eHealth, ce qui conduirait inévitablement à la constitution d'un monopole au profit de cette instance – ce qui n'est pas souhaité par le projet de loi.

63. L'hypothèse où chaque patient recevrait un seul numéro d'identification, spécifique au secteur de la santé mais utilisé par chacun au sein de ce secteur et créé par l'application d'un algorithme au numéro d'identification de la sécurité sociale, implique que cet algorithme doive être utilisé par tous les établissements de soins et tous les prestataires de soins. La Commission est consciente du fait qu'en pareil cas, la déduction du numéro d'identification spécifique au secteur de la santé est généralement possible et que l'utilisation d'un tel numéro spécifique offre à peine une protection supérieure contre un couplage illégitime de données à caractère personnel. Cette protection supplémentaire minimale ne compense donc pas le coût plus élevé et le risque d'erreurs lors de l'échange de données à caractère personnel lorsque celui-ci est permis.

64. La Commission conclut que compte tenu de tous les facteurs susmentionnés, l'instauration d'un numéro de santé sectoriel n'est pas l'instrument le plus recommandé pour garantir la protection de

²⁸ La CNIL souscrit d'ailleurs à cette dernière méthode (<http://www.cnil.fr/index.php?id=2197&print=1>).

la vie privée. Selon la Commission, l'application d'autres techniques de protection de la vie privée, comme la création d'un système dans lequel les données ne font pas l'objet d'un enregistrement centralisé et l'exigence d'une autorisation par le comité sectoriel en combinaison avec la désignation d'un médecin contrôleur (article X+7) et d'un conseiller en sécurité de l'information (article X+6), doit suffire pour pouvoir empêcher des couplages non souhaités et interdits de différents fichiers de données via la plate-forme eHealth.

65. La Commission émet donc un avis favorable pour l'utilisation du numéro de Registre national et l'accès aux données qui sont demandés, comme formulé dans les articles X+4 et X+5.

3.5. La plate-forme eHealth en tant qu'organisation intermédiaire

66. En tant qu'organisation intermédiaire, visée à l'article 1, 6° de l'A.R. du 13 février 2001, la plate-forme eHealth assure l'agrégation et le codage ou l'anonymisation de données à caractère personnel qui sont pertinentes pour des fins historiques, statistiques ou scientifiques.

67. À cet égard, la plate-forme n'enregistrera d'ailleurs en principe pas de données à caractère personnel non codées qu'elle a reçues dans le cadre de cette mission. Le résultat peut ensuite être mis à la disposition des destinataires qui le traiteront à des fins historiques, statistiques ou scientifiques, nécessaires à la connaissance, à la conception, à la gestion et à l'administration de soins de santé.

68. La Commission souhaite avant tout souligner que la notion de "*tiers de confiance*" – par opposition à l'expression "organisation intermédiaire" –, évoquée dans l'exposé des motifs, est une notion qui n'est pas définie par une loi ou un arrêté royal. Afin d'éviter une confusion, la Commission suggère dès lors de la définir ou de la supprimer du texte.

69. La Commission constate qu'avec la création de la plate-forme eHealth en tant qu'organisation intermédiaire, on répond à d'anciennes recommandations, formulées dans son avis n° 02/2007 du 17 janvier 2007.

70. D'après la Commission, des garanties doivent être prévues, lors du traitement de données à caractère personnel, pour une séparation claire et efficace des fonctions entre d'une part la collecte des données à caractère personnel et d'autre part le traitement effectif de ces données à caractère personnel.

71. L'article 11 de l'A.R. du 13 février 2001 stipule à cet égard qu'une organisation intermédiaire doit être indépendante du responsable du traitement ultérieur de données à caractère personnel.

72. Une organisation intermédiaire a en soi pour mission de regrouper, de coder ou d'anonymiser des données à caractère personnel pertinentes pour des finalités historiques, statistiques ou scientifiques et de mettre le résultat à disposition de destinataires qui traiteront ce résultat à des fins historiques, statistiques ou scientifiques.

