Comité sectoriel de la Sécurité sociale et de la Santé

CSSS/10/081

DÉLIBÉRATION N° 09/008 DU 20 JANVIER 2009, MODIFIEE LE 16 MARS 2010 ET LE 15 JUIN 2010, 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

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

Vu le rapport d'auditorat de la plate-forme eHealth du 9 décembre 2008;

Vu le rapport de monsieur Yves Roger.

1. OBJET DE LA DEMANDE

1.1. La plate-forme eHealth est une institution publique dotée de la personnalité juridique, créée par la loi du 21 août 2008, qui entend notamment promouvoir et soutenir un échange électronique et sécurisé de données à caractère personnel entre les acteurs des soins de santé (médecins, hôpitaux, pharmaciens, patients, …), tout en respectant l'intégrité de la vie privée des intéressés.

La plate-forme eHealth offre notamment plusieurs services de base qui peuvent être utilisés par tous les acteurs des soins de santé.

C'est ainsi que la plate-forme eHealth gère un site portail propre, qui fournit, d'une part, des renseignements relatifs à l'organisation, aux missions et au fonctionnement de la plate-forme eHealth et qui offre, d'autre part, un accès sécurisé à certains services électroniques, tels que par exemple EuthaConsult (une application qui permet aux médecins de vérifier, pour un patient donné, si une déclaration anticipée en matière d'euthanasie a été effectuée et enregistrée auprès

d'une commune), Registre du cancer (une application visant à la simplification et à la standardisation de l'enregistrement des cas de cancer) ou eCare-SAFE (une application qui permet d'enregistrer des données administratives à caractère personnel et des données à caractère personnel relatives à la santé dans le cadre du traitement de la polyarthrite rhumatoïde).

La plate-forme eHealth peut, par ailleurs, être chargée de l'application de la gestion intégrée des utilisateurs et des accès qui permet de garantir que seuls les prestataires de soins/organismes de soins expressément autorisés aient accès à certaines données à caractère personnel.

1.2. Les services électroniques qui sont offerts à l'intervention de la plate-forme eHealth, comprennent souvent l'échange de données à caractère personnel entre les parties concernées. Cela ne signifie pas pour autant que les données à caractère personnel en question sont toujours échangées à l'intervention de la plate-forme eHealth même. En effet, le rôle de la plate-forme eHealth, lors d'un échange de données à caractère personnel relatives à la santé dans le cadre de services électroniques, se limite souvent à la simple application de la gestion intégrée des utilisateurs et des accès, à l'occasion de laquelle elle vérifie que la personne qui utilise l'application est effectivement autorisée à le faire. À l'issue de cette vérification, les données à caractère personnel relatives à la santé sont directement échangées (moyennant l'application des mesures de sécurité utiles) entre les parties concernées (sans passage réel par la plate-forme eHealth en tant qu'institution publique dotée de la personnalité juridique).

En ce qui concerne la gestion des utilisateurs et des accès dans le secteur public, la Commission de la protection de la vie privée a formulé une recommandation (recommandation n°01/2008 du 24 september 2008). La Commission de la protection de la vie privée observe qu'un système fiable de gestion des utilisateurs et des accès détermine quel utilisateur peut avoir accès, en quelle qualité et dans quelles circonstances, à quels types de données à caractère personnel relatives à quelles personnes et à quelle période.

La *gestion des utilisateurs* comprend les aspects suivants : l'identification de l'utilisateur, l'authentification de l'identité de l'utilisateur, l'enregistrement de ses caractéristiques et mandats pertinents et la vérification de ces caractéristiques et mandats. Lors de l'utilisation d'une application, il sera donc vérifié qui est l'utilisateur (identification), s'il est bien celui qu'il prétend être (authentification) et s'il possède les caractéristiques et mandats utiles (vérification).

La *gestion des accès* comprend les aspects suivants : l'enregistrement des autorisations et la vérification des autorisations. Lors de l'utilisation d'une application, il sera donc vérifié si l'utilisateur, dont l'identité a été constatée et authentifiée sur base de ses caractéristiques et mandats, peut avoir accès à certaines données à caractère personnel.

