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

CSI/CSSS/20/102

**DÉLIBÉRATION N° 15/009 DU 17 FÉVRIER 2015, DERNIÈREMENT MODIFIÉE LE 3 MARS 2020, RELATIVE À LA MÉTHODE GÉNÉRIQUE D'ÉCHANGE DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES ET NON PSEUDONYMISÉES RELATIVES À LA SANTÉ, DANS LE CADRE DE HEALTHDATA.BE ET HEALTHSTAT.BE**

La chambre sécurité sociale et santé du Comité de sécurité de l'information (dénommée ci-après « le Comité de sécurité de l'information »);

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (Règlement Général sur la Protection des Données ou RGPD);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;*

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

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, en particulier l'article 97 ;

Vu la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, en particulier l'article 42, § 2, 3°, modifié par la loi du 5 septembre 2018 ;

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 37 ;

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

Vu l'autorisation n° 15/009 du 17 février 2015, dernièrement modifiée le 5 juin 2018;

Vu la demande de modification de la délibération ;

Vu les rapports d'auditorat de la Plate-forme eHealth;

Vu le rapport de monsieur Bart Viaene.

Émet, après délibération, la décision suivante, le 3 mars 2020.

## I. OBJET DE LA DEMANDE

**1.** Le Plan d'action eSanté 2013-2018, qui a été actualisé en 2015 sous la forme du Plan d'action eSanté 2015-2018[1], a inscrit parmi les priorités à réaliser l'inventarisation et la consolidation des registres de données à caractère personnel relatives à la santé (point d'action 18). Sciensano, anciennement l'Institut scientifique de santé publique (WIV-ISP[2]), a été chargé de la coordination et de l'exécution de ce point d'action.

**2.** Afin de concrétiser l'inventorisation et la consolidation de l'ensemble des registres belges relatifs à la santé et aux soins de santé, le service healthdata.be a été créé au sein de Sciensano. Les objectifs sont les suivants :

- faciliter l'enregistrement de données relatives à la santé et aux soins de santé en Belgique, grâce à la mise en œuvre de processus simples,
- assurer la collecte et la diffusion efficaces et sûres de données issues de banques de données scientifiques.

**3.** Sciensano a élaboré une architecture de base qui permet de réaliser la collecte et la mise à la disposition de données à caractère personnel codées relatives à la santé. Cette structure s'appelle healthdata.be (pour la collecte) et healthstat.be (pour la mise à la disposition).

**4.** Sciensano soumet maintenant à l'approbation du Comité de sécurité de l'information la demande de mise en œuvre de la méthode générique décrite ci-après en vue de la collecte, de la gestion et de la communication de données à caractère personnel relatives à la santé. Après avis positif du Comité directeur de la plate-forme Healthdata.be, des demandes spécifiques à un projet visant à obtenir l'autorisation pour la communication de données à caractère personnel sont introduites auprès du Comité de sécurité de l'information.

**5.** Le Comité directeur se compose du chef de projet de healthdata.be, de médecins indépendants (cliniciens), de médecins hommes de science, de médecins des organismes assureurs, d'experts en informatique médicale et de représentants des

[1] http://www.plan-esante.be/

[2] Depuis le 1er avril 2018, l'Institut scientifique de Santé publique (ISP) et le Centre d'Étude et de Recherches Vétérinaires et Agrochimiques (CERVA) ont fusionné pour créer le nouveau centre fédéral de recherche Sciensano (Loi du 25 février 2018 portant création de Sciensano et arrêté royal du 28 mars 2018 *portant exécution de la loi du 25 février 2018 portant création de Sciensano, en ce qui concerne le siège social, la gestion et le fonctionnement, ainsi que l'adaptation de divers arrêtés concernant les prédécesseurs légaux de Sciensano*).

organisations de patients ainsi que de représentants de l'INAMI, du SPF Santé publique, du KCE et de la Plate-forme eHealth.

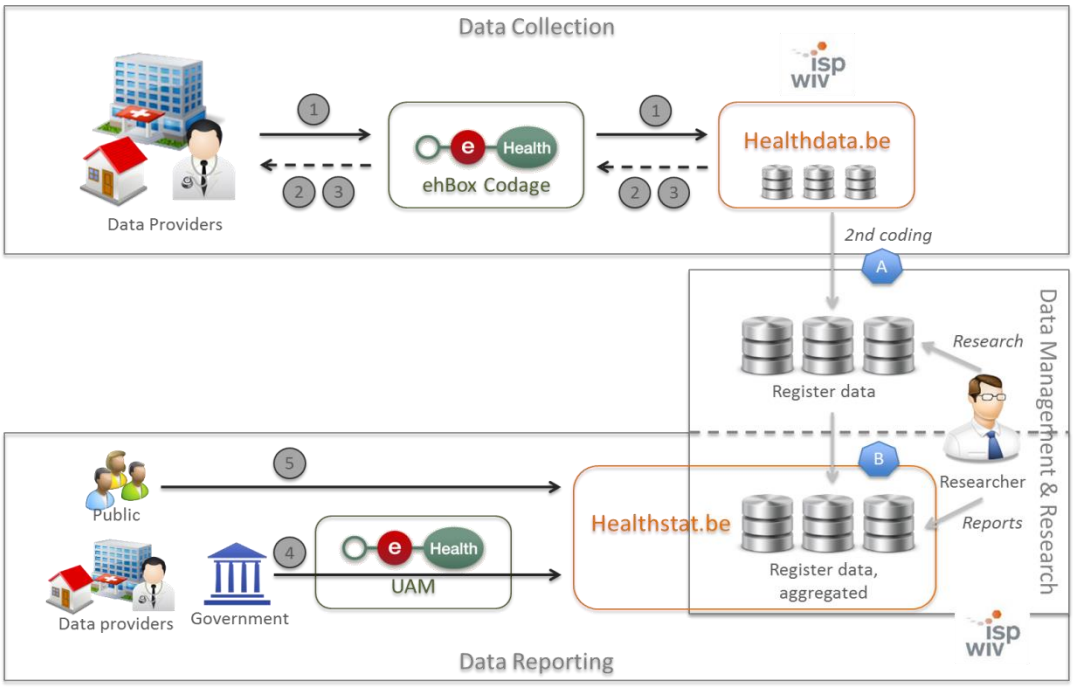
**6.** Les missions du Comité directeur qui sont les suivantes, ont été reprises dans un accord de collaboration entre l'INAMI et Sciensano :

- surveiller le respect par eHealthdata.be des principes et actions décrits dans le Plan d'action eSanté 2013-2018;
- déterminer les procédures et les critères pour la création de nouveaux registres et la maintenance de registres existants;
- l'évaluation de la recevabilité et de la priorité des nouveaux projets qui sont présentés et qui peuvent être réalisés par Healthdata.be;
- la rédaction d'Objectifs Service Level;
- l'établissement d'une liste de contrôle qui permet de suivre des Objectifs Service Level;
- l'approbation du projet de budget et du compte annuel des recettes et des dépenses.

**7.** L'objectif consiste à convertir durant la période 2014-2018, en 3 phases, les 42 registres de l'INAMI et de Sciensano en fonction de la nouvelle méthode de collecte de données et de publication via healthdata.be des résultats pour les besoins de groupes cibles spécifiques. Une vague s'étend sur environ 18 mois, dont 12 mois d'analyse fonctionnelle et de développement technique et 6 mois d'accompagnement lors de la mise en production. Le Comité de sécurité de l'information a reçu la liste complète des registres pour ces trois phases.

**8.** Dans l'architecture initialement créée par Sciensano et utilisée au cours de la période de 2015 à 2017, les flux de données se déroulaient comme suit (voir figure 1).

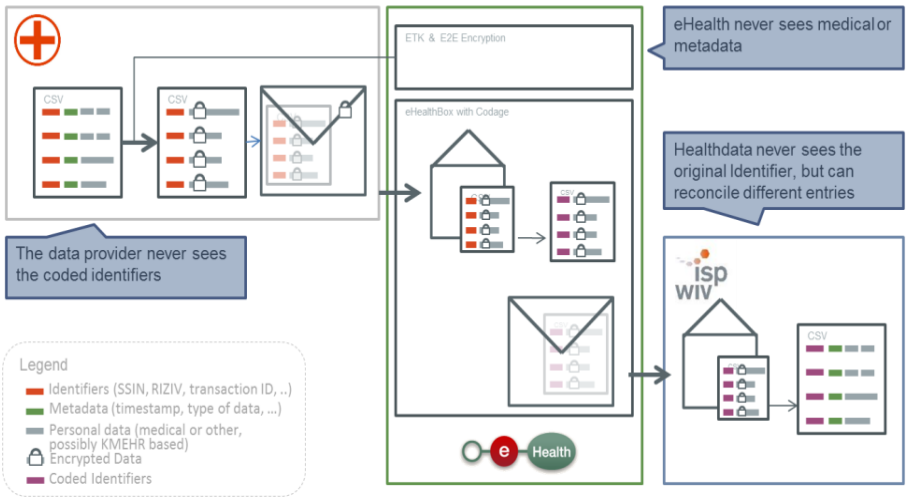
**Figuur 1: Algemeen overzicht gegevensstromen**




**9.** Collecte des données: Les fournisseurs de données collectent les données pour les registres spécifiques. Ces données sont, dans la mesure du possible, introduites directement dans les systèmes propres (tels EPD, HIMS, LIMS). Ces données sont ensuite mises à la disposition pour être envoyées à healthdata.be via le eHealthBox (eHBox) codage (envoi automatique via la boîte aux lettres électronique sécurisée de la Plate-forme eHealth au service de base de la Plate-forme eHealth). Cela peut se faire soit directement (développement propre), soit en utilisant un composant logiciel offert (HD4DP) qui est exécuté et géré localement, la plateforme healthdata.be n'ayant pas accès aux données à caractère personnel nominatives. HD4DP n'offrira pas le chiffrement des données médicales/scientifiques et leur envoi via le eHBox comme faisant partie du composant logiciel offert. La documentation utile sera offerte de sorte que ces fonctions puissent être développées par les fournisseurs de données (ou par une tierce partie désignée par elle).