73. En outre, elle peut le cas échéant tenir à jour des tableaux de concordance reprenant le lien entre d'une part les données à caractère personnel codées mises à disposition et d'autre part l'identité des personnes auxquelles elles se rapportent pour pouvoir mettre à disposition ultérieurement de nouvelles données à caractère personnel codées ou des données complémentaires au sujet des mêmes personnes.

74. Néanmoins, il apparaît préférable, en vue de la protection de la vie privée des personnes concernées, qu'eHealth elle-même ne conserve aucune donnée à caractère personnel, en-dehors des données d'identité.

75. De nouveaux couplages ainsi que des validations peuvent être effectués sur base des tableaux de concordance ne comportant que l'identité des personnes concernées (sur base de leur numéro de Registre national ou de leur numéro d'identification de la sécurité sociale dans ce contexte-ci), et l'identité codée de ces mêmes personnes. Cela permet ainsi d'éviter qu'eHealth ne conserve des bases de données comportant de nombreuses données à caractère personnel sensibles non codées.

76. L'intervention de l'organisation intermédiaire a pour but de garantir que les destinataires de données à caractère personnel, qui les traiteront à des fins historiques, statistiques ou scientifiques, ne disposent pas de plus de données à caractère personnel que celles strictement nécessaires pour atteindre ces finalités et n'agissent pas ainsi en contradiction avec le principe de proportionnalité. Ils ne peuvent pas être eux-mêmes en mesure de relier de nouveau des données à caractère personnel codées obtenues à une personne identifiée ou identifiable.

77. Pour que l'intervention d'une organisation intermédiaire puisse permettre une confiance justifiée des personnes au sujet desquelles des données à caractère personnel sont traitées, la Commission estime en outre que, pour éviter notamment des conflits d'intérêts, une telle organisation intermédiaire ne peut effectuer elle-même aucun travail d'analyse ou d'étude quant au contenu pour de telles finalités. C'est pourquoi le principe selon lequel la plate-forme ne conserve aucune donnée à caractère personnel en-dehors des données d'identité apparaît comme particulièrement important. La Commission renvoie à cet égard aux points 73 à 75 ci-dessus.

3.6. Désignation d'un conseiller en sécurité de l'information et d'un médecin sous la surveillance et la responsabilité duquel le traitement et l'analyse de données à caractère personnel relatives à la santé sont effectués

78. L'article X+6 du projet oblige la plate-forme eHealth à désigner un conseiller en sécurité de l'information parmi les membres de son personnel et après avis de la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé. Lors du choix de l'intéressé, il faut en particulier veiller à ce qu'il dispose de l'indépendance et de l'expertise nécessaires afin de remplir sa mission correctement.

79. Le conseiller en sécurité de l'information de la plate-forme eHealth est chargé du contrôle des traitements et des échanges de données à caractère personnel par la plate-forme eHealth. Dans ce cadre, il doit accorder une attention particulière à la protection de la vie privée des personnes auxquelles les données à caractère personnel en question se rapportent. Il formule des avis spécialisés à la personne chargée de la gestion journalière de la plate-forme eHealth et effectue d'autres tâches qui lui sont confiées par cette même personne.

80. Sur la base de l'article X+7, la plate-forme eHealth doit également désigner parmi les membres de son personnel – après avis de la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé – un médecin sous la surveillance et la responsabilité duquel tout traitement de données à caractère personnel relatives à la santé se fera via la plate-forme eHealth.

81. Il apparaît par ailleurs indispensable, pour que ce conseiller en sécurité de l'information et ce médecin responsable du traitement des données de santé puissent pleinement exercer le rôle important qui leur est dévolu, que le législateur détermine l'étendue des pouvoirs et compétences qui leur sont conférés, les conditions d'indépendance et d'autonomie dans lesquelles ces deux fonctions doivent être exercées, et l'étendue de leur responsabilité. La Commission invite donc le législateur ou à défaut, le Roi, à développer et préciser ces points. Les dispositions à adopter devraient par ailleurs être soumises à l'avis de la Commission. La Commission invite le législateur à le préciser aux articles X+6, § 3 et X+7, dernier alinéa.