En vue de l'enregistrement et de la vérification des caractéristiques, mandats et autorisations, il est fait appel à des banques de données à caractère personnel authentiques validées (voir infra, 2.6.).

1.3. Lorsque l'utilisateur d'une application qui est offerte à l'intervention de la plate-forme eHealth, s'annonce – en fonction du cas, à l'aide de sa carte d'identité électronique ou à l'aide d'une combinaison d'un userid, d'un mot de passe et éventuellement d'un token (la Commission de la protection de la vie privée estime par ailleurs dans sa recommandation précitée que l'usage de la carte d'identité électronique offre le plus de garanties), il est dans un premier temps procédé à l'identification de l'utilisateur et à l'authentification de son identité.

1.4. Il sera par ailleurs vérifié quelles sont les caractéristiques pertinentes et quels sont les mandats pertinents dont dispose, le cas échéant, l'utilisateur concerné.

La plate-forme eHealth vérifiera donc si l'utilisateur même ou la personne (soit une personne physique, soit une personne morale) au nom et pour le compte de laquelle l'utilisateur intervient, dispose effectivement des caractéristiques requises (qualité, qualification professionnelle, …) en vue de recevoir l'accès à l'application en question.

Afin de vérifier qu'un utilisateur (ou la personne au nom et pour le compte de laquelle il intervient) possède effectivement la caractéristique qu'il prétend posséder (ou dont il prétend que la personne au nom et pour le compte de laquelle il agit, la possède) en vue de pouvoir utiliser une application, la plate-forme eHealth fera appel à certaines banques de données à caractère personnel, notamment à la banque de données des professionnels des soins de santé et à la banque de données des agréations accordées par l'Institut national d'assurance maladie et invalidité.

Il s'agit invariablement de banques de données à caractère personnel dans laquelle il est indiqué, par personne enregistrée, qu'elle possède une certaine qualité, qualification professionnelle, …, par exemple « *professionnel des soins de santé* » ou « *agréé par l'Institut national d'assurance maladie et invalidité* ».

Étant donné que l'accès aux services électroniques à l'intervention de la plate-forme eHealth est réservé à des personnes présentant des caractéristiques déterminées, une consultation de ces banques de données s'avère nécessaire en vue d'une protection d'accès adéquate.

1.5. Les mandats sont des droits octroyés par un utilisateur identifié à un autre utilisateur identifié afin qu'il puisse effectuer des actions déterminées en son nom et pour son compte. En effet, un utilisateur n'interviendra pas toujours en son propre nom et pour son propre compte.

Afin de vérifier qu'un utilisateur possède réellement le mandat qu'il prétend posséder en vue de pouvoir utiliser une application, la plate-forme eHealth vérifiera

les rapports qui existent entre les entités (soit des personnes physiques, soit des personnes morales), notamment dans la banque de données UMOE ("*User Management Ondernemingen Entreprises*") (ce qui permet par exemple de constater qu'un utilisateur agit en tant que collaborateur administratif d'un hôpital), dans la banque de données PUHMA ("*Public Health Mandates*") (ce qui permet par exemple de constater que l'utilisateur agit pour le compte d'un infirmier ou d'un regroupement d'infirmiers) et dans la banque de données
REMAPH ("*Responsability Management Public Health*") (ce qui permet de déterminer les relations entre certaines personnes morales, certaines personnes physiques et certaines fonctions non officielles).

La plate-forme eHealth utilise à cette fin le numéro d'identification de la sécurité sociale de l'utilisateur (le NISS), soit le numéro d'identification du Registre national, soit le numéro d'identification attribué par la Banque Carrefour de la sécurité sociale en application de l'article 4 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.* En vertu de l'article 7 de la loi du 21 août 2008, la plate-forme eHealth a, pour l'exécution de ses missions, le droit d'utiliser le numéro d'identification du Registre national. L'usage du numéro d'identification attribué par la Banque Carrefour de la sécurité sociale est libre.

1.6. Dès réussite de la procédure de gestion des utilisateurs décrite ci-dessus, la plate-forme eHealth peut passer au processus de gestion des accès.

