Rôles et responsabilités pour la nouvelle politique des registres en Belgique

Ce document s'inscrit dans la **poursuite de** l'**élaboration et de l'opérationnalisation** de la nouvelle vision d'avenir de la politique des registres en Belgique, élaborée en automne 2024 par l'INAMI et le SPF SPSCAE (également disponible sur le site web de l'INAMI).

Pour réaliser cette nouvelle vision d'avenir, différents **rôles et responsabilités** seront attribués à différents acteurs afin d'opérationnaliser la politique des registres décentralisée et fédérée. Le document actuel contient un **aperçu des rôles et des responsabilités** qui constituent la base de la nouvelle politique des registres. Ces rôles et responsabilités découlent des exigences fonctionnelles identifiées pour la politique des registres. On explique ensuite **quelles parties** ou organisations sont responsables de mettre en œuvre **en pratique** les différents rôles dans le cadre de la politique des registres en Belgique

Le cas échéant, la note fait référence à l'alignement des rôles et responsabilités au sein de la politique des registres avec le **règlement EHDS européen (espace européen des données de santé)**. Dans l'analyse actuelle, il est supposé que la politique des registres relève en partie de l'utilisation secondaire des données de santé conformément au règlement EHDS, plus précisément lorsque les registres sont utilisés dans le cadre de demandes relevant de l'EHDS. L'élaboration de la politique des registres au niveau (inter)fédéral belge doit ainsi répondre aux obligations prévues par le règlement EHDS, mais peut toutefois être mise en œuvre de manière alternative dans certains domaines. Les explications supplémentaires dans la note indiqueront, à l'aide d'un **code de couleur,** les aspects pour lesquels la politique des registres est entièrement conforme au règlement et ceux pour lesquels les spécificités propres à la politique des registres entraînent de légères déviations. Là où des références sont faites au règlement EHDS et à sa mise en œuvre en Belgique, il est important de préciser que cette note ne se prononce pas sur la manière dont la mise en œuvre de l'EHDS se déroulera exactement. Cela est entièrement aligné sur la mise en œuvre telle que prévue dans le plan d'action eHealth et le plan d'action healthdata. La portée de cette note se limite à la politique des registres et à son alignement ultérieur dans le contexte de l'EHDS.

Il est important de noter que la nouvelle vision d'avenir représente un changement significatif par rapport à la manière actuelle de travailler pour la compilation, le traitement et la mise à disposition des registres. Les responsabilités sont redistribuées, les data holders et les utilisateurs assumant également des responsabilités supplémentaires conformément au règlement EHDS. Il est donc important de considérer ce document et les rôles, responsabilités et activités qui y sont décrits indépendamment de la manière dont ils sont actuellement remplis. Dans la mesure du possible, une comparaison est faite avec la situation d'aujourd'hui afin de montrer en quoi elle diffère de la vision d'avenir.

On souhaite attirer l'attention du lecteur sur la remarque générale suivante. Cette note donne une vision des rôles et des responsabilités en s'appuyant sur les informations actuellement disponibles. En même temps, la note s'inscrit dans un contexte d'évolution continue. Par exemple, tous les développements et décisions concernant la mise en œuvre du règlement EHDS en Belgique ne sont pas encore connus. Par conséquent, cette note doit être considérée comme un document dynamique qui sera encore adapté ou ajusté à l'avenir lorsque cela sera nécessaire et pertinent.

Modifications par rapport à la vision initiale de la politique des registres

En mars 2025, la nouvelle vision a été publiée, puis expliquée lors d'un webinaire[1]. Cela a naturellement soulevé des questions chez les différentes parties prenantes. À la suite de ces questions et d'une compréhension progressive, quelques modifications ont également été apportées à la terminologie utilisée et à la présentation de la nouvelle vision. La vision n'est pas 'figée' et évoluera au fur et à mesure des discussions avec les parties prenantes et des enseignements tirés.

C'est pourquoi certains termes de la vision précédente sont modifiés et clarifiés, à savoir :

- 'Registre permanent' devient '(nouveau) registre' : On ne parle plus d'un registre 'permanent'. Le terme registre permanent crée beaucoup de confusion quant à la conception même des registres et à leur utilisation. En substance, le plus grand changement concerne la manière dont les données seront récoltées et continueront à être gérées dans un registre. Il s'agit donc principalement d'une évolution technologique. Cela ne signifie pas que les data users du registre (entités bleues de la figure 1) auront automatiquement accès à tous les registres pour toutes les finalités possibles. Cela reste inchangé et sera, comme aujourd'hui, défini et déterminé dans une base juridique. Ici, l'accent sera principalement mis sur la clarification des registres existants afin d'éviter les doublons et les doubles enregistrements et traitements. Le glossaire explique plus en détail en quoi un registre actuel diffère d'un nouveau registre selon la nouvelle vision.
- 'Registre temporaire' devient 'demande de données dans l'EHDS' : Afin d'éviter toute confusion et de garantir l'alignement avec le règlement EHDS, le terme 'registre temporaire' ne sera plus utilisé à l'avenir. À la place, il est fait référence à une 'demande de données dans l'EHDS' ou, en bref, à une 'demande de données'. Pour les demandes de données pour utilisation secondaire, on s'alignera en Belgique entièrement sur le règlement EHDS.

[1] Politique des registres de données de soins de santé | INAMI

Table des matières

A. Vision concernant la nouvelle politique des registres en Belgique 4
B. Glossaire 5
C. Rôles dans le cadre de la nouvelle politique des registres en Belgique 10
D. Description détaillée des rôles dans le cadre de la nouvelle politique des registres 12

A. Vision concernant la nouvelle politique des registres en Belgique

Le **point de départ** pour déterminer les rôles et responsabilités est la vision pour la **nouvelle politique des registres**, telle que publiée sur le site web de l'INAMI. La vision est représentée de manière schématique dans **la figure ci-dessous**, comme discuté et validé lors du groupe de pilotage qui suit le projet (02/10/2024). Le **code de couleur utilisé** fait référence aux différentes composantes de la nouvelle vision, comme indiqué ci-dessous :

- **Vert** - Mise à disposition des données nécessaires pour les registres par les différents data holders avec compréhension des données fournies.
- **Bleu** - Utilisation continue des données et gestion des registres par un certain nombre de data users qui font partie du réseau fédéré.
- **Jaune** - Utilisation des données résultant de demandes de données par différents utilisateurs autorisés, ou utilisation des données de registres par des data users autorisés.

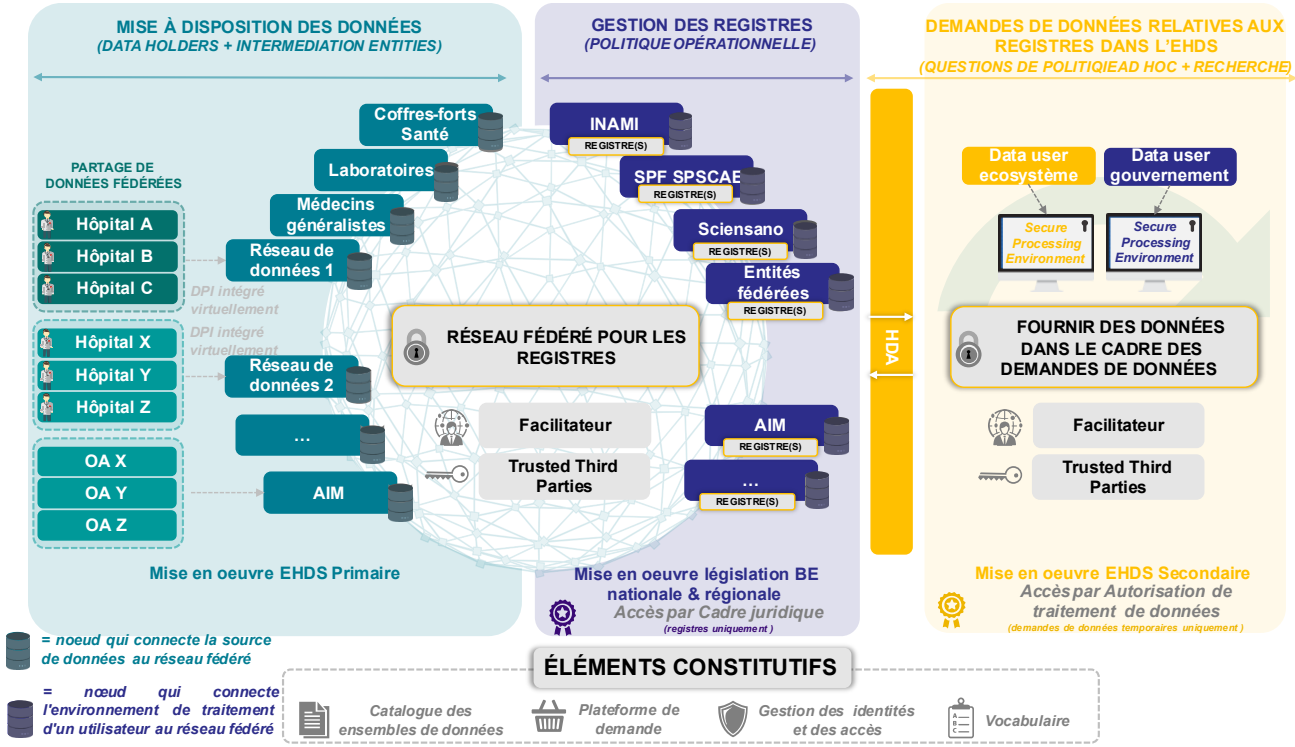

Figure 1: Représentation schématique de la nouvelle politique des registres en Belgique

B. Glossaire

Ce chapitre donne un aperçu de **plusieurs concepts importants** qui seront abordés dans la suite de la note. Ces concepts peuvent aider le lecteur à comprendre, dans d'un cadre clair, les différentes considérations présentées dans la note.

