

Rollen en verantwoordelijkheden voor het nieuwe registerbeleid in België

Voorliggend document kadert binnen de **verdere uitwerking en operationalisering** van de nieuwe toekomstvisie voor het registerbeleid in België, die in het najaar van 2024 door het RIZIV en de FOD VVVL werd opgemaakt (eveneens te raadplegen op de [website](#) van het RIZIV).

Om de nieuwe toekomstvisie te realiseren, zullen diverse **rollen en verantwoordelijkheden** worden toegewezen aan verschillende actoren om het gedecentraliseerde en gefedereerde registerbeleid operationeel te maken. Het huidige document omvat een **overzicht van rollen en verantwoordelijkheden** die aan de basis liggen van het nieuwe registerbeleid. Deze rollen en verantwoordelijkheden vloeien voort uit de functionele vereisten die voor het registerbeleid zijn geïdentificeerd. Vervolgens wordt uitgelegd **welke partijen** of organisaties **in de praktijk** instaan voor de invulling van de verschillende rollen voor het registerbeleid in België.

Waar relevant wordt in de nota verwezen naar de alignering van de rollen en verantwoordelijkheden binnen het registerbeleid met de **Europese EHDS (European Health Data Space) -verordening**. In de huidige analyse wordt verondersteld dat het registerbeleid deels valt onder het secundaire gebruik van gezondheidsgegevens volgens de EHDS-verordening, meer bepaald wanneer registers worden gebruikt in het kader van aanvragen die onder EHDS vallen. De uitwerking van het registerbeleid op Belgisch (inter)federaal niveau dient zodanig te voldoen aan de verplichtingen zoals uiteengezet in de EHDS-verordening, maar kan echter op bepaalde gebieden op een alternatieve wijze ingevuld worden. De verdere toelichting in de nota zal, aan de hand van een **kleurcodering**, aanduiden voor welke aspecten het registerbeleid volledig in lijn is met de verordening en waar eventuele eigenheden van het registerbeleid leiden tot geringe afwijkingen. Daar waar er verwijzingen gemaakt worden naar de EHDS-verordening en de implementatie ervan in België, is het belangrijk om aan te geven dat deze nota zich niet uitspreekt over hoe de EHDS-implementatie exact zal gebeuren. Hiervoor wordt volledig gealigneerd met de implementatie zoals vooropgesteld in het eHealth actieplan en het healthdata actieplan. De scope van deze nota beperkt zich tot het registerbeleid en de verdere alignering ervan binnen de EHDS-context.

Het is belangrijk mee te geven dat de nieuwe toekomstvisie een significante wijziging betekent ten opzichte van de huidige manier van werken voor het samenstellen, verwerken en ter beschikking stellen van registers. Daarbij worden verantwoordelijkheden herverdeeld waar ook data holders en gebruikers bijkomende verantwoordelijkheden opnemen in lijn met de EHDS-verordening. Het is dus belangrijk dit document en de daarin beschreven rollen, verantwoordelijkheden en activiteiten los te zien van hoe deze vandaag worden ingevuld. Waar mogelijk wordt een vergelijking gemaakt met de situatie van vandaag om aan te geven hoe deze verschilt ten opzichte van de toekomstvisie.

De aandacht van de lezer wordt graag gevestigd op volgende algemene opmerking. Deze nota biedt een visie op de rollen en verantwoordelijkheden voortbouwend op de momenteel best beschikbare informatie. Tegelijkertijd situeert de nota zich binnen een context van voortdurende evolutie. Zo zijn bijvoorbeeld nog niet alle verdere ontwikkelingen en beslissingen met betrekking tot de implementatie van de EHDS-verordening in België gekend. Bijgevolg moet deze nota als een dynamisch document beschouwd worden dat in de toekomst wanneer nodig en relevant verder zal worden aangepast of bijgestuurd.

Aanpassingen ten opzichte van de oorspronkelijke visie registerbeleid

In maart 2025 werd de nieuwe visie gepubliceerd en later toegelicht in een webinar¹. Vanzelfsprekend werpt dit vragen op bij de verschillende stakeholders. Ten gevolge van deze vragen en voortschrijdend inzicht, worden ook enkele aanpassingen gemaakt aan de gebruikte terminologie en voorstelling van de nieuwe visie. De visie is niet 'fixed' en evolueert mee naarmate gesprekken met stakeholders vorderen en inzichten verworven worden.

Daarom worden enkele termen uit de eerder visie aangepast en verduidelijkt, nl:

- 'Permanent register' wordt '(nieuw) register': Er wordt niet langer gesproken over een 'permanent' register. De term permanent register schept veel verwarring over de eigenlijke opzet van de registers en het gebruik ervan. In essentie zit de grootste verandering in de manier waarop gegevens zullen worden verzameld en verder beheerd worden in een register. Dit is dus voornamelijk een technologische evolutie. Het is daarbij niet zo dat data users van register (blauwe entiteiten uit figuur 1) zomaar toegang zullen hebben tot alle registers voor alle mogelijke doeleinden. Dit blijft ook onveranderd en zal net zoals vandaag worden vastgelegd en bepaald in een wettelijke basis. Er zal hier vooral meer worden ingezet om het inzichtelijk maken welke registers bestaan om zo dubbels en dubbele registratie & verwerking te vermijden. In het glossarium wordt verder ingegaan op hoe een huidig register verschilt van een nieuw register volgens de nieuwe visie.
- 'Tijdelijk register' wordt 'gegevensaanvraag binnen EHDS': Om verwarring te vermijden en alignering met de EHDS-verordening te waarborgen zal dan ook voortaan de term 'tijdelijk register' niet langer gebruikt worden. In de plaats daarvan wordt verwezen naar een 'gegevensaanvraag binnen EHDS' of kortweg 'gegevensaanvraag'. Voor het aanvragen van gegevens voor secundair gebruik zal men in België namelijk volledig aligneren met de EHDS-verordening.