Elle vérifiera plus précisément, à l'aide de règles d'accès définies à l'avance, si un type d'utilisateur donné peut accéder à l'application en question et communiquera au gestionnaire de l'application qu'un utilisateur donné peut recevoir accès à cette application. A cette fin, plusieurs données à caractère personnel relatives à l'utilisateur seront aussi communiquées à l'application, plus précisément son identification, le cas échéant, l'identification de la personne (soit personne physique, soit personne morale) au nom et pour le compte de laquelle l'utilisateur agit ainsi que plusieurs données à caractère personnel supplémentaires provenant des banques de données à caractère personnel authentiques, en fonction des besoins de l'application.

L'échange de données à caractère personnel qui suit, peut intervenir ou non à l'intervention de la plate-forme eHealth. Les parties concernées prévoiront cependant souvent un échange de données à caractère personnel mutuel direct, sans que la plate-forme eHealth n'intervienne ultérieurement comme institution publique dotée de la personnalité juridique.

1.7. Ce qui précède peut s'illustrer grâce à l'application Orthopride, décrite dans la délibération n° 08/48 du 2 septembre 2008 du comité sectoriel de la sécurité sociale et de la santé.
Orthopride ("*Orthopedic Prosthesis Identification Data Electronic Registry*") comprend une application, accessible via la plate-forme eHealth, permettant aux

orthopédistes agréés des hôpitaux de mettre à la disposition des données à caractère personnel relatives au placement de prothèses du genou et de la hanche, en vue de la création d'un « registre belge des remplacements articulaires » qui serait consultable par tous les orthopédistes agréés.

Lorsqu'un patient se présente dans un hôpital et qu'il fournit plusieurs données d'identification de base à l'orthopédiste traitant, celui-ci peut, moyennant l'utilisation obligatoire de sa carte d'identité électronique, se connecter à la plate-forme eHealth qui est chargée de son identification, de l'authentification de son identité et de la vérification de ses caractéristiques et mandats.

La plate-forme eHealth aura, à cette fin, notamment recours à la banque de données à caractère personnel des professionnels des soins de santé (l'intéressé est-il orthopédiste ?) et à la banque de données à caractère personnel des agréations accordées par l'Institut national d'assurance maladie et invalidité (l'orthopédiste concerné est-il agréé en tant que tel par l'Institut national d'assurance maladie et invalidité ?).

Dès réussite de ce processus, la plate-forme eHealth vérifiera, sur la base de règles d'accès définies à l'avance, si l'utilisateur concerné peut accéder à Orthopride. Si tel est le cas, le droit d'accès dans le chef de l'intéressé ainsi que plusieurs données à caractère personnel le concernant seront communiqués à l'application.

L'échange de données à caractère personnel proprement dit qui suit, intervient directement entre les orthopédistes agréés et le gestionnaire d'Orthopride. La plate-forme eHealth en tant qu'institution publique dotée de la personnalité juridique n'intervient plus ultérieurement dans cet échange.

1.8. Afin d'améliorer la performance de la gestion intégrée des utilisateurs et des accès, il est prévu un service web spécifique appelé Mazda (Medical Authorizations Data Access).

Ce service web poursuit quatre objectifs:

- Il permet, premièrement, de scinder la fonction de vérification d'accès à l'application à la vérification d'accès aux données. En effet, certaines applications, par exemple l'enregistrement du cancer, e-care safe, e-care Orthopride, Vesta,… utilisent certaines informations provenant de REMAPH et/ou PUHMA afin d'octroyer l'accès aux données.

  Ceci peut s'illustrer grâce à l'application de l'enregistrement du cancer : un administratif peut être sous la responsabilité d'un Médecin Spécialiste ou d'un Coordinateur Oncologique. S'il est mentionné sous la responsabilité d'un Médecin Spécialiste dans la source authentique REMAPH, il ne pourra que gérer les dossiers de ce dernier. Précédemment, cette information était directement fournie lors de la vérification de l'accès à l'application. Via le

webservice Mazda, l'application pourra appeler eHealth, après que le processus de la vérification d'accès à l'application soit terminé afin de récupérer les informations sur les droits d'accès aux données. Une autre méthode du webservice Mazda permet également de vérifier et de transmettre les informations provenant de la source authentique PUHMA. L'application peut fournir le NISS du mandataire, éventuellement un identifiant d'une organisation et le mandat. Il recevra en retour la liste des mandats (NISS des mandants, nom, prénom, date de validité des mandats). Une dernière méthode permet également de vérifier la qualité d'une personne et d'une organisation. Par exemple, l'application de l'enregistrement du cancer consultera cette méthode pour vérifier si le Médecin Spécialiste sélectionné lors de la recherche des relations de subordination avec le personnel administratif, possède, au moment de la consultation encore l'ensemble de ces qualités.