CONCEPTS DE BASE

- **Registre :**
  - **(selon le fonctionnement actuel) :** Un registre (de patients) est une collection - à **une ou plusieurs fins** - **d'informations uniformes et standardisées** (cliniques et autres) sur un groupe de patients **partageant une condition ou une expérience**.[2] Cette collecte se fait généralement sous la forme d'instantané capturé à partir de systèmes via un formulaire. De plus, les données qui ne sont pas encore standardisées sont saisies ou reprises à partir d'autres systèmes de manière manuelle (,par exemple à partir d'un système **dossier patient informatisé (DPI)** , semi-automatique (par exemple via un fichier CSV, extrait d'un système DPI) ou entièrement automatique (par exemple via une API liée à un système DPI). Dans la nouvelle politique des registres élaborée par l'INAMI et le SPF SPSCAE, la manière dont ces données sont récoltées est revue, en tenant compte des nouvelles évolutions technologiques et réglementaires. Si une collecte de données ne répond pas à la définition d'un registre **selon la nouvelle vision** (voir définition ci-dessous), on ne parle plus d'un registre, mais d'une **demande de données** dans l'EHDS (voir définition ci-dessous).
  - **(selon la nouvelle vision) :** Dans la nouvelle vision, les registres sont entretenus **en continu** et mis à disposition des utilisateurs autorisés pour une gestion ultérieure. La nouvelle politique des registres diffèrera de la politique actuelle sur plusieurs plans importants, à savoir la gouvernance appliquée (y compris, par exemple, les rôles décrits dans cette note), l'architecture et la configuration technique, mais aussi la rationalisation et la simplification des registres. Des principes tels que le only once, la standardisation et la poursuite d'une haute qualité à la source sont primordiaux. Les registres seront utilisés dans le cadre de la **politique opérationnelle** des institutions publiques (de santé). Un exemple illustratif en est la fourniture de données clés essentielles, telles que des données de synthèse sur l'incidence et la prévalence des maladies et des affections. Par exemple, l'incidence et les caractéristiques microbiologiques des maladies infectieuses circulantes sont récoltées via des registres afin de permettre le contrôle des infections au niveau national. La différence avec la méthode de travail actuelle réside principalement dans la mise à disposition des données nécessaires à cet effet. Celles-ci devront être disponibles en continu. Un registre sera organisé aussi **efficacement et minimaliste** que possible et contiendra un **ensemble** (limité) **de variables**. Une considération importante dans ce cadre est que les registres doivent toujours être établis dans **un cadre juridique, dans lequel sont définis les ensembles de variables nécessaires.** De plus, les data users ne doivent soumettre qu'une **seule fois** une demande pour avoir ensuite un accès illimité et permanent à un registre. Dans la nouvelle politique, les données de santé récoltées proviendront autant que possible du **dossier patient informatisé (DPI) et du dossier**

[2] https://www.ncbi.nlm.nih.gov/books/NBK164514/

médical électronique (DME) en combinaison avec des sources de données authentiques existantes (par exemple, provenant de STATBEL). La poursuite de la mise en œuvre du **résumé du dossier du patient**, qui doit être mis en place dans le cadre du règlement EHDS, peut faciliter l'échange entre le DPI et le DME. Les données de santé récoltées sont déterminées par les besoins des data users. Dans la nouvelle politique des registres, les données ne sont pas simplement mises à disposition sur demande, mais on évolue vers une mise à disposition proactive des données pertinentes. L'objectif est de donner un aperçu des données disponibles de manière structurée en les proposant, via un catalogue des ensembles de données, aux utilisateurs potentiels. À cet égard, les données disponibles sont donc rendues aussi claires que possible en vue d'une utilisation éventuelle dans un registre. Ainsi, les données similaires figurant dans différents registres seront saisies et traitées de la même manière, selon le principe du only once, et les doubles enregistrements seront évités autant que possible.

- **Demande de données relative à un registre dans l'EHDS** (selon la nouvelle vision) : Avec l'arrivée de l'EHDS, les demandes d'utilisation des données d'un registre se dérouleront comme prévu dans le règlement EHDS. Une demande de données, dans le cadre de la politique des registres, concerne une demande d'utilisation des données d'un registre à des fins autres que celles initialement prévues. À cette fin, les principes et méthodes de l'utilisation secondaire des données selon l'EHDS seront donc pleinement appliqués. Au sein de l'EHDS, l'utilisation des données de santé est liée aux différentes catégories.[3] Ces catégories font également référence aux registres. La demande de données selon l'EHDS peut se faire de différentes manières. Dans ce document, on parlera toujours de demande de données afin de limiter la complexité. Il est toutefois nécessaire de mentionner qu'une demande de données selon l'EHDS est toujours limitée dans le temps lorsqu'il s'agit de données personnelles sensibles, à savoir avec une durée maximale de 10 ans[4] et la possibilité de prolonger cela une seule fois. Il s'agit d'un ensemble spécifique de données adapté à une demande spécifique, généralement dans le cadre de la recherche scientifique et de questions de politique ad hoc. Ces demandes de données peuvent concerner les mêmes données qui sont enregistrées dans un registre, les données étant alors mises à disposition temporairement au lieu d'être disponibles en continu. Cependant, une demande de données peut également concerner une collection plus large de données, par exemple, en combinant des données provenant de plusieurs registres ou en les complétant avec d'autres sources de données, toujours alignée avec la question spécifique de recherche ou de politique. Une demande de données peut se transformer en un registre lorsqu'une disponibilité continue des données est requise au lieu d'une disponibilité temporaire (selon le délai EHDS), à condition que cette transition soit soutenue par un cadre juridique approprié.

ÉCHANGE DE DONNÉES DE SANTÉ

- **Only Once :** Only Once est un concept selon lequel les prestataires de soins ne **récoltent et n'enregistrent** les données de santé des patients **qu'une seule fois**, pour ensuite les partager avec les autres prestataires de soins dans le domaine des soins de santé, avec le consentement

[3] EHDS article 51.
[4] EHDS article 68, alinéa 12.

du patient si nécessaire. Le only Once vise à éviter les doubles enregistrements et la collection répétée des mêmes informations, ce qui stimule **l'efficacité**, améliore la dispensation des soins, optimalise l'expérience du patient, augmente la qualité des données, mais surtout réduit la charge administrative.

- **Interopérabilité sémantique :** L'interopérabilité sémantique garantit que différents systèmes peuvent non seulement échanger des données techniquement, mais aussi attribuer la **même signification** à ces données. Cela assure une **interprétation correcte des informations**, évitant ainsi les malentendus.
- **Interopérabilité technique :** L'interopérabilité technique garantit que différents systèmes peuvent communiquer entre eux et que la connexion fonctionne techniquement via des **réseaux, des formats de fichiers et des protocoles de communication**.