¹ [Registerbeleid voor gezondheidszorggegevens | RIZIV](#)

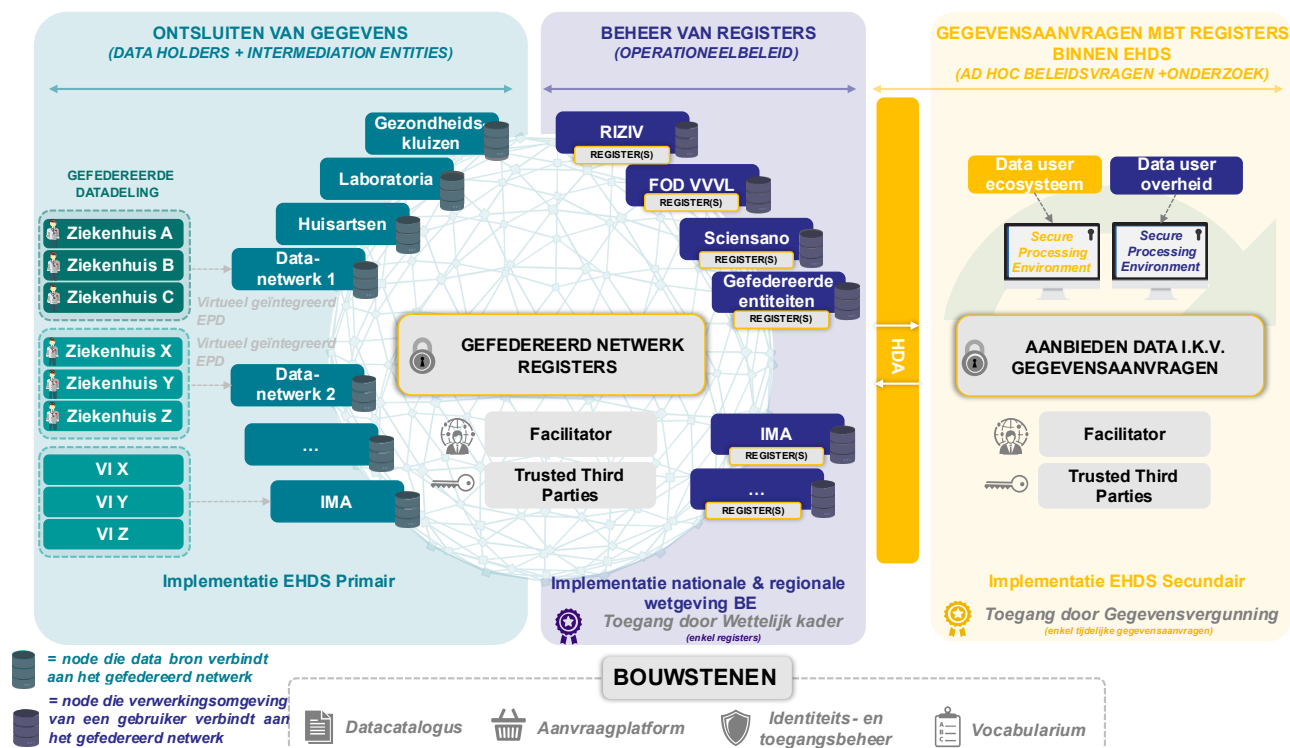
Inhoudsopgave

A. Visie betreffende het nieuwe registerbeleid in België	4
B. Glossarium.....	5
C. Rollen binnen het nieuwe registerbeleid in België	10
D. Gedetailleerde omschrijving van de rollen binnen het nieuwe registerbeleid	12

A. Visie betreffende het nieuwe registerbeleid in België

Het **startpunt** van het bepalen van de rollen en verantwoordelijkheden is de visie voor het **nieuwe registerbeleid**, zoals gepubliceerd op de [website](#) van het RIZIV. De visie wordt schematisch weergegeven in **onderstaande figuur**, zoals ook besproken en gevalideerd op de stuurgroep die het project opvolgt (02/10/2024). De **gehanteerde kleurcode** refereert telkens naar de verschillende onderdelen van de nieuwe visie zoals hieronder weergegeven:

- **Groen** - Ter beschikking stellen van nodige data voor registers door de verschillende data holders met inzicht in de verstrekte gegevens.
- **Blauw** - Continu datagebruik en beheer van registers door een aantal data users die onderdeel vormen van het gefedereerde netwerk.
- **Geel** - Datagebruik als gevolg van gegevensaanvragen door verschillende daartoe gemachtigde gebruikers, of datagebruik van registers door daartoe gemachtigde data users.



Figuur 1: Schematische voorstelling van het nieuwe registerbeleid in België

B. Glossarium

Dit hoofdstuk voorziet een overzicht van een **aantal belangrijke begrippen** die in het verdere verloop van de nota aan bod zullen komen. Deze begrippen kunnen de lezer helpen om vanuit een duidelijk kader de verschillende beschouwingen in de nota te begrijpen.