- Le webservice Mazda permet, deuxièmement, de fournir des informations complémentaires utiles pour la convivialité au sein des applications à savoir la dénomination ou la plaque adresse d'un établissement de soin qui sera affichée au sein de l'application.

- Le webservice Mazda permet, troisièmement, de fournir des informations sur la qualité d'une personne ou d'une organisation. Par exemple, l'application « Public Search » de la BCE fera appel au webservice Mazda afin de vérifier les différentes qualités de soins de santé qu'un NISS d'un professionnel de la santé possède.

- En outre, le webservice Mazda permet de récupérer et vérifier les relations docteur / patient au niveau du dossier médical global (DMG). Sur base des informations en leur possession, les applications pourront utiliser les variantes que le webservice Mazda met à disposition. Par exemple, si l'application possède le Niss du docteur et le Niss du patient, le webservice retournera si la relation existe ou non au moment de la consultation. Si l'application possède uniquement le NISS des docteurs, le webservice fournira la liste des patients ayant un DMG chez eux.

- Enfin, le service web Mazda prévoit, dans le cadre de la gestion des utilisateurs et des accès d'une application spécifique, la possibilité de coupler certains utilisateurs à certains dossiers qui ont été créés dans le cadre de l'application.

  Dans le cadre de la gestion intégrée des utilisateurs et des accès, les profils des utilisateurs sont gérés dans la banque de données REMAPH, certaines fonctions (p.ex. administratives) peuvent être assignées à certaines personnes au sein d'une institution et il est possible d'établir des liens entre les personnes qui travaillent pour une même institution. Le chargement de ces données est réalisé par les différentes institutions concernées. Afin de coupler par la suite des utilisateurs à des dossiers déterminés dans une application, l'application en question peut demander l'affichage des données qui ont été chargées dans

REMAPH via la fonctionnalité de Mazda. Ces données s'affichent pour les personnes autorisées qui peuvent finalement coupler certains utilisateurs à certains dossiers.

Ceci peut être illustré à l'aide d'un exemple. L'application Begeleiding IN Cijfers est un système d'enregistrement en ligne qui permet à des structures locales d'aide spéciale à la jeunesse de gérer les dossiers des jeunes qui leur ont été confiés, de manière uniforme et à un niveau centralisé. Dans une première phase de cette application, il était prévu que tout assistant social qui était connu en tant qu'utilisateur dans la gestion des utilisateurs et des accès de la plate-forme eHealth pour cette application avait automatiquement accès à l'ensemble des dossiers de sa structure d'aide spéciale à la jeunesse. En faisant appel à l'application Mazda, le responsable de l'enregistrement de toute structure d'aide spéciale à la jeunesse peut demander une liste de tous les utilisateurs au sein de son institution et déterminer quel assistant social peut avoir accès à quel dossier. Les droits d'accès par assistant social peuvent ainsi être limités aux dossiers dans lesquels cet assistant social intervient effectivement.

Cette fonctionnalité de Mazda peut également être utilisée pour communiquer des informations provenant de la gestion des utilisateurs et des accès de la plate-forme eHealth dans le cadre du fonctionnement de l'application même. On peut citer à titre d'exemple l'application Qermid@Pacemakers. L'application Qermid@Pacemakers organise l'enregistrement de données individuelles de nature matérielle relatives aux pacemakers. Seuls les cardiologues ayant un code de spécialisation déterminé peuvent se voir accorder l'accès à l'application par les gestionnaires locaux de l'application. Un enregistrement d'un pacemaker doit cependant être signé par deux cardiologues travaillant au sein d'un même hôpital. Le cardiologue qui crée l'enregistrement devra désigner un deuxième cardiologue qui devra cosigner l'enregistrement. Grâce au service web Mazda, il sera créée, à partir de la banque de données REMAPH, une liste de cardiologues qui travaillent dans l'hôpital du cardiologue qui crée l'enregistrement, celle-ci sera communiquée au premier cardiologue qui pourra sélectionner un deuxième cardiologue qui sera ensuite enregistré sous cette qualité.