**10.** *Etape 1*: le fournisseur des données envoie les données au eHBox codage. La Plate-forme eHealth se charge de la pseudonymisation du NISS du sujet des données (patient dont les données sont collectées) ainsi que de plusieurs autres données. A cet effet, un même algorithme est utilisé pour tous les projets qui sont opérationnalisés dans le cadre du projet healthdata.be. Les données médicales/scientifiques sont chiffrées vis-à-vis de healthdata.be. Les données sont ensuite transmises via le eHBox à la plateforme healthdata.be. Un eHBox spécifique (sur la base d'un numéro EHP) sera attribué à cet effet à healthdata.be. Voir la figure 2 pour une représentation schématique de l'échange de données via eHBox, en ce compris la pseudonymisation et le chiffrement.

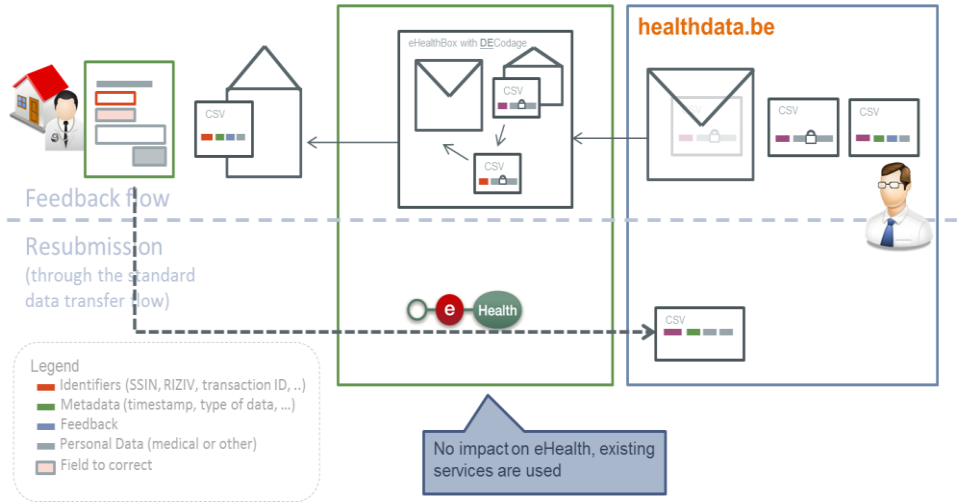
Figuur 2: Gegevensuitwisseling via ehBox Codage (incl. codering & encryptie)




**11.** *Etape 2*: suite à la réception des données par healthdata.be, une confirmation automatique est envoyée au fournisseur des données.

**12.** *Etape 3*: après contrôle et validation des données par le chercheur du registre, ce dernier a la possibilité de poser des questions supplémentaires au fournisseur des données, dans le but de faire corriger des erreurs dans les données. A cet effet, healthdata.be renvoie un message au fournisseur des données via eHBox codage. Celui-ci reprend les données pseudonymisées ainsi que les données médicales / scientifiques qui sont chiffrées par rapport au fournisseur des données. La Plate-forme eHealth se charge de la pseudonymisation du code d'identification des patients et fournit les données au fournisseur des données. Le renvoi à healthdata.be des données corrigées se déroule comme précisé à l'étape 1. Voir la figure 3 pour le détail de cet échange de données via eHBox.

Figuur 3: Terugsturen van gegevens (voor feedback / correctie) naar de data provider

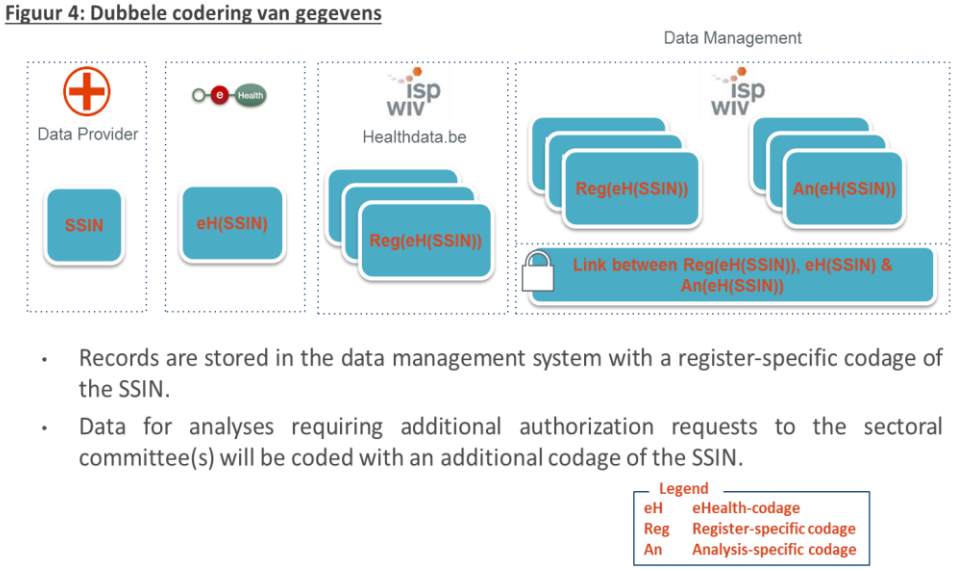


**13.** Certains registres existants ont déjà recours à une pseudonymisation du NISS via la Plate-forme eHealth. L'algorithme utilisé pour la pseudonymisation est par ailleurs différent du nouvel algorithme de healthdata.be. Afin de permettre une étude longitudinale des données existantes/historiques et des données nouvellement collectées, une repseudonymisation unique du NISS devra être réalisée pour les registres en question. Ceci sera précisé dans la demande d'autorisation spécifique par registre conformément à la procédure générale fixée en collaboration avec la Plate-forme eHealth.

**14.** Data Management et Research: Sur base des données fournies, les chercheurs du registre réalisent leurs travaux (examen et rédaction de rapports qui sont mis à la disposition du public et de groupes cibles spécifiques). A cet effet, ils reçoivent uniquement accès aux données du registre qui leur a été attribué.

**15.** *Etape A*: avant que les chercheurs puissent obtenir accès aux données individuelles du registre qui leur a été attribué, les données à caractère personnel (NISS) qui ont été pseudonymisées par la Plate-forme eHealth, sont codées une deuxième fois. Ce 2e codage est spécifique au registre et permet d'éviter que les chercheurs ne puissent établir de rapports entre les données des différents registres. Le codage spécifique au registre est réalisé au moyen d'un algorithme qui est géré et exécuté par healthdata.be. Si pour une analyse déterminée, les autorisations requises ont été obtenues afin d'établir des rapports entre les données des différents registres, un codage spécifique à l'analyse est réalisé par healthdata.be. Ce codage spécifique à l'analyse est aussi réalisé au moyen d'un algorithme qui est géré et exécuté par healthdata.be. Voir la figure 4 pour une représentation schématique de ce schéma de codage.

**Figuur 4: Dubbele codering van gegevens**




**16.** *Etape B*: préalablement à la mise à la disposition de rapports ou de publications du public et de groupes cibles spécifiques (tels que les fournisseurs de données, les promoteurs des registres, etc.) via l'application web sécurisée healthstat.be, des *data marts* spécifiques sont mis au point. Ceux-ci contiennent uniquement des données

agrégées au niveau d'agrégation adéquat et concernant lesquelles des rapports sont disponibles.

**17.** Data Reporting: Healthstat.be permet de partager des rapports scientifiques, des diagrammes et des figures avec le monde extérieur. Ce partage est réalisé au moyen d'une application web sécurisée.

**18.** *Etape 4:* les groupes cibles spécifiques (fournisseurs de données, promoteurs, administrations, etc.) ont, après authentification via l'UAM de la Plate-forme eHealth, accès aux rapports personnels qui ont été établis.

**19.** En ce qui concerne la gestion des utilisateurs et des accès (UAM), il y a lieu de distinguer les groupes d'utilisateurs suivants:
- utilisateurs individuels: citoyens, médecins;
- utilisateurs au sein d'une organisation comprenant initialement au moins les (types d') organisations suivantes: hôpitaux, laboratoires, centres de soins de santé mentale, Sciensano et healthdata.be, les pouvoirs publics tels que l'INAMI, le SPF Santé publique et les autorités régionales.