82. La Commission constate qu'une mission importante est confiée à ce conseiller en sécurité de l'information et au médecin et attire l'attention sur l'avis qui doit être émis par la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé avant leur désignation.

83. Au moment d'émettre son avis, ladite section du comité sectoriel devra vérifier si le candidat concerné dispose de connaissances suffisantes concernant le réseau du secteur des soins de santé,

l'informatique et les techniques de sécurisation. Elle devra toutefois aussi vérifier si le candidat n'exerce pas d'autre activité incompatible avec sa mission de conseiller en sécurité de l'information ou de médecin et si le temps qu'il y consacre est suffisant.

3.7. Autorisation de la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé

84. En vue également de la protection de la vie privée des personnes concernées, l'article X+8 stipule que toute communication de données à caractère personnel effectuée par l'intermédiaire de la plate-forme eHealth, sauf exceptions constatées, requiert une autorisation de la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé²⁹.

85. La Commission tient à souligner à ce propos que toute disposition légale ou réglementaire qui sera promulguée à l'avenir et qui prévoit une exception à la compétence du Comité sectoriel de la Sécurité Sociale et de la Santé, devrait lui être soumise pour avis avant son entrée en vigueur³⁰. Cela permettra en effet à la Commission d'apprécier la conformité de telles dispositions avec la LVP. La Commission encourage donc l'insertion d'une disposition en ce sens dans le projet de loi.

86. Par ailleurs, en ce qui concerne l'exception à la compétence du comité prévue à l'article X+8, dernier alinéa, l'exposé des motifs précise que les données codées peuvent être mises à la disposition de divers pouvoirs publics sans autorisation du comité sectoriel, pour autant que ces données soient destinées à "la réalisation de recherches à l'appui de la politique". La Commission remarque que cette finalité n'apparaît pas dans le corps de l'article. Elle suggère donc d'ajouter dans le texte de l'article X+8 que seules les données *destinées à des recherches statistiques ou scientifiques visant à appuyer la politique de la santé*³¹ peuvent faire l'objet de cette exception.

²⁹ Pour les modalités relatives à ce comité sectoriel, on se réfère aux articles 37 à 52 inclus de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

³⁰ Voir l'article X+8 du projet. L'article 42, § 2 de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé est d'ailleurs déjà rédigé en ce sens :

"(...) 3° accorder une autorisation de principe pour 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, sauf dans les cas suivants : (...)

- si la communication est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance, après avis de la Commission de la protection de la vie privée".

³¹ Dans ce cadre, la Commission renvoie également pour information à l'arrêt de la Cour constitutionnelle n° 15/2008 du 14 février 2008. Elle renvoie aussi aux garanties prévues par la loi du 4 juillet 1962 sur la statistique publique pour des transferts de données réalisés en vue de finalités comparables.

87. Lors de l'évaluation d'un échange de données à caractère personnel, le comité sectoriel vérifiera si cet échange est conforme aux dispositions légales et réglementaires de protection de la vie privée et en particulier s'il se conforme correctement aux principes de finalité et de proportionnalité. En vertu de ces principes, des données à caractère personnel ne peuvent en effet être échangées que pour des finalités déterminées, explicites et légitimes et doivent, au regard de ces finalités, être adéquates, pertinentes et non excessives. Le comité sectoriel examinera ensuite quelles mesures de sécurité accompagnent l'échange de données à caractère personnel. Le Roi peut fixer des modalités relatives à l'octroi d'une autorisation.

88. En cas de décision favorable du comité sectoriel au sujet d'une communication de données à caractère personnel déterminée, la plate-forme eHealth doit adapter son répertoire des références afin que la communication puisse effectivement se faire.