1.9. En vertu de l'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*, toute communication de données à caractère personnel, à l'intervention de la plate-forme eHealth ou au départ du site portail de la plate-forme eHealth, requiert une autorisation de principe préalable de la section Santé du comité sectoriel de la sécurité sociale et de la santé, sauf dans quelques cas exceptionnels.

Cependant, ni l'article 11 de la loi du 21 août 2008, ni les textes parlementaires préparatoires à ce sujet précisent ce qu'il y a lieu d'entendre par « *communication de données à caractère personnel par ou à la plate-forme eHealth* ».

Il y a par conséquent lieu de supposer que l'échange de données à caractère personnel dans le cadre d'un service électronique où le rôle de la plate-forme eHealth en tant qu'institution publique dotée de la personnalité juridique se limite à l'application de la gestion intégrée des utilisateurs et des accès requiert aussi une autorisation préalable du comité sectoriel de la sécurité sociale et de la santé.

1.10. Vu ce qui précède, il paraît opportun de prévoir une délibération qui autorise la plate-forme eHealth, de manière générale, lors de l'échange de données à caractère personnel, à se charger de l'application de la gestion intégrée des utilisateurs et des accès.

Une telle autorisation à portée générale de la section Santé du comité sectoriel de la sécurité sociale et de la santé ne porterait, par ailleurs, nullement préjudice aux compétences respectives des différents comités sectoriels créés au sein de la Commission de la protection de la vie privée en ce qui concerne l'octroi d'une autorisation pour l'échange de données à caractère personnel dans certains cas déterminés.

Cela signifie que chaque fois que la plate-forme eHealth est chargée de l'application de la gestion intégrée des utilisateurs et des accès (qui ferait donc dorénavant l'objet d'une autorisation générale), il y a aussi lieu de vérifier à titre complémentaire s'il n'est pas question d'un échange de données à caractère personnel complémentaires qui n'est pas strictement nécessaire à la gestion intégrée des utilisateurs et des accès et qui doit faire l'objet d'une autorisation préalable d'un comité sectoriel. Cet échange de données ne peut, le cas échéant, avoir lieu que pour autant que l'autorisation requise ait été donnée à cette fin.

2. EXAMEN DE LA DEMANDE

2.1. L'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth* dispose qu'en principe, 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.

La présente demande porte uniquement sur l'application, par la plate-forme eHealth, de la gestion des utilisateurs (identification de l'utilisateur, authentification de son identité et vérification de ses caractéristiques et mandats) et de la gestion des accès (vérification des autorisations) décrites ci-dessus, le webservice Mazda inclus, dans le cadre de services électroniques offerts à l'intervention de la plate-forme eHealth ou directement par le gestionnaire du service (une application ne doit pas nécessairement être accessible via la plate-forme eHealth, mais peut aussi directement être mise à la disposition, par exemple par le biais d'un site web ou d'un service web) et sur l'échange de données à caractère personnel relatives à l'identité, aux caractéristiques, aux mandats et aux autorisations qui sont nécessaires à cette fin.

2.2. La section Santé du comité sectoriel de la sécurité sociale et de la santé est priée de prévoir une autorisation à portée générale pour l'application de la gestion intégrée des utilisateurs et des accès par la plate-forme eHealth et pour l'échange de données à caractère personnel relatives à l'identité, aux caractéristiques, aux mandats et aux autorisations qui sont nécessaires à cette fin.

2.3. Lors de l'application de la gestion intégrée des utilisateurs et des accès, la plate-forme eHealth fait appel aux services du service public fédéral Technologie de l'information et de la communication, qui assure l'identification de l'utilisateur et l'authentification de son identité pour la plate-forme eHealth.