**20.** Par utilisateur, il y a lieu de communiquer les informations suivantes à healthstat.be via l'UAM: nom, langue, NISS, numéro INAMI (si disponible), qualités (médecin, dentiste, etc.) et les données relatives aux organisations (n° ID et nom). En ce qui concerne les utilisateurs au sein d'une organisation, il y a lieu de configurer un rôle au sein de l'UAM: utilisateur standard et ou gestionnaire healthstat.be.

**21.** Afin de pouvoir attribuer les droits nécessaires aux utilisateurs au sein de healthstat.be, le numéro d'identification de l'utilisateur (NISS et/ou n° INAMI) sera utilisé. Ces droits spécifiques pourront être attribués via healthstat.be aux utilisateurs d'une organisation par un utilisateur ayant un rôle de gestionnaire. Pour l'enregistrement de ces règles d'autorisation, si le NISS est utilisé, celui-ci fera l'objet d'un hachage.

**22.** *Etape 5*: des données d'un niveau fortement agrégé peuvent, si cela est souhaitable pour un registre, être offertes au grand public sans authentification.

**23.** Sciensano souhaite, à partir de 2017, également mettre l'architecture de base qu'il a développée à la disposition pour la communication de données à caractère personnel non pseudonymisées. Il renvoie à cet effet à la convention de collaboration qui décrit la mission de healthdata.be comme suit : « la facilitation technique, axée sur les processus, de l'échange de données dans le secteur des soins de santé belge selon le principe d'une collecte unique et multifonctionnelle des données et du réemploi des données pour permettre aux acteurs des soins de santé d'augmenter les connaissances de la santé de la population et d'ajuster la gestion des soins de santé, dans le respect de la protection de la vie privée du patient, du dispensateur de soins et du secret médical. ».

**24.** La mission permettant de faciliter la collecte unique et multifonctionnelle de données et la réutilisation de données a été formulée comme suit dans le plan d'action eSanté actualisé : « Accords, architecture et planning pour les collectes de données d'appui politique à des fins multiples (MyCarenet, hubs & coffres-forts, registre national des implants, etc.) ». Sciensano souligne par cette formulation que la collecte de données en vue d'un usage multidisciplinaire (et pas uniquement dans un contexte de recherche) était envisagée depuis le début, mais qu'elle sera aussi effectivement appliquée à partir de 2017, par exemple dans le cadre des enregistrements Qermid. A cet égard, il y a également lieu d'appliquer les principes du « only once ». Par ailleurs, le succès de l'approche d'intégration de healthdata.be auprès des utilisateurs finaux constitue l'occasion pour les fournisseurs de données et le monde politique d'inciter healthdata à aussi soutenir d'autres collectes de données (p.ex. pour la Fondation Registre du cancer, AFMPS, …).

**25.** Afin de faciliter ce type de collectes de données à usage multidisciplinaire, Sciensano a prévu une architecture adaptée qui permet :

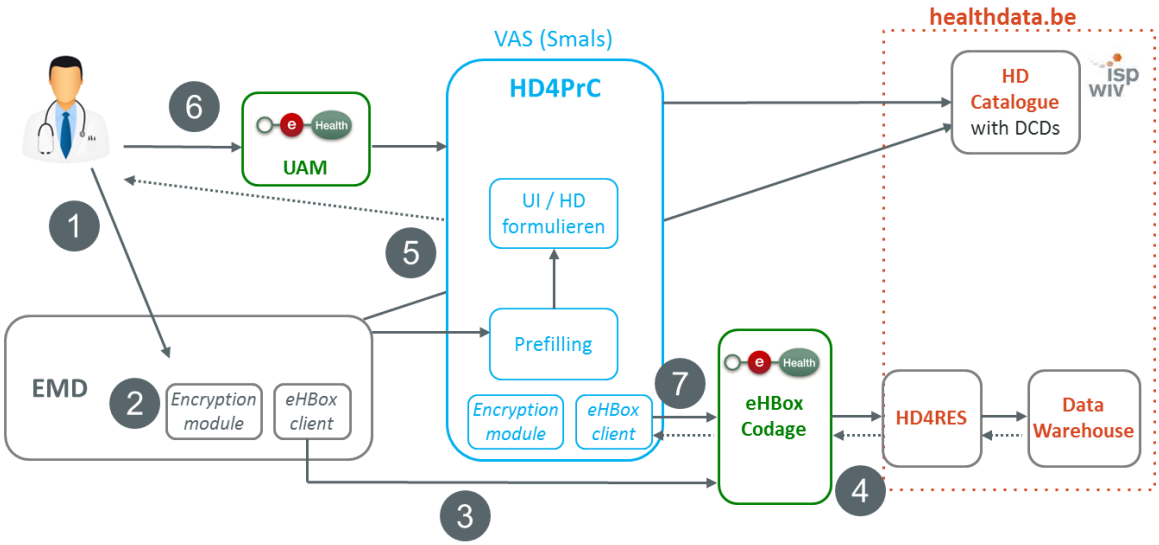
- de collecter les données de manière unique, si possible en harmonie avec l'architecture healthdata.be standard,
- finalement de fournir les données sous forme non pseudonymisée au destinataire final légitime.

**HealthData for Primary Care (HD4PrC)**

**26.** En ce qui concerne la communication de données à caractère personnel relatives à la santé par les prestataires de soins extramuraux, la plateforme Healthdata.be a développé une application HD4PrC (healthdata for primary care). Les données seront hébergées sur une plate-forme indépendante de Healthdata.be dont la gouvernance sera assurée par le Comité de gestion de la Plate-forme eHealth. Les mesures adéquates (encryption) seront prises afin d'assurer que la Plate-forme eHealth ne peut pas prendre connaissance des données médicales.

**27.** Mode de travail pour les prestataires de soins extramuraux avec DMI :

**Figuur 1: Werkwijze voor extramurale zorgverstrekkers met EMD**




**Etape 1 :** le fournisseur de données ouvre son DMI.

**Etape 2 :** dans son DMI, le fournisseur de données sélectionne un formulaire healthdata, ce qui ouvre une session HD4PrC au sein du DMI. Le formulaire est précomplété sur la base de la série de données que le DMI met à la disposition de HD4PrC. Le fournisseur de données complète la suite de l'enregistrement de façon manuelle. Avant d'envoyer l'enregistrement, les données médicales/scientifiques sont chiffrées vis-à-vis de healthdata.be.

**Etape 3 :** le fournisseur de données transmet les données à partir de son DMI vers eHBox codage. La Plate-forme eHealth se charge de la pseudonymisation du NISS du sujet des données (le patient dont les données sont collectées) et de quelques autres données. Pour ce faire, un même algorithme est utilisé pour tous les projets opérationnalisés dans le cadre du projet healthdata.be. Ensuite, les données sont transmises à la plateforme healthdata.be via eHBox.

**Etape 4 :** après contrôle et validation par le responsable de projet, il est possible de poser des questions supplémentaires au fournisseur de données ou de demander des données de suivi supplémentaires. A cet effet, healthdata.be envoie un message à HD4PrC via eHBox (de)codage. Ce message comprend les données pseudonymisées, ainsi que les données médicales/scientifiques chiffrées vis-à-vis du fournisseur de données. La Plate-forme eHealth assure le décodage des données pseudonymisées et fournit les données à HD4PrC, qui se charge de déchiffrer les données médicales/scientifiques.

**Etape 5 :** le fournisseur de données est informé du fait qu'il doit se connecter à HD4PrC pour corriger les données enregistrées précédemment ou enregistrer des données supplémentaires. Ceci est réalisé au moyen d'un message eHBox qui est

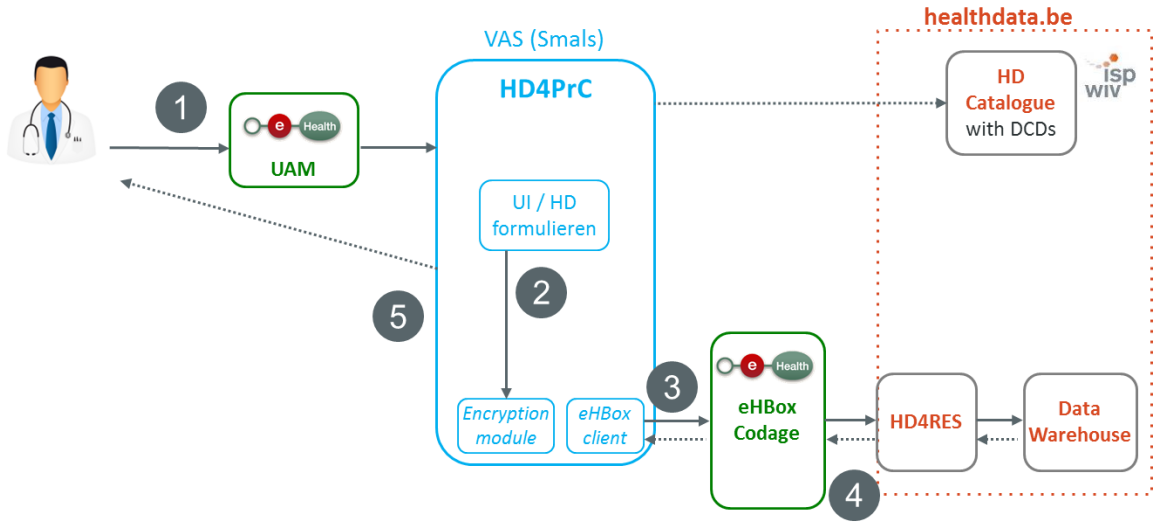
envoyé à partir de HD4PrC et qui peut être intégré dans le DMI du fournisseur de données.