BASISBEGRIPPEN

- **Register:**
 - **(volgens huidige werking):** Een (patiënten)register is een verzameling - voor **één of meerdere doeleinden** - van **uniforme, gestandaardiseerde informatie** (klinische en andere) over een groep patiënten die een **aandoening of ervaring delen**.² Deze verzameling gebeurt meestal in de vorm van een momentopname door captatie uit systemen via een formulier. Daarbij worden gegevens die nog niet zijn gestandaardiseerd handmatig (hetzij manueel uit bv. een elektronische patiëntendossier (EPD)), semiautomatisch (hetzij via een CSV-extract uit bv. het EPD-systeem) of volledig automatisch (hetzij via een API gelinkt aan bv. het EPD-systeem) ingevoerd of overgenomen uit andere systemen. In het nieuwe registerbeleid dat door het RIZIV en de FOD VVVL werd uitgetekend, wordt de manier van het verzamelen van deze gegevens herzien, rekening houdend met nieuwe evoluties in technologie en regelgeving. Indien een gegevensverzameling niet aan de definitie van een **register volgens de nieuwe visie** voldoet (zie definitie hieronder), wordt niet langer over een register gesproken, maar wordt dit als een **gegevensaanvraag** binnen EHDS beschouwd (zie definitie hieronder).
 - **(volgens nieuwe visie):** In de nieuwe visie worden registers op een **continue basis** onderhouden en ter beschikking gesteld van de daartoe gemachtigde gebruikers voor verder beheer. Het nieuwe registerbeleid zal ten opzichte van het huidige beleid verschillen op een aantal belangrijke vlakken, nl. de gehanteerde governance (waaronder bv. de rollen beschreven in deze nota), de architectuur en technische opzet maar ook het stroomlijnen en compacter maken van registers. Principes als only once, standaardisering en het nastreven van hoge kwaliteit aan de bron worden vooropgesteld. Registers zullen worden gebruikt in het kader van **operationeel beleid** van (gezondheids)overheidsinstellingen. Een illustratief voorbeeld hiervan is het verstrekken van essentiële kerngegevens, zoals overzichtsgegevens over de incidentie en prevalentie van ziektes en aandoeningen. Bijvoorbeeld, de incidentie en microbiologische karakteristieken van circulerende infectieziektes worden via registers verzameld zodat op nationaal niveau aan infectiecontrole kan gedaan worden. Het verschil met de huidige manier van werken zit voornamelijk in het ter beschikking stellen van de gegevens die hiervoor nodig zijn. Deze zullen continu & near-realtime beschikbaar moeten zijn. Een register wordt zo **efficiënt en minimaal** mogelijk georganiseerd en bevat een vooraf vastgelegde (beperkte) **set aan variabelen**. Een belangrijke overweging in dit kader is dat registers steeds moet worden opgemaakt binnen een **wettelijk kader, waarin wordt gedefinieerd welke set aan variabelen noodzakelijk zijn**. Daarbij dienen data users slechts **éénmalig** een aanvraag in te dienen om daarna onbeperkt en blijvend toegang te hebben tot een

² <https://www.ncbi.nlm.nih.gov/books/NBK164514/>

register. In het nieuwe beleid zullen de verzamelde gezondheidsgegevens zo veel mogelijk afkomstig zijn uit het **elektronische patiëntendossier (EPD)** en **elektronisch medisch dossier (EMD)** in combinatie met bestaande authentieke databronnen (bv. afkomstig vanuit STATBEL). Het verder implementeren van de **patient summary**, die in het kader van de EHDS-verordening moet worden opgezet, kan de uitwisseling uit het EPD en EMD vereenvoudigen. De gezondheidsgegevens die verzameld worden, worden daarbij bepaald door de behoeften van de data users. In het nieuwe registerbeleid worden gegevens niet louter op vraag ter beschikking gesteld maar wordt er geëvolueerd naar het proactief ter beschikking stellen van relevante gegevens. Hierbij wordt getracht inzichtelijk te maken welke gegevens structureel voorhanden zijn door deze via een datacatalogus aan te bieden aan potentiële data users. In dat opzicht is het dus zo dat beschikbare gegevens maximaal inzichtelijk zijn voor mogelijks gebruik in een register. Zo zullen gelijkaardige gegevens die voorkomen in verschillende registers op éénzelfde manier gecapteerd en verwerkt worden volgens het only once principe en worden dubbele registraties maximaal vermeden.

- **Gegevensaanvraag met betrekking tot een register binnen EHDS (volgens nieuwe visie):** Met de komst van EHDS, zullen aanvragen tot het gebruik van gegevens uit een register verlopen zoals vastgelegd in de EHDS-verordening. Een gegevensaanvraag, in het kader van het registerbeleid, betreft een aanvraag tot gebruik van gegevens uit een register voor andere doeleinden dan oorspronkelijk bepaald. Hiervoor zal dus volledig volgens de principes en methodes van secundair gebruik van data volgens EHDS worden gewerkt. Binnen EHDS is gebruik van gezondheidsdata gelinkt aan verschillende categorieën³. In deze categorieën wordt ook verwezen naar registers. Het aanvragen van gegevens volgens EHDS kan op verschillende manieren. In dit document zal steeds gesproken worden over een gegevensaanvraag om de complexiteit te beperken. Het is hierbij wel noodzakelijk te vermelden dat een gegevensaanvraag volgens EHDS steeds beperkt is in de tijd wanneer het gaat om persoonsgevoelige informatie, namelijk met een maximum van 10 jaar⁴ en de mogelijkheid om dit éénmalig te verlengen. Het betreft een specifieke set gegevens die is afgestemd op een specifieke vraag, doorgaans in het kader van wetenschappelijk onderzoek en ad hoc beleidsvraagstukken. Deze gegevensaanvragen kunnen betrekking hebben op dezelfde gegevens die zijn opgenomen in een register, waarbij de gegevens dan tijdelijk worden ter beschikking gesteld in plaats van continu beschikbaar te zijn. Een gegevensaanvraag kan echter ook betrekking hebben op een ruimere verzameling van gegevens, waarbij bijvoorbeeld data uit meerdere registers wordt gecombineerd of aangevuld met andere databronnen, telkens in lijn met de specifieke onderzoeks- of beleidsvraag. Een gegevensaanvraag kan overgaan in een register wanneer er een continue beschikbaarheid van de gegevens vereist wordt in plaats van een tijdelijke beschikbaarheid (volgens termijn EHDS), mits deze overgang door een passend wettelijke kader wordt ondersteund.

UITWISSELEN VAN GEZONDHEIDSGEGEVENS

- **Only Once:** Only Once is een concept waarbij zorgverleners gezondheidsgegevens van patiënten slechts **eenmaal verzamelen en registreren** om deze vervolgens te delen met de

³ EHDS artikel 51.

⁴ EHDS artikel 68, lid 12.

andere zorgverleners binnen de gezondheidszorg, waar nodig met toestemming van de patiënt. Only once streeft ernaar dubbele registratie en herhaalde verzameling van dezelfde informatie te voorkomen, wat de **efficiëntie** bevordert, de zorgverlening verbetert, de patiëntervaring optimaliseert, gegevenskwaliteit verhoogt maar vooral ook de administratieve belasting verlaagt.