MISE À DISPOSITION DES DONNÉES DE SANTÉ

- **Agrégation :** Appliquée aux **données indirectement identifiables et sensibles** (par exemple, domicile, âge, poids, …), l'agrégation est une technique qui groupe ces données en **catégories ou groupes plus larges**. Ainsi, les caractéristiques individuelles deviennent moins spécifiques et les données ne peuvent plus être directement ramenées à un individu lorsqu'on tient compte des 'small cells'. L'agrégation est souvent utilisée comme méthode dans la pseudonymisation et l'anonymisation.
- **Anonymisation :** L'anonymisation est le processus par lequel les **données identifiables et sensibles** sont **irréversiblement supprimées ou modifiées**, de sorte qu'elles ne peuvent plus être associées à un individu. Contrairement à la pseudonymisation, il n'est pas possible de restaurer directement les données originales plus tard dans le processus. L'objectif de l'anonymisation est d'exclure entièrement toute possibilité de (ré)identification des individus.
- **Pseudonymisation :** La pseudonymisation est le processus par lequel les **données identifiables et sensibles sont remplacées par des pseudonymes, par exemple par des codifications, des agrégations ou l'utilisation de tables de référence**. Contrairement à l'anonymisation, il subsiste toutefois le risque qu'il soit possible de récupérer les données originales, soit directement en inversant le processus, soit indirectement en réduisant le nombre de personnes auxquelles ces données peuvent se rapporter en les reliant à d'autres données. L'objectif de la pseudonymisation est de minimiser autant que possible la réidentification des individus en fonction des moyens techniques actuels, tout en conservant l'utilité des données pour l'analyse et d'autres applications.
- **Codification :** La codification (Encode/Decode) est une technique spécifique de pseudonymisation **par laquelle les données directement identifiables** sont converties en un code d'identification dénué de sens au moyen de **chiffrement**. Cela entraîne des données qui ne sont plus lisibles sans la clé appropriée, mais tout en conservant la possibilité de restituer les données originales avec la clé spécifique appropriée. Il est également fait référence aux services de pseudonymisation (par exemple, Batch codage) proposés pour eHealth[5].
- **Chiffrement :** Le chiffrement ou le cryptage est le processus par lequel les données sont converties en une **forme codée par un chiffrement cryptographique**, de sorte qu'elles ne soient ni lisibles ni accessibles. L'objectif est de garantir la **confidentialité et la sécurité** des données. Il est important que le chiffrement des valeurs soit effectué à l'identique.

[5] Pseudonymisation & Anonymisation | Platform eHealth

- **La TTP de Codification :** Cette Trusted Third Party (TTP) est responsable de la **codification des données directement identifiables** (par exemple, le numéro NISS, nom, …) champ par champ par un chiffrement avec des clés gérées par cette TTP, et offre la possibilité de chiffrer d'autres données dans leur ensemble. Cette TTP n'a pas accès à d'autres données personnelles concernant la santé de l'individu et code uniquement les données personnelles directement identifiables. Cette vision s'aligne sur la **note du CSI**[6] qui indique qu'une TTP de Codification est responsable de la codification des données personnelles et peut faciliter le lien entre les données provenant de plusieurs sources, sans avoir davantage de visibilité sur d'autres données personnelles concernant la santé. De plus, la TTP de Codification ne peut pas être impliquée en tant que responsable du traitement des données pour utilisation secondaire. Les actions effectuées par cette TTP sont décrites dans cette note comme la première étape du processus d'anonymisation et de pseudonymisation.
- **TTP d'anonymisation/pseudonymisation :** La même note du CSI mentionne également une deuxième TTP, à savoir la TTP d'anonymisation/pseudonymisation. Outre les actions de la TTP de Codification, cet acteur effectue des étapes qui anonymisent ou pseudonymisent d'autres données personnelles afin de réduire le risque d'identification de l'individu sur l'ensemble des données (par exemple, modifier un âge exact de 42 ans en une catégorie '40-45 ans'). À cet égard, il est également tenu compte du fait que l'ensemble des données ne peut être lié à des données supplémentaires qui augmentent le risque d'identification. Il est important de mentionner ici que, selon la nouvelle vision de la politique des registres, ces étapes supplémentaires d'anonymisation et de pseudonymisation ne doivent plus être effectuées par une partie distincte. Selon la nouvelle vision, ces données sont, si nécessaire, déjà rendues disponibles à la source de manière aussi anonymisée et/ou pseudonymisée que possible (c'est-à-dire le data holder ou l'intermediation entity), où l'efficacité des techniques appliquées et le risque résiduel peuvent encore être évalués par une partie indépendante au moyen d'un contrôle SCRA.
- **Contrôle SCRA :** Ce contrôle **évalue le risque d'identification d'un individu** sur base de données disponibles. Ce contrôle est rendu possible en utilisant une Small Cell Risk Analysis (SCRA) théorique ou analyse des 'petites cellules'. Cette analyse évalue les étapes d'anonymisation et de pseudonymisation qui ont été prises pour remplacer les valeurs (par exemple, par des agrégations en catégories, des abstractions, des décalages temporels, …) des données indirectement identifiables (par exemple, adresse, date de naissance, ...) et des données sensibles (par exemple, poids et taille par l'IMC) où c'est possible et adapté aux besoins d'utilisation. Ce contrôle est effectué en utilisant les métadonnées des données elles-mêmes et mises à disposition. Ces métadonnées permettent de comprendre les paramètres qui sont échangés (par exemple, poids, taille, âge, etc.), la forme (codé ou non codé), le nombre de valeurs du paramètre (par exemple, sexe à 2, âge à 120) et cetera. L'acteur qui effectue cette étape n'a donc pas besoin d'avoir accès aux données elles-mêmes et n'a donc jamais connaissance de données directement identifiables.

6 https://www.ehealth.fgov.be/ehealthplatform/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/ab0f165a4111f57011b1ca8e5d901da6babafaa0/healthdata.be-note.pdf

DEMANDES DE DONNÉES DE SANTÉ

- **Catalogue des ensembles de données :** Le catalogue des ensembles de données dans la vision de la politique des registres fournit un aperçu des **registres existants et des champs de données** qui peuvent être demandés par les data users potentiels via la plateforme de demande. Le catalogue des ensembles de données comprend des informations sur les données disponibles et les **conditions** associées, **les normes** utilisées et la manière dont la **confidentialité et la sécurité** sont garanties.
- **Plateforme de demande :** La plateforme de demande fournit une **plateforme technique** qui facilite toutes les activités liées aux demandes pour des registres et aux demandes de données. Cette plateforme peut cependant être composée de différents composants et/ou technologies. Cela inclut notamment la fourniture du catalogue des ensembles de données, qui offre un aperçu de toutes les données (de registre) disponibles, et le soutien de l'ensemble du processus de demande de données de santé.

TRAITEMENT DES DONNÉES DE SANTÉ

Secure Processing Environment (SPE) : Les Secure Processing Environments sont un élément essentiel pour la réception et le traitement des données de santé par les data users. Ces environnements sont spécifiquement conçus pour mettre ces données à disposition des data users de **manière sécurisée et contrôlée**. Dans un SPE, les data users peuvent effectuer des analyses sur les données demandées sans obtenir un accès direct aux données brutes. Les SPE garantissent que **l'échange automatisé de données** se déroule dans un environnement conforme à des **normes de sécurité strictes** et respectant **la législation en vigueur sur la protection de la vie privée**, et assurant une **gestion stricte des accès**.

C. Rôles dans le cadre de la nouvelle politique des registres en Belgique

1. APERÇU

Nous distinguons 10 rôles différents dans la nouvelle politique des registres. Ceux-ci sont représentés dans la Figure 2, y compris les responsabilités associées. Le même code de couleur que pour la Figure 1 a été utilisé, à savoir vert pour les fournisseurs de données, bleu pour les registres et jaune pour les demandes de données dans l'EHDS. La section suivante décrit l'affectation concrète de ces rôles, tandis que le chapitre suivant approfondira la description et les responsabilités associées et les éléments techniques essentiels. **Ces rôles proposés sont étroitement alignés sur les rôles définis dans le contexte EHDS, ce qui permet à la politique des registres de s'intégrer pleinement dans les structures et la gouvernance proposées par le règlement EHDS.**