**Etape 6 :** le fournisseur de données s'authentifie via la gestion intégrée des accès et des utilisateurs de la Plate-forme eHealth et obtient accès à HD4PrC.

**Etape 7 :** le fournisseur de données envoie les données à eHBox codage. La Plate-forme eHealth se charge de la pseudonymisation du NISS du sujet des données (le patient dont les données sont collectées) et de quelques autres données. Ensuite, les données sont transmises à la plateforme healthdata.be via eHBox codage. Avant d'envoyer l'enregistrement, les données médicales/scientifiques sont chiffrées vis-à-vis de healthdata.be.

**28.** Mode de travail pour les prestataires de soins extramuraux sans DMI :

**Figuur 2: Werkwijze voor extramurale zorgverstrekkers zonder EMD**




**Etape 1 :** le fournisseur de données s'authentifie via la gestion intégrée des utilisateurs et des accès de la Plate-forme eHealth et obtient accès à HD4PrC.

**Etape 2 :** le fournisseur de données sélectionne le formulaire de son choix et le complète avec les données du patient, ce qui correspond à 1 enregistrement. Avant d'envoyer l'enregistrement, les données médicales/scientifiques sont chiffrées vis-à-vis de healthdata.be.

**Etape 3** : le fournisseur de données envoie les données à eHBox codage. La Plate-forme eHealth se charge de la pseudonymisation du NISS du sujet des données (le patient dont les données sont collectées) et de quelques autres données. Pour ce faire, un même algorithme est utilisé pour tous les projets opérationnalisés dans le cadre du projet healthdata.be. Ensuite, les données sont transmises à la plateforme healthdata.be via eHBox.

**Etape 4 :** après contrôle et validation par le responsable de projet, il est possible de poser des questions supplémentaires au fournisseur de données ou de demander des données de suivi supplémentaires. A cet effet, healthdata.be envoie un message à HD4PrC via ehBox (de)codage. Ce message comprend les données pseudonymisées, ainsi que les données médicales/scientifiques chiffrées vis-à-vis du fournisseur de données. La Plate-forme eHealth assure le décodage des données pseudonymisées et fournit les données à HD4PrC, qui se charge de déchiffrer les données médicales/scientifiques.

**Etape 5 :** le fournisseur de données est informé par e-mail du fait qu'il doit à nouveau se connecter à HD4PrC pour corriger les données enregistrées précédemment ou enregistrer des données supplémentaires. Pour ce faire, il convient de parcourir à nouveau les étapes 1 à 3. Remarque : l'adresse e-mail du fournisseur de données est demandée lors de la 1ère authentification (étape 1), mais n'est jamais transmise à healthdata.be.

**29.** Les données sont toujours enregistrées de manière chiffrée sur HD4PrC et ce pour une courte durée. La durée exacte de l'enregistrement des données varie par projet et sera spécifiée dans les demandes d'autorisation spécifiques dans le cadre du projet.

**HealthData for Patient (HD4Patient)**

**30.** En ce qui concerne la communication de données à caractère personnel relatives à la santé par les patients, la plateforme Healthdata.be a développé une application HD4Patient (HealthData for Patient). La plateforme healthdata.be a formulé une demande d'extension de la présente délibération pour la mise en place de l'architecture générique HD4Patient, l'application avec laquelle healthdata.be entend soutenir l'enregistrement de données à des fins scientifiques ou d'appui à la politique à l'initiative du patient.

**31.** Il s'agit plus spécifiquement de l'architecture de soutien de l'application qui permet aux patients de notamment communiquer des données relatives à sa santé (PROM) et à son expérience avec le système de soins (PREM) à des fins scientifiques ou d'appui à la politique. Ces données qui varient en fonction des demandes d'autorisation spécifiques au projet peuvent être consultées pour ainsi se faire une idée de l'effectivité médicale des soins.

**32.** L'application HD4Patient, qui est comparable à l'application web HD4PrC, sera développée par healthdata.be et sera hébergée sur la plateforme « Value Added Services (VAS) » de la Smals. L'application HD4Patient demeure la propriété du service healthdata.be et l'opérateur de la plateforme VAS assume uniquement le rôle de sous-traitant au niveau de la plateforme d'hébergement. Le responsable du traitement pour l'application HD4Patient est désigné par le Comité de gestion de la Plate-forme eHealth qui veille à ce que les garanties nécessaires au niveau de la sécurité de l'information soient présentes. Les chercheurs responsables continuent à assumer le rôle et les responsabilités de gestionnaire des données.

**33.** L'objectif de l'application HD4Patient (HealthData for patient) est de permettre aux patients de communiquer leur perception concernant leur propre santé et leur expérience avec le système de soins. Ceci se fera au moyen de questionnaires généralement validés (PROM & PREM) pouvant contenir des questions supplémentaires spécifiques au registre.

**34.** Les Patient Reported Outcomes (PROM) et les 'Patient Reported Experience Measures' (PREM) ont été introduits pour soutenir les soins dans lesquels le patient occupe une place centrale.

1. Les PROM sont des questionnaires simples, validés pour les patients qui permettent de se faire une idée de l'effectivité médicale des soins. Les PROM reflètent la perception que la personne a de sa santé, en mesurant les symptômes, l'incertitude, l'angoisse, le fonctionnement, les soins autonomes, les besoins, etc.
2. Les PREM reflètent l'expérience d'une personne dans le système des soins de santé, souvent au moyen de questionnaires validés mesurant des indicateurs de qualité tels que délais d'attente, communication, participation au processus décisionnel. Certains pays utilisent déjà ces mesures de l'expérience du patient pour améliorer la qualité des soins.

Ceci doit se faire au moyen d'une méthode standard, dans le respect de la vie privée des personnes concernées.

**35.** Les données pseudonymisées recueillies via HD4Patient seront mises à la disposition des responsables des registres ou projets concernés via HD4RES et le datawarehouse healthdata.be, selon des modalités similaires à celles prévues pour le dossier unique « healthdata.be data collection » déjà approuvé.

**36.** De manière générale, il s'agit de patients et/ou de personnes en bonne santé qui sont recrutés dans le cadre d'un examen de santé ou de soins de santé ou qui satisfont aux critères fixés par la loi, par exemple en matière de remboursement. Les catégories plus spécifiques de personnes dont les données à caractère personnel sont traitées, sont systématiquement décrites dans les demandes d'autorisation spécifiques au projet. Le mode de sélection des personnes concernées est systématiquement décrit dans les demandes d'autorisation spécifiques au projet. Le nombre de personnes dont les données à caractère personnel seront traitées est systématiquement décrit dans les demandes d'autorisation spécifiques au projet.

**37.** Les données à caractère personnel communiquées varieront selon les projets et seront, à chaque fois, décrites dans les demandes d'autorisation spécifiques à chaque projet.

À l'instar de ce qui est décrit dans l'autorisation relative à l'architecture de base healthdata.be, il est en général possible d'opérer une distinction entre 2 types de données.

## A. Code d'identification des patients

Le NISS (numéro de registre national ou numéro bis) est utilisé comme code d'identification. Le NISS est codé par la Plate-forme eHealth au moyen du service de base TTP (eHealthbox batch codage) avant sa réception par healthdata.

Tous les enregistrements via HD4Patient utiliseront un même algorithme de pseudonymisation unique, qui est actuellement déjà utilisé et a été autorisé pour les enregistrements via HD4DP.

Avant que les chercheurs ne puissent accéder aux données individuelles du registre qui leur a été attribué, le code d'identification codé au moyen du service eHealth batch codage est codé une deuxième fois. Ce deuxième codage est spécifique au projet et permet d'éviter que les chercheurs ne puissent établir de liens entre les différents registres sans avoir reçu l'autorisation explicite à cet effet du Comité de sécurité de l'information. C'est en l'occurrence aussi le cas.

L'utilisation du NISS pseudonymisé est nécessaire pour les raisons suivantes :
- Identification des doubles enregistrements;
- Identification longitudinale du patient;
- Identification du patient au-delà des limites physiques des établissements de soins;
- Traçabilité de patients spécifiques (identifier en vue d'une participation éventuelle à des études cliniques, contrôle de qualité),;
- Couplage avec des sources authentiques, moyennant l'autorisation spécifique du Comité de sécurité de l'information;
- Couplage avec des banques de données validées, notamment avec d'autres registres sur la plateforme healthdata.be, moyennant l'autorisation spécifique du Comité de sécurité de l'information;
- Informer le patient au moyen d'un portail citoyen en ligne qui contient des références aux registres contenant des informations le concernant et à l'identité du (des) prestataire(s) et à l'utilisateur ou aux utilisateurs de ces données.