Le service public fédéral Technologie de l'information et de la communication a été autorisé par la Commission de la protection de la vie privée *loco* le Comité sectoriel du Registre national, par sa délibération n°26/2005 du 6 juillet 2005, à accéder au Registre national et à utiliser le numéro d'identification du Registre national, afin de se charger de régler la gestion des utilisateurs.

A cette occasion, il a déjà été prévu que le service public fédéral Technologie de l'information et de la communication mettrait son système de gestion des utilisateurs à la disposition d'autres institutions publiques belges, notamment, qui ont besoin d'une gestion des utilisateurs sûre, en vue de l'accomplissement de leurs tâches d'intérêt général.

2.4. Les caractéristiques de l'utilisateur ou de la personne au nom et pour le compte de laquelle l'utilisateur agit, seront vérifiées dans les banques de données à caractère personnel, telles la banque de données à caractère personnel des professionnels des soins de santé et la banque de données à caractère personnel des agréations accordées par l'Institut national d'assurance maladie et invalidité.

En ce qui concerne la recherche des mandats de l'utilisateur également, la plate-forme eHealth consultera diverses banques de données à caractère personnel, telles que les banques de données à caractère personnel UMOE, PUHMA et REMARPH décrites ci-dessus. Ces banques de données à caractère personnel constituent plutôt des banques de données administratives et contiennent uniquement des informations relatives aux rapports éventuels entre des personnes (soit des personnes physiques, soit des personnes morales).

La consultation des banques de données à caractère personnel contenant des caractéristiques et des mandats répond à des finalités légitimes, à savoir vérifier si une caractéristique déterminée qui est nécessaire à l'utilisation d'une application appartient réellement à l'utilisateur même ou à la personne au nom et pour le compte de laquelle il agit (à cet effet, il y a nécessairement lieu d'examiner les qualités, les qualifications professionnelles, … des parties concernées) et vérifier si l'utilisateur possède effectivement le mandat qu'il prétend posséder en vue de

pouvoir utiliser une application (à cet effet, il y a nécessairement lieu d'examiner les rapports entre les parties concernées).
La consultation se limite toujours à la simple indication du fait que les intéressés possédaient, au moment de l'utilisation de l'application, les caractéristiques et mandats utiles et satisfait par conséquent au principe de proportionnalité.

Conformément à l'article 7 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth* et à l'article 8 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, la plate-forme eHealth peut utiliser le numéro d'identification de la sécurité sociale lors de la consultation de ces banques de données.

2.5. Le comité sectoriel souligne que cette autorisation générale ne porte nullement préjudice aux compétences des différents comités sectoriels créés au sein de la Commission de la protection de la vie privée et qu'il y a par conséquent lieu de vérifier que l'application de la gestion intégrée des utilisateurs et des accès par la plate-forme eHealth ne s'accompagne pas d'un échange de données à caractère personnel qui n'entre pas spécifiquement dans le cadre de l'application de la gestion intégrée des utilisateurs et des accès et qui doit faire l'objet d'une autorisation préalable d'un comité sectoriel.

2.6. Le comité sectoriel de la sécurité sociale et de la santé constate que la plate-forme eHealth, en vue de l'application de la gestion intégrée des utilisateurs et des accès, fera appel aux banques de données à caractère personnel suivantes:

- la banque de données à caractère personnel des agréations accordées par l'Institut national d'assurance maladie et invalidité;
- la banque de données à caractère personnel des professionnels des soins de santé;
- le fichier central des établissements de soins ("*Centrale Instellingen / Institutions Centralisées*", CIC);
- la banque de données à caractère personnel UMOE;
- la banque de données à caractère personnel PUHMA;
- la banque de données à caractère personnel REMAPH;
- la banque de données à caractère personnel de la Vlaams Agentschap voor Jongerenwelzijn contenant la liste des personnes qui peuvent accéder à l'application RPV ("*Registratie Private Voorzieningen*") (collaborateurs du Vlaams Agentschap voor Jongerenwelziijn, la structure d'appui Bijzondere Jeugdzorg et les établissements privés agréés d'aide spéciale à la jeunesse).