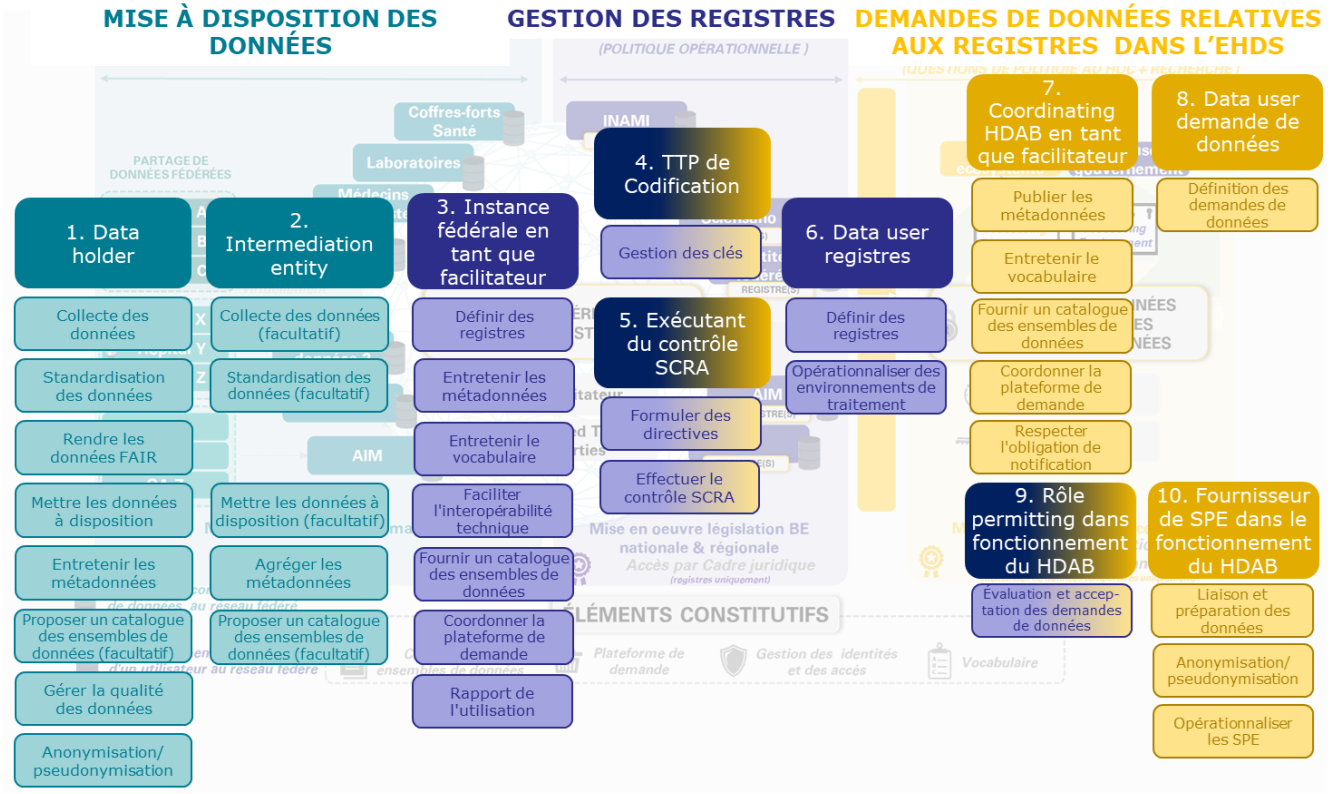

Figure 2: Représentation schématique des rôles et responsabilités dans le cadre de la nouvelle politique des registres en Belgique

2. AFFECTATION DES RÔLES DANS LA NOUVELLE POLITIQUE DES REGISTRES EN BELGIQUE

Le tableau ci-dessous présente l'affectation concrète des différents rôles nécessaires pour la mise en œuvre opérationnelle de la future politique des registres dans la pratique.

Les rôles de la politique des registres sont alignés autant que possible sur le règlement EHDS. Il est donc logique que plusieurs rôles soient attribués à la HDA. Cela ne signifie pas que la HDA doit ou peut assumer elle-même toutes les activités liées à ces rôles, mais qu'elle en organisera la gestion.

Le tableau ci-dessous présente **un aperçu des rôles définis et des acteurs impliqués** dans la politique des registres en Belgique.

	Affectation des rôles [cardinalité]
1. Data holder [n]	Hôpitaux, médecins généralistes, laboratoires, coffres-forts de données de santé, institutions de recherche, institutions publiques de santé...
2. Intermediation entity [n]	Réseaux de données, ...
3. Instance fédérale en tant que facilitateur des registres [1]	HDA
4. TTP de Codification [1... n]	eHealth, KSZ, ...
5. Exécutant du contrôle SCRA [1]	HDA
6. Data user registre [n]	Institutions publiques de santé et autres users avec base juridique
7. Coordinating HDAB en tant que facilitateur des demandes de données dans l'EHDS [1]	HDA
8. Data user demande de données dans l'EHDS [n]	Réf. utilisateurs dans le contexte EHDS
9. Rôle permitting dans le fonctionnement du HDAB [1 ... n]	Suivi de la désignation dans le contexte EHDS
10. Fournisseur de SPE dans le fonctionnement du HDAB [1 ... n]	Suivi de la désignation dans le contexte EHDS

Table 1: Affectation des rôles dans le cadre de la nouvelle politique des registres en Belgique

D. Description détaillée des rôles dans le cadre de la nouvelle politique des registres

Ce chapitre approfondit chaque rôle dans la nouvelle politique des registres. Cela se fait à l'aide d'une **fiche unique** par rôle, qui fournit une description détaillée de (1) la **description** concrète du rôle, (2) les **tâches et responsabilités** spécifiques associées au rôle et (3) les **éléments techniques essentiels** sous-jacents aux rôles. Pour chaque rôle, la description indique également la **cardinalité** de ce rôle.

1. DATA HOLDER

Description du rôle

Les data holders sont des parties qui **collectent et traitent des données de santé** électroniques pour (1) la dispensation des soins de santé ou (2) des objectifs dans les domaines de la santé publique, des remboursements, de la recherche et de l'innovation, de l'élaboration de politiques, des statistiques officielles, de la sécurité des patients ou de la réglementation. Cette définition est analogue à celle des data holders dans le cadre du règlement EHDS. Des **exemples** de data holders dans la politique des registres (et donc dans le règlement EHDS) incluent les hôpitaux et/ou réseaux de données, laboratoires, médecins (généralistes), l'AIM, entreprises pharmaceutiques, compagnies d'assurances privées, institutions de recherche mais aussi les institutions publiques de santé elles-mêmes.

Cardinalité : Multiple

Tâches et responsabilités

- **Collecte des données :** *La collecte des données comprend l'enregistrement précis et minutieux des informations pertinentes sur les patients et les services de soins de santé par les professionnels de santé dans les hôpitaux, laboratoires, cabinets de médecins généralistes, ... Cela inclut la collecte de données sur les antécédents médicaux, les traitements, les médicaments, les résultats de laboratoire et d'autres informations cliniques pertinentes, de préférence dans le DPI.*
- **Standardisation des données :** *Mettre en œuvre et maintenir une nomenclature et des normes uniformes pour l'enregistrement, le stockage et l'échange de données de santé afin de garantir que les données soient cohérentes et interopérables entre différents systèmes et établissements de soins. L'application de ces normes doit se faire autant que possible à la source, c'est-à-dire chez le data holder lui-même. Les nomenclatures et normes importantes dans ce cadre incluent OMOP, SNOMED CT, ICD-10/11, ...*
- **Rendre les données FAIR :** *Les données récoltées et stockées doivent être Findable, Accessible, Interoperable et Reusable (FAIR). Concrètement, les données doivent être stockées et documentées de manière structurée et uniforme, afin qu'elles puissent être facilement trouvées, accessible, utilisées et réutilisées par les prestataires de soins, les autorités et d'autres parties prenantes dans le domaine des soins de santé. Pour rendre les données FAIR, la mise en œuvre doit également se faire autant que possible à la source ou chez le data holder lui-même.*
- **Mettre les données à disposition :** *Les données de santé doivent être récoltées, traitées et préparées de manière accessible et structurée par le data holder, afin qu'elles puissent être consultées, utilisées et analysées par d'autres prestataires de soins, autorités et parties prenantes dans le domaine des soins de santé. Cela inclut la mise en œuvre de normes d'échange telles que FHIR. Les normes d'échange à suivre sont déterminées par le facilitateur afin de garantir l'interopérabilité technique avec d'autres systèmes.*

- **Entretenir les métadonnées :** *Élaborer et entretenir des informations sur les champs de données mis à disposition selon la norme de* ***métadonnées HealthDCAT-AP****. Cela inclut la définition d'informations descriptives sur les données, telles que leur signification, leur source, leur format, leurs droits d'accès et les normes utilisées. Cela ne relève pas uniquement de la responsabilité du data holder, mais d'autres rôles (intermediation entity, facilitateur, coordinating HDAB) seront également impliqués dans la publication de métadonnées actuelles*[7]*.*
- **Proposer un catalogue des ensembles de données (facultatif) :** *Créer et tenir à jour un catalogue structuré des ensembles de données de santé disponibles chez le data holder. Ce catalogue comprend des informations sur les données disponibles, les normes utilisées et les mesures de confidentialité et de sécurité. L'élaboration d'un tel catalogue au niveau local semble appropriée pour avoir une vue claire des (méta)données du data holder. Ces catalogues locaux peuvent ensuite être reliés au catalogue des ensembles de données de l'intermediation entity (le cas échéant) et/ou du facilitateur.*
- **Gérer la qualité des données :** *Gérer la qualité des données comprend la surveillance, la description et la documentation de l'exactitude, de l'exhaustivité et de la cohérence des données récoltées, ainsi que l'identification des erreurs ou incohérences.* ***Cette activité est alignée sur l'exigence du règlement EHDS selon laquelle les data holders doivent documenter la qualité de leurs données.***
- **Anonymisation et/ou pseudonymisation des données :** *Éliminer, transformer ou remplacer (par exemple, modifier un âge exact de 42 ans en une catégorie '40-45 ans') les informations identifiantes dans les données de santé avant de les mettre à disposition des data users, afin de garantir la protection de la vie privée des individus. Cette responsabilité est assumée par les data holders à la source. Les activités relevant de cette responsabilité font directement référence aux activités reprises dans la note du CSI, mentionnées dans le glossaire, et qui sont aujourd'hui partiellement reprises par la TTP d'anonymisation/de pseudonymisation. Pour la pseudonymisation ultérieure des données personnelles identifiables telles que le numéro NISS, il sera fait appel à la TTP de codification et aux services qu'elle propose (voir plus loin).* ***Cette vision est conforme à la position du règlement EHDS, selon laquelle ces activités doivent être effectuées autant que possible à la source.***