## B. Variables de registres

Les variables de registres sont constituées de *données médicales et de données à caractère personnel*. Les données à caractère personnel sont obtenues directement auprès des intéressés. Les données (médicales) spécifiquement demandées dépendent du projet et seront souvent demandées au moyen de questionnaires validés (au niveau international) qui ont pour objet de se faire une idée de la perception du patient concernant sa santé et de son expérience avec le système des soins de santé.

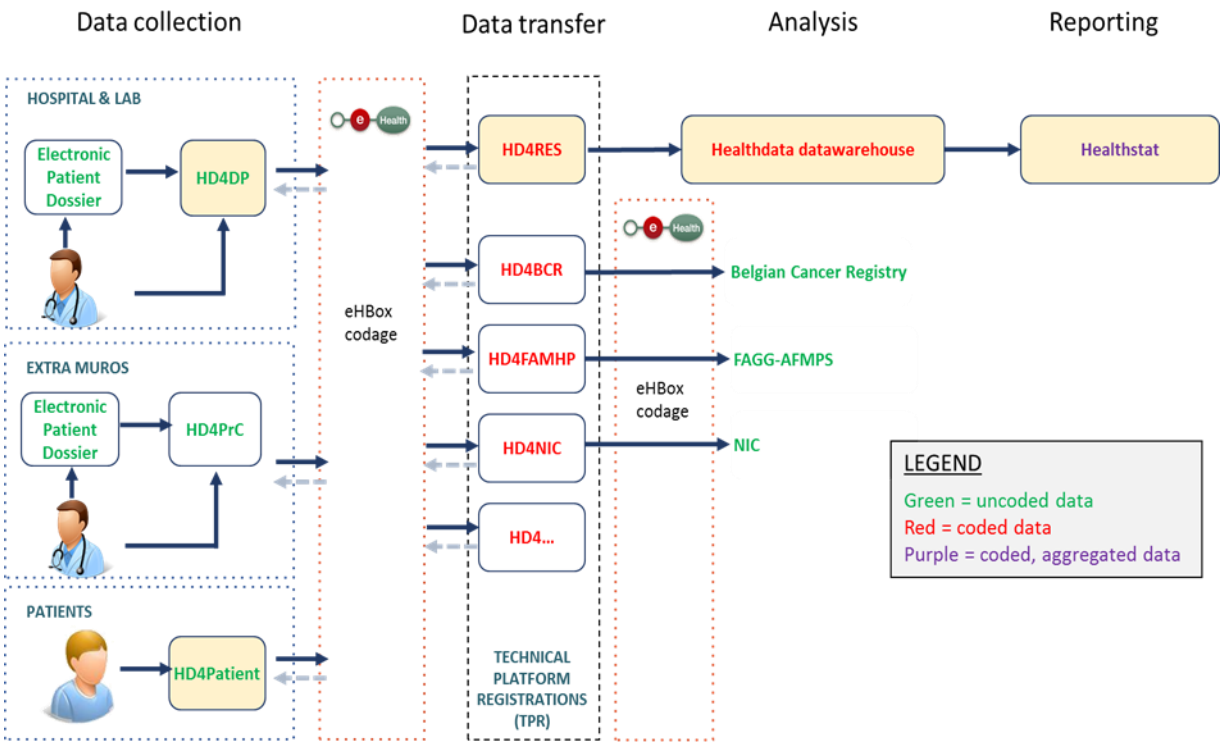
Ces données sont classées dans des registres spécifiques et sont chiffrées vis-à-vis de healthdata.be.

La raison de la communication de ces données à caractère personnel est à chaque fois décrite dans les demandes d'autorisation spécifiques au projet. Ces données sont en

général demandées pour ainsi se faire une idée de l'effectivité médicale et de la qualité des soins.

**Représentation schématique des flux de données**

Architecture de base générale avec situation du HD4Patient:




**38.** L'application web HD4Patient, comparable à l'application HD4PrC, sera développée par healthdata.be et sera hébergée sur la plateforme « Value Added Services (VAS) » de la Smals.

L'application HD4Patient demeure la propriété du service healthdata.be et l'opérateur de la plateforme VAS assume uniquement le rôle de sous-traitant au niveau de la plateforme d'hébergement.

Le responsable du traitement pour l'application HD4Patient est désigné par le Comité de gestion de la Plate-forme eHealth qui veille à ce que les garanties nécessaires au niveau de la sécurité de l'information soient présentes.

Les chercheurs responsables continuent à assumer le rôle et les responsabilités de gestionnaire des données pseudonymisées.

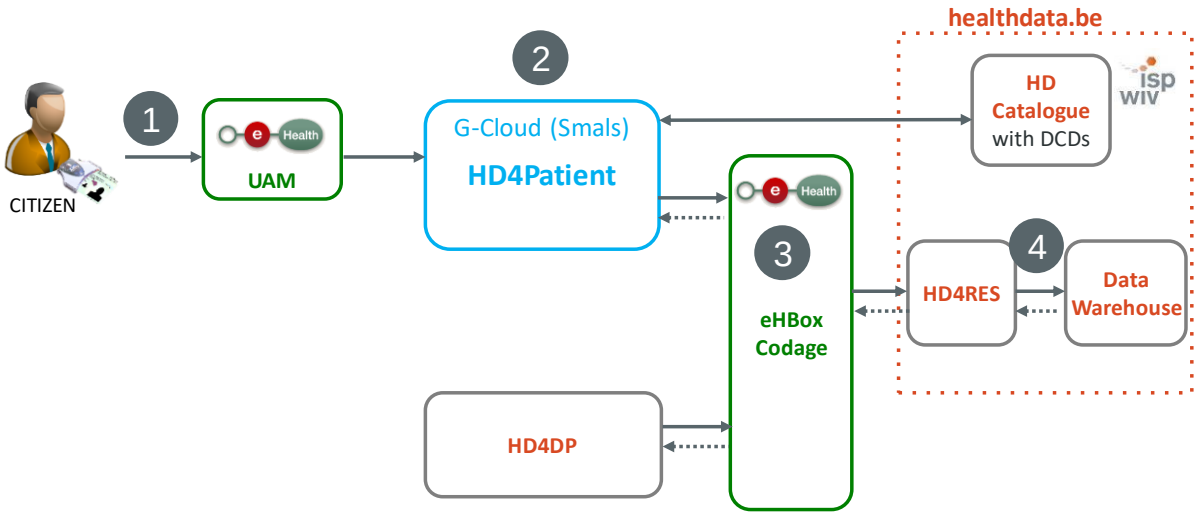
**Procédure pour les patients:**

Etape 1: Le patient se rend sur le site internet public de HD4Patient et s'authentifie au moyen de la gestion intégrée des utilisateurs et des accès de la Plate-forme eHealth. Il reçoit accès à HD4Patient.

Etape 2: Le patient remplit le formulaire lui soumis et initie l'envoi des données.

Etape 3: La Plate-forme eHealth se charge de la pseudonymisation du NISS du patient. Un même algorithme est à cet égard utilisé pour tous les projets qui sont facilités par le projet healthdata.be. Les données pseudonymisées sont ensuite transmises via le eHBox à la plateforme healthdata.be. Pour tout enregistrement reçu, Healthdata.be envoie un accusé de réception automatique via l'eHBox decodage. Cet accusé de réception contient uniquement l'identifiant technique de l'enregistrement. Il ne contient pas de données à caractère personnel.

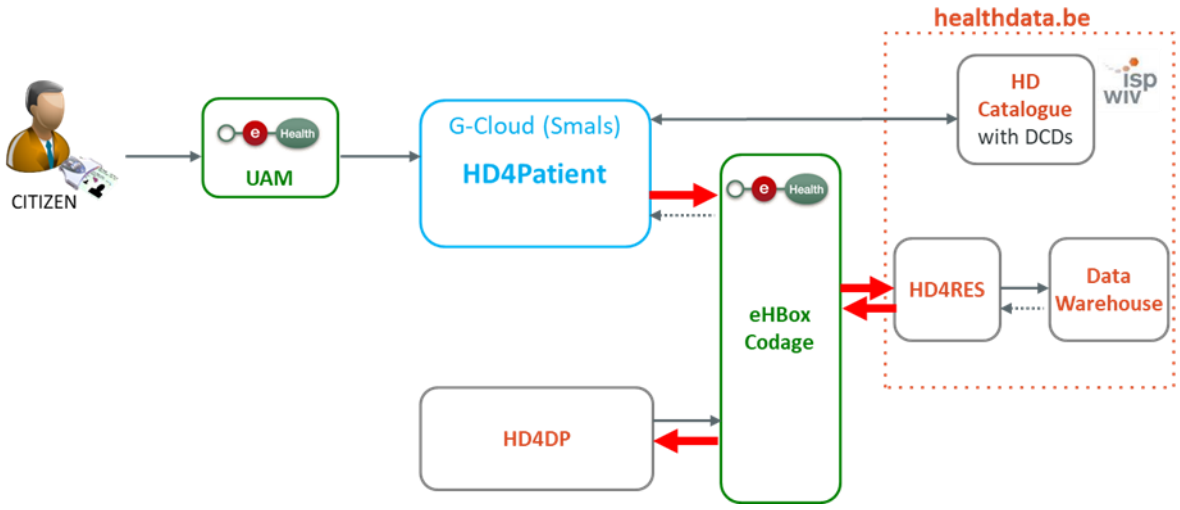
Etape 4: Au départ de HD4RES, ces données sont mises à la disposition des chercheurs en vue de la validation et du stockage dans le datawarehouse.