- **Semantische interoperabiliteit:** Semantische interoperabiliteit zorgt ervoor dat verschillende systemen niet alleen technisch gegevens kunnen uitwisselen, maar ook dat ze **dezelfde betekenis** aan die gegevens geven. Dit garandeert een **correcte interpretatie van informatie**, waardoor misverstanden worden vermeden.
- **Technische interoperabiliteit:** Technische interoperabiliteit zorgt ervoor dat verschillende systemen met elkaar kunnen communiceren en dat de verbinding werkt op technisch vlak door middel van **netwerken, bestandsformaten en communicatieprotocollen**.

BESCHIKBAAR STELLEN VAN GEZONDHEIDSGEGEVENS

- **Aggregatie:** Toegepast op **indirecte identificeerbare en gevoelige gegevens** (bv. woonplaats, leeftijd, gewicht, ...) is aggregatie een techniek waarbij deze gegevens worden samengevoegd in **breder categorieën of groepen**. Hierdoor worden individuele kenmerken minder specifiek en kunnen de gegevens niet meer direct naar een individu worden herleid wanneer men rekening houdt met 'small cells'. Aggregatie wordt vaak gebruikt als een methode binnen pseudonimiseren en anonimiseren.
- **Anonimiseren:** Anonimiseren is het proces waarbij **identificeerbare en gevoelige gegevens onomkeerbaar** worden **verwijderd of aangepast**, zodat deze niet meer geassocieerd kunnen worden met een individu. In tegenstelling tot pseudonimiseren bestaat er geen mogelijkheid om de oorspronkelijke gegevens later in het proces rechtstreeks te herstellen. Het doel van anonimiseren is om elke mogelijkheid van (her)identificatie van individuen volledig uit te sluiten.
- **Pseudonimiseren:** Pseudonimiseren is het proces waarbij **identificeerbare en gevoelige gegevens worden vervangen door pseudoniemen, bijvoorbeeld door coderingen, aggregaties of gebruik van referentietabellen**. In tegenstelling tot anonimiseren blijft echter het risico dat het mogelijk is om de oorspronkelijke gegevens terug te halen, hetzij rechtstreeks door het proces om te keren of onrechtstreeks door het aantal personen op wie deze gegevens betrekking kan hebben te reduceren door andere gegevens te koppelen. Het doel van pseudonimiseren is om heridentificatie van individuen op basis van de huidige technische middelen zoveel mogelijk te minimaliseren, terwijl de bruikbaarheid van de gegevens voor analyse en andere toepassingen behouden blijft.
- **Codering:** Codering (Encode/Decode) is een specifieke pseudonimiseringstechniek **waarbij direct identificeerbare gegevens** worden omgezet naar een betekenisloze identificatiecode door middel van **versleuteling**. Dit resulteert in gegevens die niet langer leesbaar zijn zonder de juiste sleutel, maar waarbij de mogelijkheid om de originele gegevens te restitueren met de juiste, specifieke sleutel behouden blijft. Hierbij wordt tevens verwezen naar de pseudonimiseringsdiensten (bv. Batch codage) aangeboden voor eHealth⁵.
- **Versleuteling:** Versleuteling of encryptie is het proces waarbij gegevens worden omgezet in een **gecodeerde vorm via cryptografische versleuteling**, zodat ze zonder de juiste sleutel niet leesbaar of toegankelijk zijn. Het doel is om de **vertrouwelijkheid en beveiliging** van gegevens

⁵ [Pseudonimisering & Anonimisering | eHealth-platform](#)

te waarborgen. Belangrijk hierbij is dat de versleuteling van waardes één op één wordt doorgevoerd.

- **Coderings-TTP:** Deze Trusted Third Party (TTP) is verantwoordelijk voor de **codering van direct identificeerbare gegevens** (bv. INSZ-nummer, naam, ...) veld per veld door middel van versleuteling met sleutels die deze TTP beheert, en biedt de mogelijkheid om andere gegevens als geheel te versleutelen. Deze TTP heeft verder geen toegang tot andere persoonsgegevens over de gezondheid van het individu en codeert louter de rechtstreeks identificeerbare persoonsgegevens. Deze visie sluit aan bij de **IVC-nota**⁶ die aangeeft dat een Coderings-TTP instaat voor de codering van persoonsgegevens en kan faciliteren bij het linken van gegevens over meerdere databronnen heen, zonder verder zicht te hebben op andere persoonsgegevens over de gezondheid. Verder mag de Coderings-TTP niet betrokken zijn als verwerkingsverantwoordelijke voor de gegevens van secundair gebruik. De acties die deze TTP uitvoert, worden in deze nota omschreven als de eerste stap in het anonimiserings- & pseudonimiseringsproces.
- **Anonimiserings/pseudonimiserings-TTP:** In dezelfde IVC-nota wordt tevens gesproken over een tweede TTP, nl. de anonimiserings/pseudonimiserings-TTP. Deze actor voert, naast de acties van de Coderings-TTP, stappen uit die andere persoonsgegevens anonimiseert of pseudonimiseert zodat men op het geheel van de gegevens de kans op identificatie van het individu reduceert (bv. een exacte leeftijd van 42 jaar aanpassen naar een categorie '40-45 jaar'). Daarbij wordt ook rekening gehouden dat de totale set aan gegevens niet kan koppelen aan bijkomende gegevens die de kans op identificatie vergroten. Het is hierbij belangrijk te vermelden dat deze bijkomende anonimiserings- en pseudonimiseringsstappen volgens de nieuwe visie van het registerbeleid niet langer door een afzonderlijke partij dienen te gebeuren. Volgens de nieuwe visie worden deze gegevens waar nodig reeds bij de bron (lees de data-holder of intermediation entity) maximaal geanonimiseerd en/of gepseudonimiseerd beschikbaar gesteld, waarbij wel nog de doeltreffendheid van de toegepaste technieken en het resterend risico beoordeeld kunnen worden door een onafhankelijke partij door middel van een SCRA-controle.
- **SCRA-controle:** Deze controle **beoordeelt het risico op de identificatie van een individu** aan de hand van de beschikbare gegevens. Deze controle wordt mogelijk gemaakt door gebruik te maken van een theoretische Small Cell Risk Analysis (SCRA) of analyse van 'kleine cellen'. Deze analyse beoordeelt de anonimiserings- en pseudonimiseringsstappen die genomen zijn om waarden te vervangen (zoals via aggregaties in categorieën, abstracties, tijdsverschuivingen, ...) van indirect identificeerbare gegevens (bv. adres, geboortedatum, ...) en gevoelige gegevens (bv. gewicht en lengte door BMI waar mogelijk en binnen de noden van het gebruik. Deze controle wordt uitgevoerd door gebruik te maken van de metagegevens van de eigenlijke data die men ter beschikking stelt. Deze metagegevens dienen inzicht te geven in de parameters die worden uitgewisseld (bv. gewicht, lengte, leeftijd, etc.), de vorm (gecodeerd of niet gecodeerd), het aantal waarden van de parameter (bv. geslacht à 2, leeftijd à 120) enzovoort. De actor die deze stap uitvoert, hoeft dus geen toegang te hebben tot de eigenlijke gegevens en heeft dus nooit kennis van rechtstreeks identificeerbare gegevens.