89. La Commission prend acte du fait que l'on prévoit un système de logging pour l'échange électronique de données à caractère personnel en vue de traiter d'éventuelles plaintes ou de rechercher d'éventuelles irrégularités.

90. La Commission insiste par ailleurs une fois de plus sur la répartition fonctionnelle décentralisée des tâches quant à savoir quel acteur des soins de santé enregistre quelles données à caractère personnel dans des sources authentiques validées. Cette répartition des tâches évite une centralisation inutile, des menaces inutiles pour la protection de la vie privée et de multiples contrôles et enregistrements de loggings identiques.

91. Ensuite, conformément à l'article X+26, la Commission estime en effet recommandé, en vue de la cohérence requise, que l'avis juridique et technique relatif aux dossiers de la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé soit en principe rédigé en un seul endroit et que cette rédaction soit confiée à la plate-forme eHealth³². La Commission insiste d'ailleurs sur la mise en place rapide de la section précitée du Comité sectoriel de la Sécurité Sociale et de la Santé³³.

92. Elle souligne à cet égard le point mentionné dans son avis n° 01/2008 du 16 janvier 2008 concernant les flux de données électroniques entre différents niveaux de pouvoir. En vue d'une

³² Le président du comité sectoriel ou la plate-forme eHealth peuvent toutefois toujours recourir à l'expertise du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement, de l'INAMI, du Centre Fédéral d'Expertise des Soins de Santé et de la Fondation contre le cancer lors de la rédaction de l'avis juridique et technique.

³³ La Commission invite le Roi à prendre les mesures requises pour que la section santé du Comité sectoriel de la Sécurité Sociale et de la Santé puisse accomplir ses missions telles que définies à l'article 42 de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*.

application cohérente de la réglementation en matière de protection de la vie privée et des règles relatives à la protection des données à caractère personnel, il est en effet très important de permettre au plus vite la coordination entre les différents comités et leurs décisions. Cela se fera idéalement en concertation entre l'État fédéral, les Communautés et les Régions.

3.8. Nature des données enregistrées dans le répertoire des références et des données échangées via la plate-forme eHealth

93. La Commission remarque qu'il est prévu à l'article X+10 que les données échangées par l'intermédiaire d'eHealth soient considérées comme faisant foi jusqu'à preuve du contraire, c'est-à-dire qu'elles bénéficient d'une présomption d'exactitude. Elle comprend qu'une telle présomption puisse éventuellement être accordée aux données enregistrées dans le répertoire des références mais pas aux données échangées via la plate-forme eHealth.

94. Il paraît en effet imprudent de faire bénéficier d'une telle présomption des données extrêmement nombreuses, et pour lesquelles il n'existe aucune garantie de qualité. Il ne faut pas oublier que les données qui bénéficient de ce genre de présomption, comme celles du Registre national, sont des données protégées par des procédures d'enregistrement spéciales (constatation par un officier d'État civil, etc.). Ce n'est pas le cas des données qui transiteront par eHealth. Il paraît donc injustifié et dangereux pour les personnes concernées de leur attribuer une présomption d'exactitude. Cette présomption irait par ailleurs directement à l'encontre des droits de rectification et de suppression prévus par la LVP.

95. La Commission propose dès lors de remplacer la présente disposition – à condition que la plate-forme eHealth prévoie à cet effet les garanties de sécurité nécessaires – par une disposition qui stipule que les données échangées via la plate-forme eHealth ont la même force probante que les données échangées sur un support papier. La Commission souligne que la plate-forme eHealth est censée garantir l'intégrité de la transmission des données.

3.9. Avis complémentaire de la Commission

96. La Commission souligne qu'il serait souhaitable que les arrêtés à prendre par le Roi concernant la sécurité, le soient après avis de sa part (article X+11, deuxième alinéa).