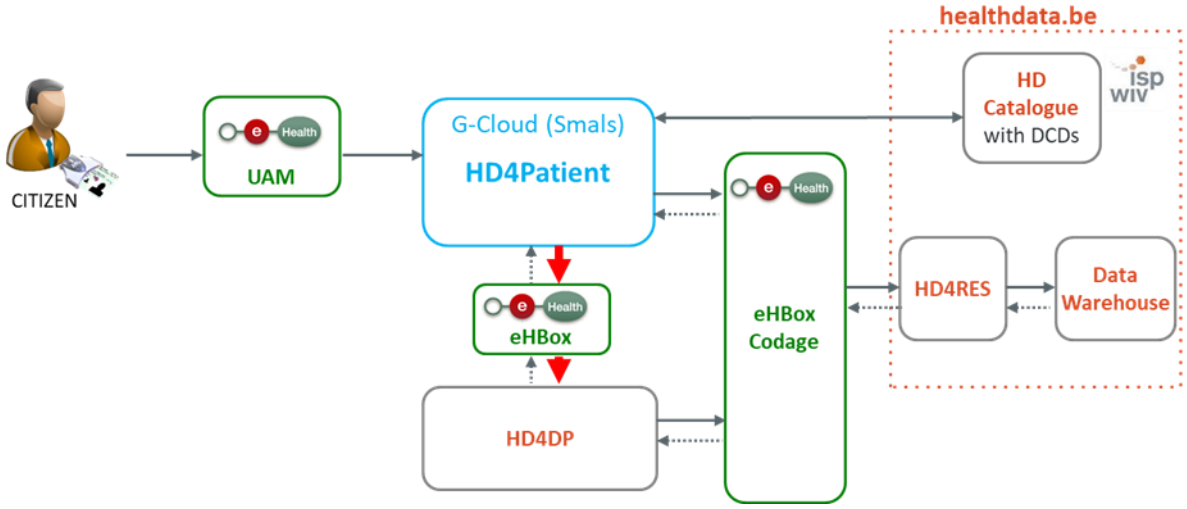

Etape 5: Les données enregistrées par le patient sont aussi transmises à l'installation HD4DP de l'hôpital/du laboratoire du médecin traitant, de sorte que le médecin puisse prendre connaissance des réponses de son/ses patient(s). Ceci en vue de l'appui de son fonctionnement opérationnel.

Pour ce transfert de HD4Patient vers HD4DP, il existe une méthode de travail temporaire et une procédure définitive.

**Flux de données temporaire**: Le transfert de HD4Patient vers HD4DP se déroule via HD4RES comme indiqué avec les flèches rouges sur la figure ci-dessous. La raison est que l'architecture de base actuelle de healthdata.be ne prévoit pas la possibilité pour HD4DP de communiquer avec l'eHBox (sans codage) et que cette possibilité supplémentaire n'est pas réalisable à bref délai.




**<u>Flux de données définitif</u>**: Dans la solution définitive, le transfert de HD4Patient vers HD4DP se fera via l'eHBox (sans codage), comme indiqué avec les flèches rouges sur la figure ci-dessous. De cette manière, les données médicales sont envoyées directement, sous forme non pseudonymisée, via l'eHBox (toutefois sous forme chiffrée) entre le patient et son (ses) prestataire(s) de soins connu(s).




Pour pouvoir réaliser ceci, il s'avère nécessaire d'adapter l'architecture de base de healthdata.be, en ce compris le module de chiffrement. Étant donné que celle-ci est développée par plusieurs parties externes, il y a lieu de tenir compte de la planification des développements utiles par chaque partie et de leurs tests détaillés. Pour ces raisons, il est proposé que le **passage de la solution temporaire à la solution définitive ait lieu au plus tard le 1er juillet 2020**.

**39.** La Plate-forme eHealth intervient comme organisation intermédiaire. Un découplage/décodage pour la raison suivante: dans des cas exceptionnels, le sous-traitant doit pouvoir vérifier vis-à-vis du responsable du traitement et vis-à-vis du patient qui exerce ses droits dans le cadre du nouveau RGPD l'intégrité/l'exactitude de l'identité du demandeur/patient.

**40.** Cette demande de délibération concerne uniquement l'architecture d'échange de données (collecte de données). Les modalités de l'analyse des données ne changent pas par rapport à l'approche standard de healthdata.be. Cela signifie que les données captées via HD4Patient seront, à l'instar des données captées via HD4DP, soumises à une analyse de risque « small cells » selon l'approche standard de healthdata.be.

**41.** L'architecture HD4Patient est paramétrable. Cela signifie qu'il est possible de mettre en place un filtre qui limiterait la communication de certaines données du patient au médecin généraliste. Ce filtrage des données ne serait réalisé que si c'est opportun en fonction de l'étude à laquelle le patient a participé.

**Applications HD4DP, HD4PrC et HD4Patient de la 2ième génération**

**42.** Pour faire face de manière efficace et modulable à la complexité croissante des flux de données et soutenir la transmission de données par des établissements de soins au moyen de divers protocoles (e.a. HL7-FHIR, OpenAPI) et formats (XML, JSON, CSV, VCF, …), la plateforme healthdata.be a développé une nouvelle génération de ses applications, en l'occurrence HD4DP 2.0, HD4PrC 2.0 et HD4Patient 2.0. Celles-ci sont conçues de manière modulaire avec notamment un « integration engine » (NextGen Connect), un « form renderer » (Form.io) et « Business Intelligence application » (Metabase).

**43.** Lors de la mise en service de HD4DP 2.0, HD4PrC 2.0 et HD4Patient 2.0, les projets qui ont actuellement recours à la première génération HD4DP, HD4PrC et HD4Patient seront progressivement migrés vers HD4DP 2.0, HD4PrC 2.0 et HD4Patient 2.0. Afin de garantir la continuité de ces projets, les applications de la première génération HD4DP, HD4PrC et HD4Patient continueront à être proposées en parallèle en production jusqu'au 31 décembre 2021.

**Communications distinctes du code d'identification des patients et des variables de registres**

**44.** La plateforme healthdata.be a introduit une demande d'extension de la présente délibération en vue de la mise en œuvre d'une répartition de la communication de données à caractère personnel par les prestataires de soins, les établissements de soins et les patients à la plateforme healthdata.be en une communication distincte du code d'identification des patients, d'une part, et une communication distincte des variables de registres, d'autre part (voir le schéma ci-dessous « Dataflow 1 : de DP vers healthdata.be »).

**45.** La communication distincte du code d'identification des patients, accompagné d'un code technique d'enregistrement créé de manière aléatoire par l'application HD4PD 2.0 (unique pour l'enregistrement, mais pas pour le patient), est réalisée au moyen de l'architecture existante et donc au moyen du service TTP de la Plate-forme eHealth. Dans ce cadre, l'expéditeur chiffre le code technique d'enregistrement mais pas le

code d'identification du patient. Le service TTP de la Plate-forme eHealth pseudonymise donc uniquement le code d'identification des patients.

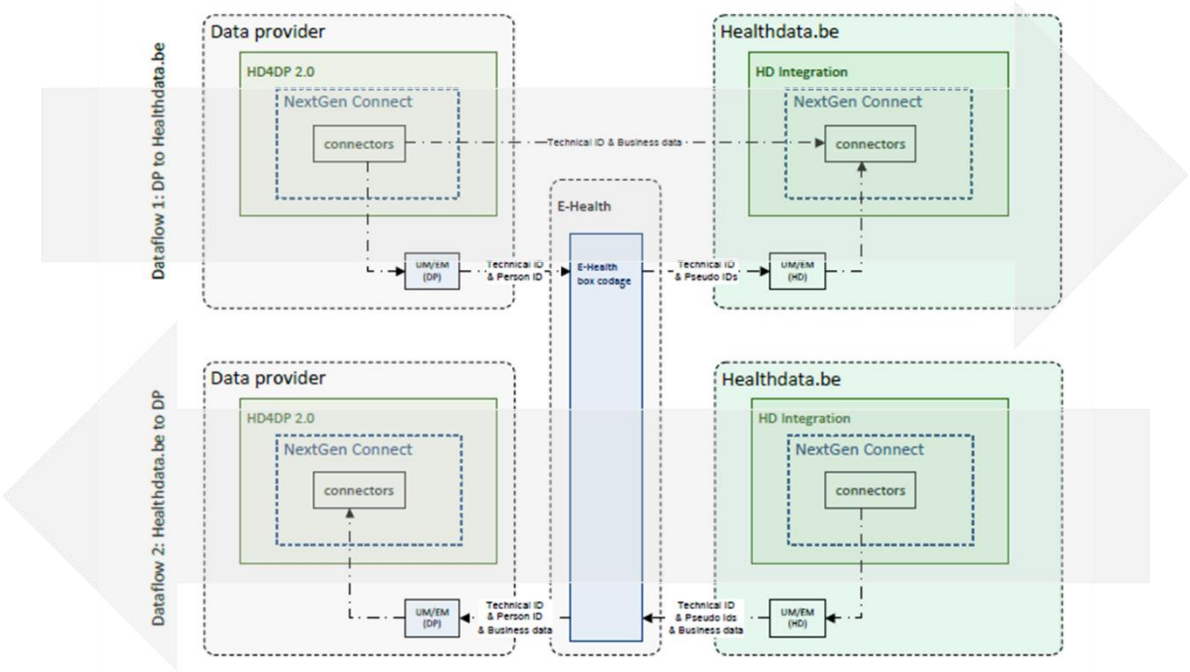
**46.** La communication distincte des variables de registres, accompagnées du code technique d'enregistrement (le même que le code technique pour le code d'identification des patients) s'effectue directement (service web) de manière chiffrée entre l'expéditeur et la plateforme healthdata.be.