6

<https://www.ehealth.fgov.be/ehealthplatform/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/5b9b3a020231182706416967127494da04709ce7/healthdata.be-nota.pdf>

AANVRAGEN VAN GEZONDHEIDSGEGEVENS

- **Datacatalogus:** De datacatalogus binnen de visie op het registerbeleid geeft een overzicht van de **bestaande registers en gegevensvelden** die door potentiële data users kunnen worden opgevraagd in het aanvraagplatform. De datacatalogus omvat informatie omtrent welke gegevens beschikbaar zijn en onder welke **voorwaarden**, welke **standaarden** worden gebruikt en hoe **privacy en beveiliging** worden gewaarborgd.
- **Aanvraagplatform:** Het aanvraagplatform voorziet in een **technisch platform** dat alle activiteiten met betrekking tot zowel aanvragen voor registers als gegevensaanvragen faciliteert. Dit platform kan echter uit verschillende componenten en/of technologieën bestaan. Dit omvat onder meer het verstrekken van de datacatalogus dat een overzicht biedt van alle beschikbare (register)gegevens en het ondersteunen van het volledige aanvraagproces voor gezondheidsgegevens.

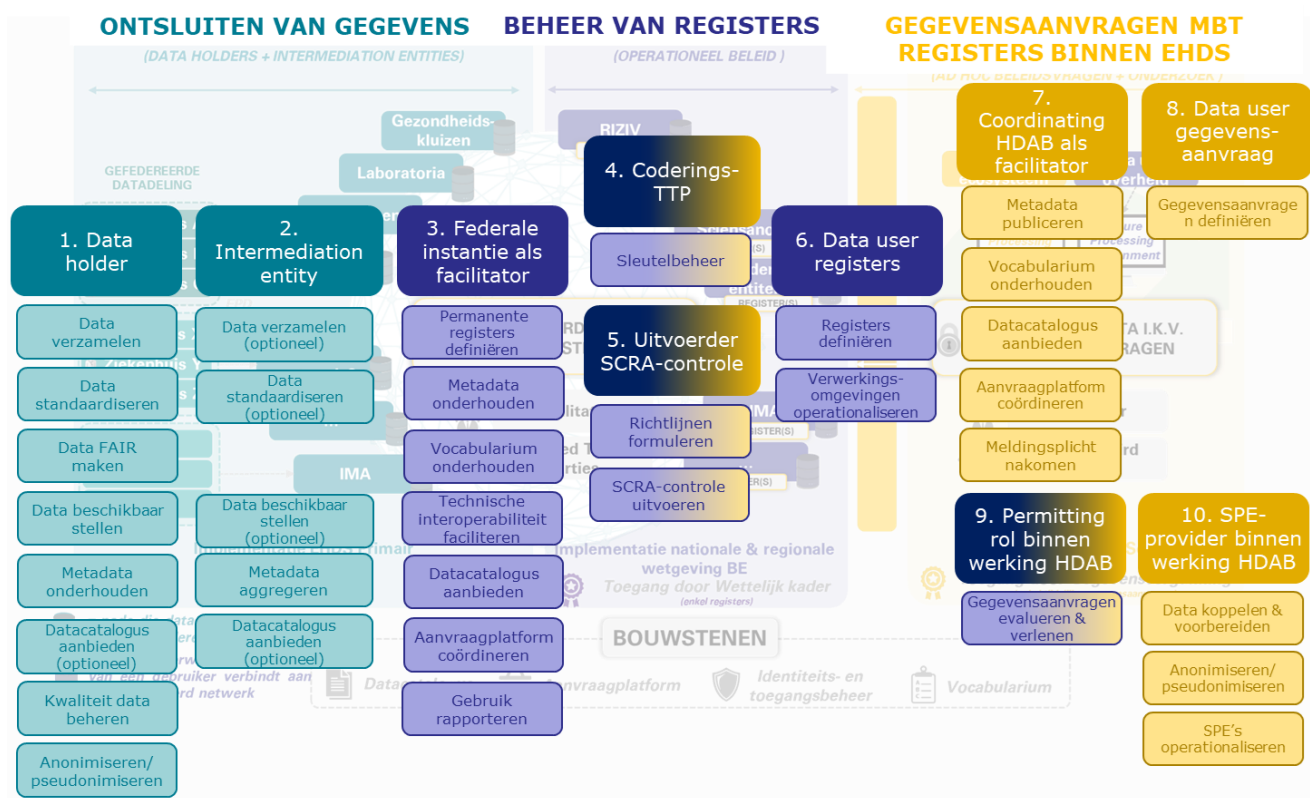
VERWERKEN VAN GEZONDHEIDSGEGEVENS

- **Secure Processing Environment (SPE):** Secure Processing Environments zijn een essentiële bouwsteen voor het ontvangen en verwerken van gezondheidsgegevens door data users. Deze omgevingen zijn specifiek ontworpen om op een **veilige en gecontroleerde wijze** deze gegevens beschikbaar te stellen aan data users. Binnen een SPE kunnen data users analyses uitvoeren op de opgevraagde gegevens, zonder een directe toegang tot de onbewerkte gegevens te verkrijgen. SPE's waarborgen dat **geautomatiseerde gegevensuitwisseling** plaatsvindt binnen een omgeving die voldoet aan **strikte veiligheidsnormen** en die de **geldende privacywetgeving** naleeft en waarborgen een **strik toegangsbeheer**. Een SPE is een permanente infrastructuur waarbinnen er op basis van specifieke aanvragen een aparte werkomgeving kan worden opgezet waartoe een data user toegang krijgt tot de gevraagde gegevens. In deze nota volgt de SPE de vereisten die door de EHDS-regelgeving worden vooropgesteld of nog worden uitgewerkt.

C. Rollen binnen het nieuwe registerbeleid in België

1. OVERZICHT

We onderscheiden 10 verschillende rollen in het nieuwe registerbeleid. Deze zijn op Figuur 2 weergegeven, inclusief de bijhorende verantwoordelijkheden. Hierbij werd dezelfde kleurencode als voor Figuur 1 gehanteerd, nl. groen voor dataverleners, blauw voor registers en geel voor gegevensaanvragen binnen EHDS. In de volgende sectie wordt de concrete invulling van deze rollen beschreven, terwijl het volgende hoofdstuk dieper zal ingaan op de omschrijving en bijhorende verantwoordelijkheden en conceptuele technische bouwstenen. *Deze voorgestelde rollen zijn nauw gealigneerd met de rollen die binnen de EHDS-context zijn vastgelegd, waardoor het registerbeleid sterk inpast in de voorgestelde structuren en governance van de EHDS-verordening.*