3.10. Création d'une association sans but lucratif

97. La Commission souhaite avant tout souligner que, tant dans l'exposé des motifs que dans le texte de la loi, les mots "dépersonnalisation des données" devraient être remplacés par "anonymisation des données" (article X+34, *in fine*). En effet, la notion de "données dépersonnalisées" ne figure nulle part dans la LVP et n'est à ce titre pas définie en soi.

98. La Commission prend acte du fait que le projet de loi prévoit la possibilité d'association réciproque entre certains acteurs³⁴ afin de promouvoir la qualité de la pratique médicale et de stimuler la coopération réciproque en matière d'organisation de la plate-forme eHealth.

99. La Commission constate que, dans l'exposé des motifs du projet, il est fait référence à plusieurs reprises à l'importance du respect de la législation relative à la protection de la vie privée³⁵. Sur la base de cet exposé, elle constate également que cette association est placée sous le contrôle du Comité sectoriel de la Sécurité Sociale et de la Santé³⁶. Néanmoins, la Commission formule le souhait que le texte légal précise que les missions de cette association ne portent en rien préjudice aux compétences du comité sectoriel en vue d'autoriser les communications de données relatives à la santé.

3.11. Ambiguïtés et imprécisions dans le texte du présent projet de loi

100. La Commission signale que la notion d' "acteurs des soins de santé" (article X+3, 4°) n'est pas définie dans le projet. En vue de créer, au sein du grand public, la confiance nécessaire dans la plate-forme eHealth, il est souhaitable que cette notion vague soit définie.

101. La Commission souhaite également souligner une autre imprécision dans le texte du présent projet. D'une part, l'article X du projet donne l'impression que toute législation valable pour la Banque-carrefour de la Sécurité sociale s'applique également à la plate-forme eHealth. D'autre part, on pourrait déduire de l'article X+14 du projet que la législation concernant la Banque-carrefour ne s'applique qu'aux aspects que le projet indique en tant que tels. La Commission insiste pour que soient apportés des éclaircissements à ce sujet.

³⁴ Il s'agit plus précisément de l'État (le Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement et les Communautés et Régions), l'Institut national d'assurance maladie-invalidité, les mutualités et les associations scientifiques de prestataires de soins (article X+33 du projet).

³⁵ Voir les deuxième et quatrième alinéas à la p. 5 de l'exposé des motifs.

³⁶ Voir le quatrième alinéa à la p. 5 de l'exposé des motifs.

102. La Commission estime également que l'article X+29, dans sa formulation actuelle, donne l'impression que le Roi reçoit de très grandes compétences pour modifier certaines règles. Après concertation avec les auteurs du projet de loi, il s'avère qu'en rédigeant cette disposition, ils avaient uniquement pour but d'offrir au Roi la possibilité d'entreprendre des démarches afin que toutes les procédures existantes qui s'effectuent encore actuellement sur papier soient à l'avenir exécutées par voie électronique. La Commission insiste pour que le projet de loi soit dès lors adapté en ce sens. Elle souhaite également souligner que le Roi, en vertu de sa compétence de modification prévue à l'article X+29, ne peut pas prendre d'initiatives qui pourraient avoir une influence sur le texte du présent projet de loi, sur les principes de la LVP, sur l'A.R. du 13 février 2001 ou sur la loi du 22 août 2002 *relative aux droits du patient*.

103. Enfin, la Commission fait remarquer que l'article X+20 stipule que les personnes qui, en raison de leurs fonctions, participent à la collecte, au traitement ou à la communication de données à caractère personnel par la plate-forme eHealth ou ont connaissance de telles données, sont tenues d'en respecter le *caractère confidentiel*. La Commission constate que cette disposition s'inspire clairement de l'article 28 de la loi du 15 janvier 1990³⁷. Elle souhaite toutefois attirer l'attention sur le fait que la LVP – qui est entrée en vigueur deux ans plus tard – stipule que le professionnel des soins de santé et ses préposés ou mandataires sont soumis au *secret* lorsqu'ils participent au traitement de données à caractère personnel relatives à la santé³⁸. Elle suggère dès lors que le projet de loi fasse référence au devoir de secret au sens de l'article 7, § 4, *in fine* de la LVP.