Une brève description de ces banques de données à caractère personnel, dans leur état actuel, est jointe en annexe 1 de la présente délibération. Lors de l'évolution de ces banques de données à caractère personnel, la plate-forme eHealth publiera les informations actualisées nécessaires (www.ehealth.fgov.be).
Dès qu'il est fait appel à des banques de données à caractère personnel supplémentaires, il y a lieu d'en informer le comité sectoriel, en vue de l'adaptation

de la présente délibération, plus précisément en vue de compléter l'énumération des banques de données à caractère personnel donnée à l'alinéa précédent. Le comité sectoriel doit donc, à tout moment, pouvoir disposer d'une liste actualisée et exhaustive des banques de données à caractère personnel concernées.

2.7. Le comité sectoriel de la sécurité sociale et de la santé constate par ailleurs que la plate-forme eHealth est déjà, aux conditions de la présente délibération, chargée de l'application de la gestion intégrée des utilisateurs et des accès pour les applications suivantes : eCare-SAFE, eCare-Orthopride, EuthaConsult, Vesta, eTCT et Registre du cancer.

Pour les applications suivantes également, qui ne sont cependant pas encore en production à l'heure actuelle, la plate-forme eHealth sera chargée d'appliquer la gestion intégrée des utilisateurs et des accès : BelRAI, Facturation Tiers Payant, Assurabilité, Medega, eBirth, eCare-Implants, ICE-SEC et ONP.

Une brève description de ces applications, dans leur état actuel, est jointe en annexe 2 de la présente délibération. Lors de l'évolution de ces banques de données à caractère personnel, la plate-forme eHealth publiera les informations actualisées nécessaires (www.ehealth.fgov.be).

Par ces motifs,

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

accorde, aux conditions précitées, l'autorisation en vue, d'une part, de 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 et, en vue de l'échange de données à caractère personnel y nécessaires relatives à l'identité, aux caractéristiques, aux mandats et aux autorisations des parties concernées.

Yves ROGER
Président

ANNEXE 1
BANQUES DE DONNÉES À CARACTÈRE PERSONNEL VISÉES AU POINT 2.6.

la banque de données à caractère personnel des agréations accordées par l'Institut national d'assurance maladie et invalidité (INAMI)

L'INAMI organise, gère et contrôle les assurances obligatoires en matière de soins de santé et indemnités en Belgique. Pour réaliser cette mission, l'INAMI dispose des données de toutes les personnes et institutions pouvant dispenser des soins et remplissant les conditions de remboursement par l'assurance maladie. La plate-forme eHealth peut utiliser la banque de données à caractère personnel en question afin de contrôler si une personne déterminée est reconnue en tant que professionnel des soins de santé (médecin, infirmier, …), si une institution déterminée a été agréée et afin de prendre connaissance des données d'adresse de cette institution.

la banque de données des professionnels des soins de santé

Cette banque de données fédérale (aussi appelée "*cadastre*") contient une liste des professionnels des soins de santé. La plate-forme eHealth utilise ce cadastre pour vérifier les qualités et les compétences des professionnels de la santé, autrement dit s'ils possèdent un diplôme spécifique dans le domaine des soins de santé et s'ils ont des compétences ou des titres particuliers (spécialisation dans un domaine médical: radiologie, cardiologie,…).

le fichier central des établissements de soins ("*Centrale Instellingen / Institutions Centralisées*", CIC)

Le but du projet CIC est de créer une banque de données centralisée des institutions de soins en Belgique qui contiendra les données descriptives relatives aux institutions, leurs coordonnées, leurs dénominations exactes et les descriptions détaillées de l'encadrement des activités de soins.

la banque de données à caractère personnel UMOE

Les données s'y trouvant permettent de définir quelle personne a reçu quel droit d'accès à quelle application au nom de quelle organisation. L'introduction des données est gérée par les différentes organisations concernées.

la banque de données à caractère personnel PUHMA

La banque de données à caractère personnel PUHMA ("*Public Health Mandates*") contient les relations entre les personnes et/ou les institutions. Pour certaines applications, une personne ou une institution qui a accès à cette application peut conférer un mandat à une autre personne ou institution (prestataire de soins). Ce mandataire/prestataire de soins peut alors utiliser une application au nom et à la place du mandant.