Figuur 2: Schematische voorstelling van de rollen en verantwoordelijkheden binnen het nieuwe registerbeleid in België

2. INVULLING VAN DE ROLLEN BINNEN HET NIEUWE REGISTERBELEID IN BELGIË

In de onderstaande tabel wordt de concrete invulling van de diverse rollen nodig voor de operationalisering van het toekomstig registerbeleid in de praktijk, gepresenteerd.

De rollen van het registerbeleid worden maximaal gealigneerd met de EHDS-verordening. Het is dan ook een logisch gevolg dat HDA een aantal rollen krijgt toegewezen. Dit betekent niet dat de HDA alle betrokken activiteiten van deze rollen zelf kan of moet opnemen, maar wel het beheer ervan zal organiseren.

In onderstaande tabel, is een overzicht verstrekt van de **vastgestelde rollen en betrokken actoren** binnen het registerbeleid in België.

	Rolinvulling [kardinaliteit]
1. Data holder [n]	Ziekenhuizen, huisartsen, labo's, gezondheidsdatakluisen, onderzoeksinstituten, overheidsgezondheidsinstellingen...
2. Intermediation entity [n]	Datanetwerken, ...
3. Federale instantie als facilitator registers [1]	HDA
4. Codings-TTP [1 ... n]	eHealth, KSZ, ...
5. Uitvoerder SCRA-controle [1]	HDA
6. Data user register [n]	Overheidsgezondheidsinstellingen en andere users met wettelijke basis
7. Coordinating HDAB als facilitator gegevensaanvragen binnen EHDS [1]	HDA
8. Data user gegevensaanvraag binnen EHDS[n]	Ref. gebruikers binnen de EHDS-context
9. Permitting rol binnen werking HDAB [1 ... n]	Volgen van de aanduiding binnen de EHDS-context
10. SPE-provider binnen werking HDAB [1 ... n]	Volgen van de aanduiding binnen de EHDS-context

Tabel 1: Invulling van de rollen binnen het nieuwe registerbeleid van België

D. Gedetailleerde omschrijving van de rollen binnen het nieuwe registerbeleid

In dit hoofdstuk wordt dieper ingegaan op elk van de rollen binnen het nieuwe registerbeleid. Dit gebeurt aan de hand van een **unieke fiche** per rol, die een gedetailleerde beschrijving geven van (1) de concrete **omschrijving** van de rol, (2) de specifieke **taken en verantwoordelijkheden** die zijn verbonden aan de rol en (3) de conceptuele **technische bouwstenen** die aan de rollen ten grondslag liggen. Voor iedere rol wordt in de omschrijving eveneens aangegeven wat de **kardinaliteit** is van deze rol.

1. DATA HOLDER

Omschrijving rol

Data holders zijn partijen die elektronische **gezondheidsgegevens verzamelen en verwerken** voor (1) de verstrekking van gezondheidszorg of (2) doelstellingen op het gebied van volksgezondheid, vergoedingen, onderzoek en innovatie, beleidsvorming, officiële statistieken, patiëntveiligheid of regelgeving. **Deze definitie is analoog aan de definitie van data holders onder de EHDS-verordening.** Voorbeelden van data holders binnen het registerbeleid (en aldus de EHDS-verordening) zijn onder meer ziekenhuizen en/of datanetwerken, laboratoria, (huis)artsen, het IMA, farmaceutische bedrijven, private verzekeringsinstellingen, onderzoeksinstituten maar ook overheidsgezondheidsinstellingen zelf.