**47.** La plateforme healthdata.be déchiffre les deux communications distinctes dès réception et consolide les communications sur base du code technique d'enregistrement. Après la consolidation et le contrôle de qualité technique, le code technique d'enregistrement est supprimé sans délai et de manière définitive de l'infrastructure healthdata.be. Un logging de ces processus techniques sera conservé par la plateforme healthdata.be.

**48.** Dans le cadre du flux de feed-back (en vue du contrôle de la qualité des données) de la plateforme healthdata.be vers le fournisseur de données, cette répartition n'est pas appliquée. Ce flux est réalisé au moyen de l'architecture existante (voir le schéma ci-dessous « Dataflow 2 : de healthdata.be vers DP ». Ce flux de feed-back est limité en termes de volume et de nombre.

**49.** Les communications distinctes du code d'identification des patients et des variables de registres seront appliquées de manière générique lors de la mise en service des applications de la deuxième génération HD4DP 2.0, HD4PrC 2.0 et HD4Patient 2.0.

Schéma : communications distinctes du code d'identification des patients et des variables de registres au moyen de HD4DP 2.0.




**50.** Au moyen de ces communications distinctes, la plateforme healthdata.be veut limiter l'impact du nombre croissant de communications et des volumes de ces communications sur la performance des composants intermédiaires de l'architecture (e.a. applications clientes eHBox des prestataires de soins et établissements de soins, service TTP de la Plate-forme eHealth).

**51.** La communication distincte du code d'identification des patients et des variables de registres a été soumise par la plateforme healthdata.be au groupe de travail Architecture du Comité de concertation des utilisateurs de la Plate-forme eHealth pour évaluation. Le groupe de travail Architecture a rendu un avis favorable en date du 20/12/2019 en ce qui concerne l'architecture avec des communications distinctes du code d'identification des patients et des variables de registres.

## II. COMPÉTENCE

**52.** Conformément à l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, la chambre sécurité sociale et santé du Comité de sécurité de l'information est en principe compétente pour toute communication de données à caractère personnel relatives à la santé.

**53.** 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 et portant dispositions diverses, la chambre sécurité sociale et santé du Comité de sécurité de l'information doit rendre une délibération pour toute communication de données à caractère personnel à la Plate-forme eHealth.

**54.** Le Comité de sécurité de l'information estime dès lors qu'il est compétent pour se prononcer sur cette communication de données à caractère personnel relatives à la santé.

## III. EXAMEN DE LA DEMANDE

**55.** Le Comité de sécurité de l'information prend acte du fait que Sciensano a été chargé, dans le cadre du Plan d'action eSanté 2013-2018, actualisé en 2015 sous la forme du Plan d'action eSanté 2015-2018, de la coordination et de l'élaboration d'un inventaire et de la consolidation des registres contenant des données à caractère personnel relatives à la santé.

**56.** La loi du 10 avril 2014 *portant des dispositions diverses en matière de santé* (art. 9) a créé un cadre qui permet à l'INAMI de renforcer et de systématiser sa collaboration avec Sciensano[3], en particulier en vue de la coordination et de l'appui des collectes de données qui doivent permettre d'augmenter les connaissances sur la santé de la population. Cette tâche de coordination et de soutien a été confiée à healthdata.be, une nouvelle entité au sein de la personne juridique de Sciensano, plus précisément au sein de la Direction opérationnelle Expertise, prestations de services et relations clients.

**57.** Il existe une séparation stricte au niveau administratif et comptable entre le service public Sciensano et la personne juridique de Sciensano qui a été créée par la loi du 25 février 2018[4]. La personne juridique dispose d'un management autonome qui gère librement les moyens propres, d'organes de décision propres, de règlements internes propres et est compétente pour conclure des conventions avec des établissements autres que les établissements fédéraux et pour engager du personnel propre.

**58.** Le positionnement de healthdata.be au sein de la personne juridique de Sciensano devrait permettre une prestation de services intergouvernementale aux administrations fédérale et fédérées qui sont compétentes en matière de santé et de soins de santé.

**59.** Le Comité de sécurité de l'information prend acte du fait que healthdata.be joue un rôle de facilitateur dans la collecte de données à caractère personnel pseudonymisées à des fins scientifiques et épidémiologiques et dans la collecte de données à caractère personnel non pseudonymisées à d'autres fins. Une architecture générique est mise en œuvre à cet effet, dont les points de départ sont les suivants:

- La collecte des données à partir des systèmes sources utilisés par les fournisseurs de données. Les données peuvent être transmises directement au moyen d'un message eHBox contenant des données structurées. En outre, est offerte une option permettant d'utiliser une application logicielle (au niveau local chez le fournisseur des données) qui soutient la collecte des données.

[3] Art. 66 de la loi du 25 février 2018

[4] Loi du 25 février 2018 portant création de Sciensano, M.B. du 21 mars 2018, p.27924.

- Les données sont envoyées par le fournisseur de données via l'eHBox à la Plate-forme eHealth en vue de la pseudonymisation des données à caractère personnel. A cet effet, les données médicales sont chiffrées vis-à-vis de healthdata.be en tant que destinataire final.
- Les données pseudonymisées destinées à des fins d'analyse sont directement transmises au datawarehouse de la plateforme healthdata.be.
- Après traitement et analyse par les chercheurs des données recueillies, des rapports et des résultats déterminés sont mis à la disposition des acteurs concernés (fournisseurs des données), des promoteurs/propriétaires des registres et du grand public via healthstat.be. Healthstat.be intervient comme plate-forme de publication pour ces rapports, figures et diagrammes au moyen d'une application web sécurisée et contrôlée.

**60.** Le Comité de sécurité de l'information estime qu'il est souhaitable que les composants techniques du côté des fournisseurs de données soient réutilisés de sorte à permettre une communication de données efficace pour diverses finalités. Le Comité de sécurité de l'information est cependant d'avis que la plateforme Healthdata.be doit veiller à ce que l'utilisation de ses services pour le traitement de données à caractère personnel ait toujours un rapport avec ses propres missions.

**61.** Le Comité de sécurité de l'information prend acte du décommissionnement de TPR par la plateforme Healthdata.be. La plateforme healthdata.be se conforme ainsi à la délibération précédente du Comité de sécurité de l'information qui disposait que le TPR n'est pas le moyen le plus approprié lorsque la collecte de données à caractère personnel est réalisée via les services de la plateforme Healthdata.be en vue de la communication de données à caractère personnel non-pseudonymisées à un destinataire légitime sans qu'il n'y ait de rapport avec le datawarehouse de la plateforme Healthdata.be.

**62.** En ce qui concerne la communication concrète de données à caractère personnel, les demandes d'autorisation spécifiques au projet mentionneront les modalités concrètes (les fournisseurs des données, les catégories de données, les finalités de la communication, les catégories de destinataires, le délai de conservation, etc.).

**63.** En ce qui concerne l'identification des patients, seul le numéro d'identification de la sécurité sociale (pseudonymisé) du patient est utilisé.

**64.** La Plate-forme eHealth procède à la pseudonymisation des codes d'identification préalablement à leur réception par Sciensano. Le Comité de sécurité de l'information prend acte du fait qu'un algorithme de pseudonymisation unique sera utilisé pour tous les projets qui seront opérationnalisés sur la plateforme healthdata. Si des données à caractère personnel pseudonymisées sont mises à la disposition de tiers (chercheurs) dans le cadre d'un registre déterminé, le code d'identification déjà pseudonymisé est codé une deuxième fois. Ce deuxième codage est spécifique au registre et permet d'éviter que les chercheurs ne puissent établir de liens entre les différents registres

sans avoir reçu l'autorisation explicite du Comité de sécurité de l'information ou d'une autre instance compétente.