la banque de données à caractère personnel REMAPH

Cette base de données permet de gérer les profils des utilisateurs, d'assigner certaines personnes à certaines fonctions au sein d'un organisme (par exemple: administratif) et de créer des liens entre les personnes travaillant pour un même organisme. L'introduction des données est gérée par les différentes organisations concernées.

la banque de données à caractère personnel RPV

Il s'agit de la banque de données de la Vlaams Agentschap voor Jongerenwelzijn qui est utilisée afin de déterminer les utilisateurs de l'application RPV ("*Registratie Private Voorzieningen*"): collaborateurs du Vlaams Agentschap voor Jongerenwelzijn, de la structure d'appui Bijzondere Jeugdzorg et des établissements privés agréés d'aide spéciale à la jeunesse. La gestion de cette banque de données est entièrement entre les mains de la Vlaams Agentschap.

ANNEXE 2
APPLICATIONS VISÉES AU POINT 2.7.

eCare-SAFE	Cette application vise notamment à créer un registre des patients atteints d'une polyarthrite rhumatoïde et à le rendre consultable.
eCare-Orthopride	Cette application vise à créer un registre belge des prothèses de la hanche et des genoux (enregistrement de données à caractère personnel relatives à leur placement) et à le rendre consultable par des orthopédistes.
EuthaConsult	Cette application intervient dans le cadre de l'application de l'arrêté royal du 27 avril 2007 réglant la façon dont la déclaration anticipée en matière d'euthanasie est enregistrée et est communiquée aux médecins concernés. Toute personne ayant la qualité de médecin pourra consulter si une déclaration en la matière a été effectuée et enregistrée auprès d'une commune.
Vesta	Vesta est un système électronique d'échange de données entre la Vlaams Agentschap voor Zorg & Gezondheid et les services d'aide familiale. Ce système sert à la collecte des données nécessaires pour les subsides aux services d'aide familiale. Cette application permet également de partager des données à caractère personnel relatives à un utilisateur avec, dans un premier temps, d'autres services d'aide familiale qui fournissent une aide au même utilisateur. Ainsi est constitué un seul dossier de soin par utilisateur, tenu à jour.
eTCT	eTCT ("*Technische Cel/Cellule Technique*") est une banque de données contenant les données en matière de consommation médicale des hôpitaux, qui offre notamment un aperçu du coût des traitements médicaux et des frais remboursés par l'assurance maladie.
Enregistrement du cancer	L'enregistrement du cancer constitue la base pour une étude épidémiologique. Cette application vise à une simplification et à une standardisation de l'enregistrement des cas de cancer et permet également un contrôle de la qualité des données en mode en ligne. Les programmes de soins de base en oncologie trouveront ici un outil pour répondre aux normes de qualité de l'enregistrement obligatoire du cancer prescrites par l'arrêté royal du 21 mars 2003.
BelRAI	Cette application a pour but de permettre aux différents prestataires de soins de créer, de remplir ou de modifier les questionnaires d'évaluation RAI ("*Resident Assessment Instrument*") pour un patient.
Facturation Tiers Payant	Cette application permet aux infirmiers et aux groupements d'infirmiers de transmettre des factures tiers payant aux mutualités.
Assurabilité	Cette application permet aux infirmiers et aux groupements d'infirmiers de demander les données d'assurabilité de leurs patients.
MEDEGA	Cette application est chargée de la gestion électronique de services de garde de médecins et de dentistes.

eBirth	Cette application vise à optimaliser les échanges de données à caractère personnel entre l'ensemble des acteurs impliqués par le traitement des déclarations de naissance initiées par les prestataires de soins qui pratiquent les accouchements.
eCare-Implants	Cette application vise à alimenter et à consulter le registre des implants cardiaques.
ICE-SEC	L'application ICE-SEC offre une interface de communication sur les expériences entre donneurs d'ordre, comités éthiques et les autorités compétentes.
RPV	L'application "*Registratie Private Voorzieningen*" (RPV), développée à la demande du Vlaams Agentschap voor Jongerenwelzijn et de la structure d'appui Bijzondere Jeugdzorg, vise à un enregistrement uniforme des dossiers des établissements privés agréés d'aide spéciale à la jeunesse, et ce grâce à la création d'une application web qui leur permet de gérer leurs dossiers dans une banque de données à caractère personnel centrale.