Kardinaliteit: Meerdere

Taken en verantwoordelijkheden

- **Data verzamelen:** Het verzamelen van data omvat onder meer het zorgvuldig en nauwkeurig vastleggen van relevante informatie over patiënten en gezondheidszorgdiensten door de zorgprofessionals binnen ziekenhuizen, laboratoria, huisartspraktijken, ... Dit omvat het verzamelen van data over medische geschiedenis, behandelingen, medicatie, laboratoriumresultaten en andere relevante klinische informatie, bij voorkeur in het EPD.
- **Data standaardiseren:** Het implementeren en handhaven van uniforme nomenclatuur en standaarden voor het vastleggen, opslaan en uitwisselen van gezondheidsgegevens om ervoor te zorgen dat gegevens consistent en interoperabel zijn over diverse systemen en zorginstellingen. Het toepassen van uniforme nomenclatuur en standaarden dient zoveel mogelijk bij de bron of de data holder zelf te gebeuren. Belangrijke nomenclatuur en standaarden in dit kader zijn OMOP, SNOMED CT, ICD-10/11, ...
- **Data FAIR maken:** Gegevens die worden verzameld en opgeslagen zijn Findable, Accessible, Interoperable en Reusable. Concreet worden gegevens op een gestructureerde en uniforme manier opgeslagen en gedocumenteerd, zodat deze eenvoudig te vinden, toegankelijk, gebruiken en hergebruiken zijn door zorgverleners, overheden en andere stakeholders in de gezondheidszorg. Ook voor het FAIR maken van data dient de implementatie zoveel mogelijk bij de bron of de data holder zelf te gebeuren.
- **Data beschikbaar stellen:** Gezondheidsgegevens worden op een toegankelijke en gestructureerde manier verzameld, verwerkt en voorbereid door de data holder, zodat deze kunnen worden geraadpleegd, gebruikt en geanalyseerd door andere zorgverleners, overheden en stakeholders in de gezondheidszorg. Deze voorbereiding omvat onder andere de implementatie van uitwisselingsstandaarden zoals FHIR. Welke uitwisselingsstandaarden

gevolgd moeten worden, wordt bepaald door de facilitator om technische interoperabiliteit met andere systemen te garanderen.

- **Metadata onderhouden:** Het opmaken en onderhouden van informatie over de ter beschikking gestelde gegevensvelden volgens de [metadata standaard HealthDCAT-AP](#). Dit omvat onder meer het definiëren van beschrijvende informatie over de gegevens, zoals hun betekenis, bron, formaat, toegangsrechten en gehanteerde standaarden. Dit valt niet enkel onder de verantwoordelijkheid van de data holder, maar ook andere rollen (intermediation entity, facilitator, coordinating HDAB) zullen betrokken zijn bij het publiceren van actuele metadata.⁷
- **Datacatalogus aanbieden (optioneel):** Het creëren en onderhouden van een gestructureerde catalogus van de beschikbare gezondheidsgegevens van de data holder. De datacatalogus omvat informatie omtrent welke gegevens beschikbaar zijn, welke standaarden worden gebruikt, en hoe privacy en beveiliging worden gewaarborgd. De opmaak van dergelijke datacatalogus op lokaal niveau lijkt aangewezen om een duidelijk overzicht te hebben van de (meta)gegevens waarover de data holder beschikt. Dergelijke lokale datacatalogi kunnen vervolgens gekoppeld worden met de datacatalogus van de intermediation entity (indien van toepassing) en/of de facilitator.
- **Kwaliteit data beheren:** De kwaliteit van data beheren omvat het monitoren, beschrijven en documenteren van de juistheid, volledigheid en consistentie van de verzamelde data, en het identificeren van fouten of inconsistenties. [Deze activiteit is gealigneerd met de EHDS-verordening dat data holders de kwaliteit van hun data moeten documenteren.](#)
- **Data anonimiseren en/of pseudonimiseren:** Het elimineren, transformeren of vervangen (bv. een exacte leeftijd van 42 jaar aanpassen naar een categorie '40-45 jaar') van identificerende informatie binnen de gezondheidsgegevens alvorens deze ter beschikking te stellen aan data users, om ervoor te zorgen dat de privacy van individuen wordt beschermd. Deze verantwoordelijkheid wordt opgenomen door de data holders aan de bron. De activiteiten onder deze verantwoordelijkheid verwijzen rechtstreeks naar de activiteiten die in de IVC-nota, vermeld in het glossarium, vandaag deels worden opgenomen door de anonimiserings/pseudonimiserings-TTP. Voor verdere pseudonimisering van identificeerbare persoonsgegevens zoals het INSZ-nummer zal beroep worden gedaan op de Coderings-TTP en de diensten die deze aanbiedt (zie later). [Deze visie is in lijn met het standpunt binnen de EHDS-verordening waarbij deze activiteiten zoveel mogelijk aan de bron moeten gebeuren.](#)

Technische bouwstenen

- **EPD:** Het EPD is het Elektronisch Patiëntendossier waarin alle medische informatie van patiënten digitaal wordt verzameld en gedocumenteerd door zorgverleners. Dit is het centrale aanspreekpunt voor de medische toestand van patiënten. Voor het registerbeleid wordt geëvolueerd naar een virtueel geïntegreerd patiëntendossier, gebaseerd op de principes van het BIHR zoals opgenomen in het eHealth actieplan, waarbij het EPD optreedt als een belangrijke databron voor zowel de registers als de gegevensaanvragen.
- **Interne IAM:** De interne IAM-component (Identity & Access Management) zorgt ervoor dat de organisatie achter de gebruiker wordt herkend en het juiste certificaat of token kan worden

⁷ Data holders voorzien metadata voor de door hen aangeleverde gezondheidsgegevens, de intermediation entity (IE) aggregeert de metadata van de data holders die aan de IE zijn verbonden, de facilitator publiceert metadata in het aanvraagplatform i.f.v. het opvragen van permanente registers en de coordinating HDAB publiceert metadata in het aanvraagplatform i.f.v. tijdelijke gegevensaanvragen door het bredere publiek.

meegeleverd aan de externe IAM-component. Deze interne IAM-component is steeds partij-afhankelijk, wat betekent dat de implementatie van deze component kan variëren per organisatie.