Éléments techniques essentiels

- **DPI :** *Le DPI est le dossier patient informatisé dans lequel toutes les informations médicales des patients sont récoltées et documentées numériquement par les prestataires de soins. Il s'agit du point de contact central pour l'état de santé des patients. En ce qui concerne la politique des registres, le DPI évolue vers un dossier patient intégré , basé sur les principes du BIHR tels qu'inclus dans le plan d'action eHealth, dans lequel le DPI agit comme une source de données importante tant pour les registres que pour les demandes de données.*
- **IAM interne :** *Le composant IAM interne (Identity & Access Management) garantit que l'organisation derrière l'utilisateur est reconnue et que le certificat ou le jeton approprié peut être inclus avec le composant IAM externe. Ce composant IAM interne dépend toujours des parties concernées, ce qui signifie que sa mise en œuvre peut varier d'une organisation à l'autre.*

[7] *Les data holders fournissent des métadonnées pour les données de santé qu'ils fournissent, l'intermediation entity (IE) agrège les métadonnées des data holders qui sont liées à l'IE, le facilitateur publie les métadonnées sur la plateforme de demande en fonction des demandes de registres et le coordinating HDAB publie les métadonnées sur la plateforme de demande en fonction des demandes de données temporaires par le grand public.*

- **IAM externe :** *Le composant IAM externe identifie, authentifie et autorise toutes les parties autorisées sur base d'un certificat ou d'un jeton de l'utilisateur fourni par le composant IAM interne. Concrètement, le composant IAM externe permet aux utilisateurs de toutes les parties autorisées de se connecter, entre autres, au metadata management tool, à la plateforme de demande,... et les droits sont déterminés via la plateforme eHealth, afin qu'ils aient accès aux tools nécessaires.*
- **Data input tool :** *Dans le data input tool, les données peuvent être saisies et stockées via un formulaire. En plus du DPI, ces données peuvent également servir de source de données pour la saisie du data management tool.*
- **Data management tool :** *Le data management tool sert comme une plateforme de données où les données peuvent être téléchargées et stockées, et où des transformations peuvent être effectuées sur ces données. Les connexions automatiques aux sources de données et les pipelines ETL (Extract Transform Load) peuvent y être configurés. De plus, des standardisations et des ajustements peuvent être effectués pour rendre les données plus FAIR.*
- **Metadata management tool :** *Dans ce tool, les utilisateurs peuvent compléter, modifier, ajouter et tenir à jour des métadonnées. Les métadonnées devraient garantir que les registres et les données de santé mises à disposition sont trouvables, accessibles, interopérables et réutilisables (FAIR). Les métadonnées sont d'abord documentées auprès du data holder, éventuellement consolidées par l'intermediation entity (IE) le cas échéant , puis récupérées et complétées par le facilitateur.*
- **Data gateway :** *Les données sont mises à disposition par le composant data gateway chez le data holder, lorsque les données sont demandées depuis l'environnement de traitement ou le SPE pour les demandes de données. Ce composant permet de récupérer des données dans un format standardisé (par exemple, par des appels API), c'est-à-dire le 'pull' des données. En ayant ce composant chez le data holder (source des données), la version la plus récente des données est transmise et cela contribue à un système de données décentralisé. Cela diffère du fonctionnement actuel, où les données sont transmises à un processeur via un service ou un formulaire, c'est-à-dire le 'push' des données.*

  Outre la mise à disposition des données pour l'élaboration des registres, le gateway peut également donner accès à des données agrégées et de benchmarking relatives aux données mises à disposition. De cette manière, cela offre des avantages supplémentaires au data holder pour acquérir des connaissances, ce qui est particulièrement intéressant pour par exemple les hôpitaux.
- **Catalogue des ensembles de données (facultatif) :** *Le catalogue des ensembles de données est un inventaire centralisé des données disponibles. Il offre des fonctionnalités telles que la recherche et le filtrage, ce qui rend les données faciles à trouver et accessibles*
- **Service pour l'anonymisation/pseudonymisation :** *Le service pour la pseudonymisation des données limite le risque de réidentification et prévoit l'exécution de techniques pour remplacer les valeurs des données indirectement identifiables (par exemple, adresse, date de naissance, ...) et des données sensibles (par exemple, poids, taille, …). Cela se fait autant que possible chez le data holder lui-même dans le data management tool. Cette vision est conforme à la note du CSI*[8] *dans laquelle l'anonymisation ou la pseudonymisation a lieu le plus tôt possible dans la chaîne.*

8 https://www.ehealth.fgov.be/ehealthplatform/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/ab0f165a4111f57011b1ca8e5d901da6babafaa0/healthdata.be-note.pdf

Pour cela, le data holder doit partiellement faire appel aux services proposés par eHealth, notamment le Batch codage en ce qui concerne les données directement identifiables.

2. INTERMEDIATION ENTITY

Description du rôle

Les intermediation entities déchargeront **partiellement les data holders** en reprenant des tâches spécifiques. Ainsi, les intermediation entities peuvent, par exemple, assurer l'**agrégation ou la standardisation** des données, là où les data holders individuels ne dispose pas toujours de la capacité et de l'expertise nécessaires pour le faire eux-mêmes. Pour le fonctionnement concret de l'intermediation entity, il faudra examiner si elle opérera localement chez les data holders eux-mêmes, ou si elle va plutôt agréger les données au sein de leurs propres systèmes et les rendre accessibles à partir de là. Les intermediation entities peuvent à la fois **stocker et traiter efficacement** les données des data holders et **gérer uniquement les métadonnées**. Les réseaux de données de santé sont un **exemple** d'intermediation entities. **Cette définition est conforme à la définition du règlement EHDS pour les intermediation entities. À cet égard, le règlement stipule que ces entités reprennent des tâches spécifiques de certaines catégories de data holders, dans le but de réduire la charge administrative pesant sur les data holders et de soutenir l'objectif d'efficacité et d'effectivité. En pratique, les intermediation entities sont en mesure de traiter les données de santé et de les mettre à disposition pour une utilisation secondaire, sur la base des données fournies par les data holders. Conformément au règlement EHDS, il est interdit à une intermediation entity d'agir en tant que HDAB.**

Cardinalité : Multiple

Tâches et responsabilités

- **Collecte, standardisation & mise à disposition des données (optionnel) :** *La collecte, la standardisation et la mise à disposition des données pour utilisation primaire et secondaire, comme indiqué dans le règlement EHDS. Cependant, l'affectation effective pourrait varier selon le type de partie prenante. Si l'intermediation entity joue un rôle à cet égard, elle peut, dans le cadre de la politique des registres, contribuer à la mise à disposition des données pour l'élaboration des registres et répondre aux demandes de données dans l'EHDS.*
- **Agrégation des métadonnées :** *Agréger et communiquer au facilitateur les métadonnées des data holders associés à l'intermediation entity. Si les data holders ne disposent pas des capacités et des connaissances suffisantes, les intermediation entities peuvent apporter un soutien supplémentaire pour créer elles-mêmes les métadonnées et s'assurer qu'elles répondent aux normes requises (par exemple, formatage selon la norme HealthDCAT-AP).*
- **Fournir un catalogue des ensembles de données (facultatif) :** *La création et la mise à jour d'un catalogue structuré des ensembles de données de santé disponibles à partir des data holders associés à l'intermediation entity. Le catalogue des ensembles de données comprend des informations sur les données disponibles, les normes utilisées et la manière dont la confidentialité et la sécurité sont garanties. La création d'un tel catalogue des ensembles de données au niveau local semble appropriée afin d'avoir une vue d'ensemble des (méta)données dont dispose l'intermediation entity. Ces catalogues des ensembles de données locaux peuvent ensuite être liés au catalogue des ensembles de données du facilitateur.*