3.12. Remarques finales

104. La Commission tient à souligner que la mise sur pied de la plate-forme eHealth en vue de permettre le transit sécurisé des données relatives à la santé ne porte en rien préjudice à l'applicabilité des diverses dispositions légales et réglementaires relatives au traitement des données de santé (article 7 de la LVP et articles 25 à 27 de l'A.R. du 13 février 2001 portant exécution de la LVP notamment), ou relatives aux modalités d'exercice des professions de soins de santé (*secret professionnel, etc.*).

105. Il en découle notamment que le consentement écrit des personnes concernées à l'introduction de leurs données à caractère personnel dans un traitement informatisé devra toujours être demandé en l'absence d'une autre base légitimant le traitement de ces données.

³⁷ Loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.

³⁸ Article 7, § 4, *in fine* de la LVP.

IV. CONCLUSION

106. La Commission est positive à l'égard de ce projet de loi portant institution et organisation de la plate-forme eHealth. Néanmoins, elle souhaite attirer l'attention sur les remarques formulées ci-avant :

- a. il faut prévoir une règle générale qui stipule que le projet ne porte en rien préjudice à la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, à la loi du 22 août 2002 *relative aux droits du patient*, ni aux règles légales concernant l'exercice des professions des soins de santé (point 22) ;
- b. il faut prévoir les mesures nécessaires afin que le patient puisse toujours savoir qui a accédé à ses données et à quel moment (points 36 et 37) ;
- c. l'expression "*trusted third party*" doit être définie ou remplacée par l'expression "organisation intermédiaire" (point 68) ;
- d. il convient de prévoir qu'eHealth remplira sa mission en tant qu'organisation intermédiaire sur base de tableaux de concordance ne reprenant que des données d'identité codées et non codées (points 73 à 77) ;
- e. les pouvoirs, les compétences, l'indépendance et la responsabilité du conseiller en sécurité de l'information et du médecin responsable du traitement doivent être déterminés avec précision et les arrêtés royaux qui seront adoptés dans ce cadre doivent être soumis à l'avis de la Commission (point 81) ;
- f. il convient de prévoir que toute nouvelle disposition prévoyant une exception à la compétence du Comité sectoriel de la Sécurité Sociale et de la Santé devra être soumise à l'avis de la Commission de la protection de la vie privée (point 85) ;
- g. il convient d'ajouter à l'article X+8 que seules les finalités de recherche statistique ou scientifique font l'objet de cette exception et de déterminer les garanties accompagnant cette exception (point 86) ;
- h. la règle en matière de renversement de la charge de la preuve concernant l'exactitude des données transitant par eHealth devrait être revue (point 95) ;
- i. les arrêtés qui doivent être pris en exécution de l'article X+11, deuxième alinéa en matière de sécurité doivent être soumis à l'avis de la Commission (point 96) ;
- j. remplacer le mot "dépersonnalisation" par "anonymisation" (point 97) ;
- k. préciser que les missions de l'association sans but lucratif à créer ne portent pas préjudice aux compétences du Comité sectoriel de la Sécurité Sociale et de la Santé (point 99) ;
- l. définir la notion d' "acteurs des soins de santé" (point 100) ;
- m. clarifier et préciser les cas dans lesquels la loi du 15 janvier 1990 sur la Banque-carrefour de la sécurité sociale s'applique (point 101) ;

n. l'article X+29, qui semble octroyer de très grandes compétences au Roi, doit être revu (point 102) ;

o. l'article X+20 doit faire référence au devoir de secret (point 103).

PAR CES MOTIFS,

107. Sous réserve des remarques formulées ci-avant, la Commission émet un avis positif quant au présent projet de loi portant institution et organisation de la plate-forme eHealth.

Pour L'Administrateur e.c.,
Le Chef de section OMR

Le Président,

(sé) Patrick Van Wouwe

(sé) Willem Debeuckelaere