**65.** Le Comité de sécurité de l'information estime que l'utilisation du Registre national est acceptable vu la nécessité d'identification des doubles enregistrements; identification longitudinale du patient; identification du patient au-delà des limites physiques des établissements de soins, traçabilité de patients spécifiques (dans le cadre d'une participation éventuelle à des études cliniques, contrôle de la qualité); couplage à d'autres sources authentiques (moyennant l'autorisation spécifique des instances compétentes), couplage aux banques de données validées dont d'autres registres à la plateforme ehealthdata.be (moyennant l'autorisation spécifique des instances compétentes); information du patient (via un portail citoyen en ligne) au moyen d'un renvoi aux registres contenant des données le concernant ainsi que l'identité du (des) fournisseur(s) et de l' (des) utilisateur(s) de ces données.

**66.** En exécution de l'article 5 de la loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier, le Comité de sécurité de l'information autorise l'utilisation du numéro de registre national lors de l'échange de données dans le cadre de healthdata.be et de healthstat.be.

**67.** Pour rappel, la Plate-forme eHealth est chargée de la pseudonymisation des numéros d'identification des intéressés. Etant donné le caractère longitudinal des registres, la Plate-forme eHealth doit conserver le lien entre le numéro d'identification et le numéro pseudonymisé.

**68.** En ce qui concerne la collecte de données à caractère personnel pseudonymisées qui seront également mises à la disposition sous forme pseudonymisée, le demandeur sollicite un décodage dans deux cas bien précis:

- pour un contrôle de qualité. Lorsque le sous-traitant des données (p.ex. le chercheur) présume que des données relatives à un patient déterminé ont éventuellement été enregistrées de manière erronée dans le registre, le sous-traitant doit pouvoir communiquer avec le centre concernant ce patient afin de vérifier si les données sont correctes et de pouvoir apporter les corrections.
- pour le recrutement de patients spécifiques pour des études cliniques: le centre/le médecin doit être informé des patients qui entrent en considération pour des études cliniques.

Les données à caractère personnel seront uniquement visibles pour le centre ou le médecin qui a introduit les données. Le Comité de sécurité de l'information estime qu'un décodage est acceptable dans ces deux cas bien précis.

**69.** Le Comité de sécurité de l'information prend également acte de la demande de la plateforme healthdata.be pour un envoi direct (au moyen d'un service web) de manière chiffrée et non-pseudonymisée à la fois des variables de registres et d'un code technique des fournisseurs de données vers la plateforme healthdata.be et du

fait que ce code technique serait immédiatement et définitivement supprimé de l'architecture healthdata.be dès la consolidation des variables de registres et du code d'identification pseudonymisé des patients. Le logging de ces processus doit prouver qu'ils ont effectivement eu lieu.

**70.** Le Comité de sécurité de l'information prend acte du fait que l'analyse des risques « small cell » sera réalisée sous la responsabilité du Comité directeur. L'analyse des risques « small cell » doit être réalisée conformément aux critères auxquels doit satisfaire tout TTP qui procède au codage de données à caractère personnel relatives à la santé[5], tels que définis par le Comité de sécurité de l'information. Les modalités concrètes de l'analyse des risques « small cell » seront décrites dans le cadre des demandes d'autorisation spécifiques par registre.

**71.** Les messages qui sont envoyés par les fournisseurs de données à healthdata.be contiennent des métadonnées: ID envoi (pseudonymisé par la Plate-forme eHealth), ID registre (chiffré par rapport à healthdata.be), statut/action (new, update, etc.) (chiffré vis-à-vis de healthdata.be) et fournisseur des données: numéro d'identification et type (chiffrés vis-à-vis de healthdata.be). Ces données sont nécessaires au contrôle de qualité, aux rapports de feedback et à la notification des candidats éventuels pour les études cliniques.

**72.** Le Comité de sécurité de l'information prend, en outre, acte du fait que les données à caractère personnel relatives à la santé seront traitées dans le cadre de healthdata.be et de healthstat.be sous la surveillance et la responsabilité d'un praticien des soins de santé, plus précisément d'un médecin.

**73.** Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est tenu de prendre des mesures dans les onze domaines d'action suivants liés à la sécurité de l'information: politique de sécurité; désignation d'un délégué à la protection des données; organisation et aspects humains de la sécurité (engagement de confidentialité du personnel, information et formations régulières du personnel sur le thème de la protection de la vie privée et sur les règles de sécurité); sécurité physique et de l'environnement; sécurisation des réseaux; sécurisation logique des accès et des réseaux; journalisation, traçage et analyse des accès; surveillance, revue et maintenance; système de gestion des incidents de sécurité et de la continuité (systèmes de tolérance de panne, de sauvegarde, …); respect et documentation. Le demandeur est dès lors tenu de prendre toutes les mesures utiles permettant d'assurer la confidentialité des données à caractère personnel codées traitées.

**74.** Le Comité de sécurité de l'information prend acte du fait qu'un délégué à la protection des données a été désigné et que la politique Sciensano relative au traitement de données à caractère personnel contient aussi une police de sécurité spécifique. Par ailleurs, les collaborateurs scientifiques de Sciensano sont tous tenus

[5] Délibération n° 14/059 du 15 juillet 2014 (voir https://www.ehealth.fgov.be/fr/propos/organisation/comite-sectoriel/deliberations-2014)

contractuellement de respecter strictement le secret professionnel et de traiter les données d'une manière déontologique et éthique.

**75.** Le Comité de sécurité de l'information estime qu'il est opportun que le délégué à la protection des données concerné communique une copie de son rapport annuel relatif à la sécurité de l'information au Comité de sécurité de l'information.

**76.** Le Comité de sécurité de l'information rappelle qu'il est interdit d'entreprendre toute action visant à convertir les données à caractère personnel pseudonymisées en données à caractère personnel non pseudonymisées. Le non-respect de cette interdiction peut donner lieu à une amende. Le Comité de sécurité de l'information rappelle également qu'en cas de condamnation du chef d'infraction à l'article 39, le juge peut prononcer la confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction (fichiers manuels, disques et bandes magnétiques, …) ou ordonner l'effacement de ces données. Le juge peut également interdire de gérer, personnellement ou par personne interposée, et pour deux ans au maximum, tout traitement de données à caractère personnel.

**77.** Le Comité de sécurité de l'information souligne qu'en vertu de l'article 111, alinéa 1er, de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, sans préjudice des pouvoirs de contrôle de l'Autorité de protection des données, les autorisations accordées par les comités sectoriels de la Commission de la protection de la vie privée avant l'entrée en vigueur de cette loi gardent leur validité juridique. Les modalités de la délibération n° 15/009 du 17 février 2015, dernièrement modifiée le 5 juin 2018, relative à la méthode générique d'échange de données à caractère personnel codées et non pseudonymisées relatives à la santé, dans le cadre de healthdata.be et healthstat.be restent donc d'application.

**78.** Le Comité de sécurité de l'information estime nécessaire de rappeler que depuis le 25 mai 2018, la plateforme healthdata.be ainsi que Sciensano, sont tenus de respecter les dispositions et les principes du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

**79.** Le Comité de sécurité de l'information constate que la plateforme healthdata.be remplacera le flux de données temporaire pour HD4Patient par un flux définitif au moyen de HD4Patient 2.0 pour le 1er juillet 2020.

Par ces motifs,

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

vu la délibération n° 15/009 du 17 février 2015, dernièrement modifiée le 5 juin 2018, relative à la méthode générique d'échange de données à caractère personnel codées et non codées relatives à la santé, dans le cadre de healthdata.be et healthstat.be ;

prend acte du fait que la plateforme healthdata.be s'engage à adapter HD4Patient pour le 1er juillet 2020. Le Comité de sécurité de l'information autorise la mise en place d'un flux de données temporaire tel que décrit au point 38 ;

prend acte du fait que la plateforme healthdata.be s'engage à procéder au décommissionnement de la Plateforme Technique Enregistrements pour le 1er juillet 2020.

prend acte du fait que lors de la mise en service des applications de la 2ième génération HD4DP 2.0, HD4PrC 2.0 et HD4Patient 2.0, la communication du code d'identification des patients d'une part et des variables de registres d'autre part, chacun couplé à un code technique (unique à l'enregistrement, mais pas au patient), est effectuée séparément : le code d'identification des patients est transmis via l'architecture existante et donc au moyen du service TTP de la Plate-forme eHealth, tandis que les variables de registres sont transmises directement à la plateforme healthdata.be au moyen d'un service web chiffré ;

prend acte du fait que des demandes de délibération spécifiques seront introduites par registre destiné à figurer dans healthdata.be et healthstat.be ainsi que pour chaque intervention de healthdata.be dans le cadre de la communication de données à caractère personnel non pseudonymisées ;

autorise la Plate-forme eHealth à conserver le lien entre le numéro d'identification réel et le numéro pseudonymisé et à procéder au décodage dans des cas bien précis tels que décrits dans la présente délibération ;

conclut que la communication de données à caractère personnel, telle que décrite dans la présente délibération, est autorisée moyennant le respect des mesures de protection de la vie privée qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Bart VIAENE

Le siège de la chambre sécurité sociale et santé du Comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles (tél. 32-2-741 83 11).