Éléments techniques essentiels

- **IAM interne :** *Le composant IAM interne (Identity & Access Management) garantit que l'organisation derrière l'utilisateur est reconnue et que le certificat ou le jeton approprié peut être inclus avec le composant IAM externe. Ce composant IAM interne dépend toujours des parties concernées, ce qui signifie que sa mise en œuvre peut varier d'une organisation à l'autre.*

- **IAM externe :** *Le composant IAM externe identifie, authentifie et autorise toutes les parties autorisées sur base d'un certificat ou d'un jeton de l'utilisateur fourni par le composant IAM interne. Concrètement, le composant IAM externe permet aux utilisateurs de toutes les parties autorisées de se connecter, entre autres, au metadata management tool, à la plateforme de demande,... et les droits sont déterminés via la plateforme eHealth, afin qu'ils aient accès aux tools nécessaires.*
- **Metadata management tool :** *Dans ce tool, les utilisateurs peuvent compléter, modifier, ajouter et mettre à jour des métadonnées. Les métadonnées devraient garantir que les registres et les données de santé mises à disposition sont trouvables, accessibles, interopérables et réutilisables (FAIR). Les métadonnées sont d'abord documentées avec l'IE, puis sont récupérées et complétées par le facilitateur.*
- **Catalogue des ensembles de données (facultatif) :** *Le catalogue des ensembles de données est un inventaire centralisé des données disponibles. Il offre des fonctionnalités telles que la recherche et le filtrage, ce qui rend les données faciles à trouver et accessibles.*

3. INSTANCE FÉDÉRALE EN TANT QUE FACILITATEUR DES REGISTRES

Description du rôle

L'instance fédérale, en tant que facilitateur, soutient l'utilisation des registres et veille à ce que ceux-ci soient accessibles de manière simple et automatisée.

. Dans son fonctionnement, le facilitateur publie, entre autres, un **catalogue des ensembles de données** qui fournit des informations sur tous les registres disponibles. De plus, le facilitateur collabore étroitement avec les parties prenantes et le terrain afin d'aboutir, sur base d'une expertise partagée, à des **accords et des directives** concernant, entre autres, les normes.

Cardinalité : Un

Tâches et responsabilités

- **Définir les registres :** *Les données des registres sont récupérées autant que possible à partir du **dossier patient informatisé** (DPI). Le facilitateur se concerte avec le(s) data user(s) du registre pour déterminer quels champs de données sont nécessaires à l'élaboration du registre en fonction des finalités d'utilisation. L'élaboration d'un registre repose toujours sur une base juridique .*
- **Tenir à jour les métadonnées :** *Création et mise à jour des informations sur les champs de données qui composent les registres selon la norme de métadonnées HealthDCAT-AP. Cela inclut la définition d'informations descriptives sur les données, telles que leur signification, leur source, leur format, leurs droits d'accès, les normes utilisées et la qualité des données. En pratique, le facilitateur reçoit les métadonnées des data holders et des intermediation entities pour les registres disponibles et les agrégera. La mise à jour et la documentation des métadonnées selon la norme HealthDCAT-AP relèvent de la responsabilité du coordinating HDAB conformément au règlement EHDS.*
- **Gérer les accords d'interopérabilité sémantique :** *Gérer, adapter et tenir à jour la terminologie, les classifications à utilisation secondaire et celles utilisées pour enregistrer les données de registre. Cela permet de clarifier quelle signification et quelle définition sont attribuées aux données. Ce vocabulaire est complété par le coordinating HDAB pour les demandes de données, afin d'assurer l'alignement entre l'utilisation secondaire et l'alignement avec le niveau européen. En outre, on s'appuie également sur la gestion de l'interopérabilité sémantique dans le domaine technique par eHealth et la norme sémantique (par exemple, SNOMED CT, ICD-10, etc.) par le SPF SPSCAE.*
- **Appliquer les accords d'interopérabilité technique :** *L'application des accords qui stimulent l'interopérabilité technique, tels que la définition des normes d'échange technique (par exemple, FHIR) qui doivent être utilisées pour assurer un échange de données fluide et efficace. Ici aussi, on se base sur la gestion de telles normes d'échange par eHealth.*
- **Fournir un catalogue des ensembles de données :** *Créer et tenir à jour un catalogue structuré des ensembles de données de registre disponibles. Le catalogue des ensembles de données contient des informations sur les données disponibles et les conditions, les normes utilisées et la manière dont la confidentialité et la sécurité sont garanties. Le facilitateur agrège les catalogues des ensembles de données des data holders et des intermediation entities pour les registres disponibles.*
- **Coordonner la plateforme de demande pour les registres (facultatif) :** *La coordination de la plateforme de demande dans laquelle les data users des registres peuvent consulter divers*

éléments essentiels tels que le catalogue des ensembles de données, le vocabulaire et la politique d'utilisation et récupérer les registres via une demande simple et automatique.

- **Rapport d'utilisation :** *Rapport sur les activités du facilitateur et l'utilisation effective (et l'élaboration) des registres par (pour) les data users des registres. Ceci est conforme aux dispositions juridiques selon lesquelles il faut pouvoir rapporter sur l'utilisation des données à des fins secondaires. Selon les dispositions dans l'EHDS et selon la législation nationale.*

Éléments techniques essentiels

- **IAM interne :** *Le composant IAM interne (Identity & Access Management) garantit que l'organisation derrière l'utilisateur est reconnue et que le certificat ou le jeton approprié peut être inclus avec le composant IAM externe. Ce composant IAM interne dépend toujours des parties concernées, ce qui signifie que sa mise en œuvre peut varier d'une organisation à l'autre.*
- **IAM externe :** *Le composant IAM externe identifie, authentifie et autorise toutes les parties autorisées sur base d'un certificat ou d'un jeton de l'utilisateur fourni par le composant IAM interne. Concrètement, le composant IAM externe permet aux utilisateurs de toutes les parties autorisées de se connecter, entre autres, au metadata management tool, à la plateforme de demande, ... et les droits sont déterminés via la plateforme eHealth, afin qu'ils aient accès aux tools nécessaires.*
- **Metadata management tool :** *Dans ce tool, les utilisateurs peuvent compléter, modifier, ajouter et mettre à jour des métadonnées. Les métadonnées doivent garantir que les registres et les données de santé mises à disposition sont trouvables, accessibles, interopérables et réutilisables (FAIR). Les métadonnées sont d'abord documentées auprès de l'intermediation entity (IE) le cas échéant, puis sont récupérées et complétées auprès du facilitateur.*
- **Catalogue des ensembles de données :** *Le catalogue des ensembles de données est un inventaire centralisé des données disponibles et des registres qui ont été rendus accessibles. Il offre des fonctionnalités telles que la recherche et le filtrage, ce qui rend les données faciles à trouver et accessibles. Ce catalogue des ensembles de données doit combiner et consolider toutes les informations disponibles dans les catalogues des data holders et des intermediation entities, afin qu'un catalogue national unique existe, dans lequel les informations sont présentées de manière consolidée. Il s'agit du même catalogue que celui décrit plus tard dans « 7. Coordinating HDAB en tant que facilitateur des demandes de données dans l'EHDS ».*
- **Plateforme de demande (facultatif) :** *La plateforme de demande offre un environnement où les data users peuvent soumettre des demandes de nouveaux registres, et où ces demandes peuvent être gérées. Les data users des registres obtiennent accès sur base d'une base juridique. Lorsqu'une plateforme de demande est proposée, il est préférable d'utiliser le même module que celui mentionné dans « 7. Coordinating HDAB en tant que facilitateur des demandes de données dans l'EHDS ».*

4. TTP DE CODIFICATION

Description du rôle

Cette Trusted Third Party (TTP) est responsable de la codification des **données directement identifiables** (par exemple, le numéro NISS, nom, ...) champ par champ au moyen d'un chiffrement avec des clés gérées par la TTP, et offre la possibilité de chiffrer d'autres données dans leur ensemble. Cela s'aligne avec la manière dont les activités sont décrites aujourd'hui pour la TTP de Codification et la première étape dans la note du CSI mentionnée précédemment dans le glossaire.

Cardinalité : Multiple

Tâches et responsabilités

- **Gestion des clés :** *La gestion en toute sécurité des clés et la codification des données pour garantir la confidentialité et l'intégrité des données de santé échangées. Cette responsabilité est assumée par la TTP de Codification qui est chargée de conserver les clés permettant d'établir le lien entre les données originales et les données mises à disposition des data users.*

Éléments techniques essentiels

- **Service de codification :** *Le service de codification est responsable pour le chiffrement des données directement identifiables (par exemple, numéro de registre national, ...) au niveau du champ avec des clés gérées par la TTP de Codification. De plus, le service offre la possibilité de chiffrer d'autres ensembles de données dans leur intégralité, ce qui contribue à la sécurité et à la confidentialité des données.*

5. EXÉCUTANT DU CONTRÔLE SCRA

Description du rôle

L'exécutant du contrôle SCRA évalue le risque d'identification d'un individu en exécutant un contrôle SCRA et fournit des directives pour éviter ce risque, en utilisant des techniques pour remplacer les valeurs (par exemple, via des agrégations en catégories, des abstractions, des décalages temporels, …) de **données indirectement identifiables** (par exemple, adresse, date de naissance, ...) et de données sensibles (par exemple, poids, IMC, ...). Cet acteur n'a pas accès aux données elles-mêmes échangées pour l'exécution de ses responsabilités, mais utilise uniquement les métadonnées nécessaires (voir contrôle SCRA dans le glossaire).

Cardinalité : Un

Tâches et responsabilités

- **Formuler les directives :** *La formulation des directives pour le data holder et le fournisseur de SPE afin de prévoir l'anonymisation et la pseudonymisation des données de santé mises à disposition. L'exécutant du contrôle SCRA agit en tant qu'organe de contrôle et de supervision, dans lequel le data holder à la source (pour les données individuelles) et le fournisseur de SPE dans le SPE (pour les données agrégées) sont responsables des activités concernées.*
- **Exécuter le contrôle SCRA :** *L'évaluation et l'identification des risques de sécurité potentiels et des problèmes d'intégrité des données liés aux petites cellules de données dans les données de santé qui sont mises à la disposition des data users. Concrètement, l'exécutant du contrôle SCRA exécutera un contrôle SCRA lors de la mise à disposition des données, afin de valider l'anonymisation/pseudonymisation réalisée par le data holder, la TTP de Codification et/ou le fournisseur SPE. Si l'analyse SCRA donne un avis négatif, une nouvelle pseudonymisation sera à nouveau effectuée chez le data holder à partir de la source.*

Éléments techniques essentiels

- **Service SCRA** : *Dans le cadre du service SCRA, on vérifie que la réidentification de petits groupes est évitée. Cela peut être réalisé par une SCRA théorique (faire une prédiction de risque à l'aide des valeurs théoriques par variable) ou une SCRA quantitative (faire une prédiction de risque à l'aide des différentes valeurs réelles par variable). L'exécutant du contrôle SCRA se concentrera presque exclusivement sur la SCRA théorique lorsque les données seront rendues accessibles dans un SPE, car aucun accès aux données elles-mêmes n'est requis pour cela.*

6. DATA USER REGISTRES

Description du rôle

Les data users des registres sont des **parties autorisées** au sein du réseau qui ont accès à la **plateforme de demande** pour demander des registres. Ils n'ont accès qu'aux registres pour lesquels ils disposent de la base juridique nécessaire et qu'ils peuvent recevoir de manière sécurisée afin de les traiter aux fins fixées. Les registres doivent toujours être configurés dans un **cadre juridique**. L'accès à un registre est possible dès qu'un data user remplit les **conditions requises.**

Des **exemples** d'entités qui agissent dans la pratique en tant que data user des registres sont, entre autres, l'INAMI, le SPF SPSCAE, l'IAM, Sciensano et les entités fédérées. Dans certains cas, des associations scientifiques ou des universités peuvent également agir comme data user d'un registre si elles reçoivent un mandat attribué par une institution publique de santé.

Cardinalité : Multiple

Tâches et responsabilités

- **Définir les registres :** *Les données des registres sont extraites autant que possible du **dossier patient informatisé** (DPI). **Le data user définit quelles données sont nécessaires pour atteindre l'objectif ou les objectifs fixés.** Le facilitateur peut soutenir le(s) data user(s) de registre en indiquant quels champs de données sont déjà disponibles pour l'élaboration du registre en fonction des fins d'utilisation. On évalue si une base juridique issue la législation belge ou d'autres législations européennes est utilisée.*
- **Opérationnalisation des environnements de traitement :** *La réception des registres par les data users s'effectue dans un propre environnement de traitement, que le data user de registre exploite localement. Ces environnements de traitement sont des environnements sécurisés, situés chez le data user lui-même et qui garantissent l'utilisation sécurisée et le traitement des registres. Les données atterrissent dans les environnements de traitement sous forme chiffrée (cryptée), où le décryptage n'a lieu qu'après la validation automatisée de la SCRA théorique par l'exécutant du contrôle SCRA.*

Éléments techniques essentiels

- **IAM interne :** *Le composant IAM interne (Identity & Access Management) garantit que l'organisation derrière l'utilisateur est reconnue et que le certificat ou le jeton approprié peut être inclus avec le composant IAM externe. Ce composant IAM interne dépend toujours des parties concernées, ce qui signifie que sa mise en œuvre peut varier d'une organisation à l'autre.*
- **IAM externe :** *Le composant IAM externe identifie, authentifie et autorise toutes les parties autorisées sur base d'un certificat ou d'un jeton de l'utilisateur fourni par le composant IAM interne. Concrètement, le composant IAM externe permet aux utilisateurs de toutes les parties autorisées de se connecter, entre autres, au metadata management tool, à la plateforme de demande, ... et les droits sont déterminés via la plateforme eHealth, afin qu'ils aient accès aux tools nécessaires.*
- **Environnement de traitement :** *L'environnement de traitement chez le data user lui-même permet de disposer d'un environnement de traitement pour la réception sécurisée et le traitement des données des registres. Pour chaque data user, c'est-à-dire l'organisation ou les organisations qui soumettent une demande, un tel environnement de traitement sera mis en place. Les data users des registres devront donc les stocker eux-mêmes. Un tel environnement*

de traitement permettra, si nécessaire, de demander de nouvelles données aux data holders via les data gateways et de les traiter dans leur propre environnement.

7. COORDINATING HDAB EN TANT QUE FACILITATEUR POUR LES DEMANDES DE DONNÉES DANS L'EHDS

Description du rôle

Le coordinating HDAB en tant que facilitateur soutient l'**utilisation temporaire** des données de santé, et coordonne les demandes de données via la plateforme de demande. Dans son fonctionnement, le coordinating HDAB publie, entre autres, un **catalogue des ensembles de données** qui fournit des informations sur toutes les données de santé disponibles. **Le coordinating HDAB dans le cadre de la politique des registres est la même entité que le coordinating HDAB selon le règlement EHDS et fonctionne donc de manière transversale, en s'appuyant sur des blocs de construction communs.**

Cardinalité : Un

Tâches et responsabilités

- **Publier les métadonnées :** *Comme indiqué précédemment, les data holders doivent créer et entretenir des métadonnées pour les champs de données mis à disposition conformément à la norme de métadonnées HealthDCAT-AP.* ***Le coordinating HDAB en tant que facilitateur publie ensuite les métadonnées dans la plateforme de demande en fonction de la demande de données temporaires.*** *En outre, un rôle de facilitateur est attribué au coordinating HDAB pour soutenir l'élaboration de métadonnées chez les data holders, par exemple en formulant des directives et des bonnes pratiques relatives à l'élaboration des métadonnées.*
- **Entretenir le vocabulaire :** *Adapter et mettre à jour la terminologie, les classifications et les systèmes de codification utilisés pour documenter, inventorier et rendre disponibles les données de santé.* ***Ce vocabulaire est encore enrichi par le coordinating HDAB en tant que facilitateur pour les demandes de données, afin d'encourager l'alignement en matière d'utilisation secondaire et l'alignement avec le niveau européen.***
- **Fournir un catalogue des ensembles de données :** *La création et la mise à jour d'un catalogue structuré des ensembles de données de santé disponibles. Le catalogue des ensembles de données comprend des informations sur les données disponibles et les conditions, les normes utilisées et la manière dont la confidentialité et la sécurité sont garanties. Le coordinating HDAB en tant que facilitateur pour les demandes de données, fournit un catalogue fédéré contenant des informations sur toutes les données de santé disponibles. Cela se fait par l'agrégation des données du catalogue des data holders et des intermediation entities.* ***Ce catalogue des ensembles de données est intégré dans le catalogue des ensembles de données général et central du coordinating HDAB.***
- **Coordonner la plateforme de demande pour les demandes de données dans l'EHDS :** *La coordination de la plateforme de demande dans laquelle les data users de demandes de données peuvent consulter différents éléments essentiels tels que le catalogue des ensembles de données, le vocabulaire et la politique d'utilisation et demander des données de santé via une demande manuelle, sur base d'un formulaire d'information détaillé.*
- **Respecter l'obligation de notification :** *Communiquer publiquement toutes les demandes reçues et traitées dans la plateforme de demande, y compris les décisions de fournir ou non des données. Ces informations sont complétées par l'utilisation rapportée par le facilitateur pour les registres.* ***La responsabilité liée à l'obligation de notification repose sur l'obligation des HDAB, conformément au règlement EHDS, qui stipule que les HDAB doivent rapporter tous les deux ans toutes les demandes reçues.***

Éléments techniques essentiels

- **Metadata management tool :** *Dans ce tool, les utilisateurs peuvent compléter, modifier, ajouter et mettre à jour des métadonnées. Les métadonnées devraient garantir que les registres et les données de santé mises à disposition sont trouvables, accessibles, interopérables et réutilisables (FAIR). Les métadonnées sont d'abord documentées auprès du data holder ou intermédiation entity (IE) le cas échéant, puis sont récupérées et complétées auprès du facilitateur.*
- **Catalogue des ensembles de données :** *Le catalogue des ensembles de données est un inventaire centralisé des données de santé disponibles et des registres qui ont été rendus accessibles. Il offre des fonctionnalités telles que la recherche et le filtrage, ce qui rend les données faciles à trouver et accessibles. Ce catalogue des ensembles de données doit combiner et consolider toutes les informations disponibles dans les catalogues des data holders et des intermediation entities, afin qu'un catalogue national unique existe, dans lequel les informations sont présentées de manière consolidée.*
- **Plateforme de demande :** *La plateforme de demande offre un environnement où les data users peuvent soumettre des demandes de données, et où ces demandes peuvent être gérées. Les data users des demandes de données obtiennent les données demandées par demande. Si la demande concerne des données individuelles, ces données sont mises à disposition via un environnement SPE pour les demandes de données, et ce pendant la période indiquée dans l'autorisation de traitement de données.*

8. DATA USER DEMANDE DE DONNÉES

Description du rôle

Les data users des demandes de données **ne participent pas directement** au réseau fédéré. Ils soumettent une **demande de données (conformément au règlement EHDS)** via la plateforme de demande, la demande est ensuite traitée par le coordinating HDAB. Dans leur demande, les data users doivent entre autres **motiver** clairement les fins spécifiques pour lesquelles ils souhaitent utiliser les données, et indiquer si les conditions établies sont remplies.

Les data users des demandes de données doivent soumettre **une nouvelle demande** auprès du coordinating HDAB pour chaque demande de données. Pour chaque demande, les données ne pourront être consultées ou reçues qu'après l'obtention d'une **décision positive de la part du HDAB**. Si une autorisation d'utilisation de données individuelles est nécessaire, cette autorisation sera évaluée dans le fonctionnement permitting du HDAB (voir plus loin) et accordée conformément au cadre juridique. Ce cadre est en principe le règlement EHDS, qui est un affinement (« lex specialis ») du RGPD, mais les alternatives peuvent aussi être des cadres juridiques spécifiques qui sont établis par des arrêtés royaux (fédéraux), des arrêtés (flamands/wallons), des ordonnances ou des règlements (Bruxelles). Les autorisations de traitement de données sont toujours **limitées dans le temps**.

Toute personne physique ou organisation peut en principe agir en tant que data user de demande de données, à condition qu'elles répondent aux critères établis. **En pratique**, les chercheurs, les décideurs politiques, les entreprises privées et les établissements de santé sont des exemples courants d'utilisateurs.

Cardinalité : Multiple

Tâches et responsabilités

- **Définir les demandes de données :** *Pour obtenir un accès temporaire aux données de santé, le data user doit soumettre une demande d'accès aux données de santé ou une demande de données de santé – selon la nature des données souhaitées, voir la définition de la demande de données dans l'EHDS au Chapitre B. ci-dessus – via la plateforme de demande. Si souhaité et si cela est pertinent, les demandes de données peuvent être établies à partir des données figurant dans un registre existant et, par exemple, complétées par un certain nombre de champs de données supplémentaires provenant ou non d'autres sources de données.*

Éléments techniques essentiels

- **/**

9. RÔLE PERMITTING DANS LE FONCTIONNEMENT DU HDAB

Description du rôle

Un HDAB doit décider si le demandeur peut obtenir accès aux données. Lorsque cela concerne l'accès à des données individuelles, une autorisation ou un permis devra être accordé. C'est pourquoi le HDAB exerce également un rôle d'entité 'permitting'. Dans le cadre de ce rôle permitting, le HDAB traitera les demandes de données de santé en soutenant la **prise de décision** concernant l'octroi ou non d'une **autorisation** (permanente ou temporaire). Actuellement, le **Comité de sécurité de l'information (CSI)** joue un rôle important en Belgique en matière de conseils sur les permis. **L'instance qui sera responsable des activités permitting dans le cadre du fonctionnement du HDAB au sein de la politique des registres est la même entité que celle relevant du règlement EHDS, et fonctionne donc de manière globale, en s'appuyant sur des blocs de construction communs.**

Cardinalité : Une ou plusieurs

Tâches et responsabilités

- **Évaluer et accorder les demandes de données : Evaluer** *les demandes et décider d'autoriser ou de refuser l'accès aux données de santé pour utilisation secondaire. Cela comprend entre autres le contrôle du respect de la réglementation en vigueur et des normes éthiques.*

Éléments techniques essentiels

- **Permit management tool :** *Le permit management tool évalue et accorde les autorisations d'accès aux données de santé contenant des données personnelles. Pour les data users des registres, c'est automatisé autant que possible conformément aux politiques d'utilisation des registres. Pour les data users des demandes de données, il y aura par contre toujours une intervention manuelle.*

10. FOURNISSEUR DE SPE DANS LE FONCTIONNEMENT DU HDAB

Description du rôle

La mise à disposition d'un SPE pour les demandes de données dans le fonctionnement du HDAB concerne la facilitation et la mise à disposition d'un **Secure Processing Environment** afin que les data users puissent recevoir et traiter des données de santé dans un environnement sécurisé. Au sein du SPE, un espace de travail séparé et sécurisé est prévu spécifiquement pour chaque demande et limité dans le temps. Le SPE lui-même est créé sans date de fin et est donc de nature continue. En fonction de la manière dont ce rôle est intégré dans le fonctionnement d'un HDAB, il est nécessaire de séparer/distinguer les équipes, les fonctions et les accès pour le traitement des données et des demandes de données, comme prévu dans le règlement EHDS[9].

Cardinalité : Un ou plusieurs

Tâches et responsabilités

- **Couplage et préparation des données :** *Préparer les données demandées pour créer des données fiables et exploitables pour les analyses, les rapports et l'élaboration de politiques. Cela inclut, entre autres, la standardisation des formats de données, la validation des données, l'association des données provenant de diverses sources et la réalisation de certaines activités supplémentaires d'anonymisation ou de pseudonymisation. Ces responsabilités sont incluses dans les tâches de processing d'un HDAB.*
- **Anonymisation et/ou pseudonymisation des données :** *Éliminer, transformer ou remplacer les informations d'identification au sein des données de santé avant de les mettre à la disposition des data users, afin d'assurer la protection de la vie privée des individus. Cette responsabilité est assumée par les data holders sur les différentes sources de données à la source, ainsi que par le HDAB dans le cadre de ses tâches liées à l'agrégation de différentes sources de données.* **Cela est conforme à la position au sein de l'EHDS selon laquelle ces activités devraient être menées à la source autant que possible.**
- **Opérationnaliser les SPE pour les demandes de données :** *La réception de données de santé par les data users à la suite d'une demande de données s'effectue dans des Secure Processing Environments (SPE) exploités par un fournisseur de SPE désigné. Au moins un SPE est prévu, mais la possibilité de créer plusieurs SPE (par exemple, par domaine de données) reste ouverte. Au sein de ces SPE, des espaces de travail temporaires séparés et sécurisés sont créés, qui s'inscrivent spécifiquement dans les finalités d'une seule demande de données, afin d'assurer l'utilisation et le traitement sécurisés des données de santé. Les données arrivent dans l'espace de travail sous forme chiffrée (cryptée), où le décryptage n'a lieu qu'après la validation automatisée de la SCRA théorique par l'exécutant du contrôle SCRA.*

Éléments techniques essentiels

- **Service pour l'anonymisation/pseudonymisation :** *Ce service limite le risque de réidentification et prévoit l'exécution de techniques pour remplacer les valeurs des données indirectement identifiables (par exemple, adresse, date de naissance, ...) et les données sensibles (par exemple, poids, IMC, ...). Comme indiqué précédemment pour le rôle de data holder, cela se fait autant que possible chez le data holder lui-même dans le data management tool. Le fournisseur de SPE n'interviendra que si une anonymisation et/ou une pseudonymisation supplémentaire s'avère*

[9] Réglement EHDS article 55 (3)

*nécessaire après le couplage des données.***SPE pour les demandes de données :** *Un SPE pour les demandes de données permet aux data users de recevoir et de traiter en toute sécurité les données de santé pour une utilisation temporaire. Ces SPE sont toujours mis en place par un fournisseur de SPE désigné qui crée un espace de travail spécifiquement dédié à chaque demande.*