- **Externe IAM:** *De externe IAM-component zorgt voor identificatie, authenticatie en machtiging van alle gemachtigde partijen op basis van het certificaat of token van de gebruiker dat door de interne IAM-component wordt meegeleverd. Concreet zorgt de externe IAM-component dat gebruikers van alle gemachtigde partijen kunnen inloggen op o.a. de metadata management tool, het aanvraagplatform, ... en rechten bepaald worden via het eHealth platform, zodat ze toegang hebben tot de benodigde tools.*
- **Data input tool:** *In de data input tool kunnen gegevens via een formulier ingevuld worden en opgeslagen worden. Deze gegevens kunnen naast het EPD ook als gegevensbron dienen voor de input van de data management tool.*
- **Data management tool:** *De data management tool dient als een data platform waar data kan worden opgeladen en opgeslagen, en waar transformaties op deze data kunnen worden uitgevoerd. Automatische connecties met databronnen en ETL (Extract Transform Load) pipelines kunnen hierin opgezet worden. Daarnaast kunnen standaardisaties en aanpassingen worden doorgevoerd om de data meer FAIR te maken.*
- **Metadata management tool:** *In deze tool kunnen gebruikers metadata aanvullen, aanpassen, toevoegen en onderhouden. De metadata moet ervoor zorgen dat registers en de beschikbaar gestelde gezondheidsgegevens vindbaar, toegankelijk, interoperabel en herbruikbaar (FAIR) zijn. De metadata wordt eerst gedocumenteerd bij de data holder eventueel geconsolideerd door intermediation entity (IE) indien van toepassing, en wordt daarna opgehaald door en aangevuld bij de facilitator.*
- **Data gateway:** *Gegevens worden beschikbaar gesteld via de data gateway component bij de data holder, wanneer data wordt opgevraagd vanuit de verwerkingsomgeving of SPE voor gegevensaanvragen. Deze component maakt het mogelijk om gegevens op te halen in een gestandaardiseerd formaat (bv. via API-calls), lees het 'pullen' van gegevens. Door deze component bij de data holder (gegevensbron) te hebben, wordt de meest recente versie van de gegevens doorgegeven en draagt dit bij tot een gedecentraliseerd datasysteem. Dit verschilt van de huidige van werken waarbij gegevens via een service of formulier worden doorgestuurd naar een verwerker, lees het 'pushen' van gegevens.*

Naast ontsluiten van gegevens voor het opmaken van de registers, kan de gateway ook toegang geven tot geaggregeerde en benchmarking gegevens met betrekking tot de gegevens die ontsloten worden. Op die manier biedt dit bijkomende voordelen voor de data holder in het verkrijgen van inzichten. Dit laatste is vooral interessant voor bijvoorbeeld ziekenhuizen.

- **Datacatalogus (optioneel):** *De datacatalogus is een centrale inventaris van de beschikbare gegevens. Het biedt functionaliteiten zoals het zoeken en filteren hiervan, waardoor deze eenvoudig vindbaar en toegankelijk zijn.*
- **Service voor anonimiseren/pseudonimiseren:** *De service voor het pseudonimiseren van gegevens beperkt het risico op heridentificatie en voorziet de uitvoering van technieken om waarden te vervangen van indirecte identificeerbare gegevens (bv. adres, geboortedatum, ...) en gevoelige gegevens (bv. gewicht, lengte, ...). Dit gebeurt zoveel mogelijk bij de data holder*

zelf in de data management tool. Deze visie komt overeen met de IVC-nota⁸ waarbij de anonimisering of pseudonimisering zo vroeg mogelijk in de ketting gebeurt. Hiervoor dient de data holder deels beroep doen op de diensten aangeboden door eHealth, namelijk de Batch codage voor wat betreft de rechtstreeks identificeerbare gegevens.

2. INTERMEDIATION ENTITY

Omschrijving rol

Intermediation entities zullen **data holders deels ontlasten** door specifieke taken van hen over te nemen. Zo kunnen intermediation entities bijvoorbeeld voorzien in **aggregatie of standaardisatie** van gegevens, daar waar individuele data holders niet steeds over de capaciteit en expertise beschikken om dit zelf te doen. Voor de concrete werking van de intermediation entity zal bekeken dienen te worden of ze lokaal zullen opereren bij de data holders zelf, of ze veeleer gegevens zullen aggregeren binnen hun eigen systemen en deze zelf van hieruit zullen ontsluiten. Intermediation entities kunnen zowel gegevens van de data holders **effectief bewaren en verwerken** als **uitsluitend metadata** beheren. Een **voorbeeld** van intermediation entities zijn de gezondheidsdatanetwerken. Deze omschrijving is in overeenstemming met de definitie van de EHDS-verordening voor intermediation entities. De verordening schrijft hieromtrent voor dat deze entiteiten specifieke taken van bepaalde categorieën van data holders overnemen, met als doel de administratieve belasting voor data holders te verminderen en het streven naar efficiëntie en effectiviteit te ondersteunen. In de praktijk zijn de intermediation entities in staat om gezondheidsgegevens te verwerken en beschikbaar te stellen voor secundair gebruik, op basis van de gegevens verstrekt door de data holders. Conform de EHDS-verordening is het verboden dat een intermediation entity optreedt als HDAB.

Kardinaliteit: Meerdere

Taken en verantwoordelijkheden

- **Data verzamelen, standaardiseren & beschikbaar stellen (optioneel):** Het verzamelen, standaardiseren en beschikbaar stellen van data voor primair & secundair gebruik. Dit zoals aangegeven in de EHDS-verordening. Echter zal de effectieve invulling wellicht verschillen per type stakeholder. Indien de intermediation entity in deze een rol speelt, kan ze in het kader van het registerbeleid mee instaan voor het ontsluiten van gegevens voor de opmaak van registers en het beantwoorden van gegevensaanvragen binnen EHDS.
- **Metadata aggregeren:** Het aggregeren en ontsluiten van de metadata van de data holders die zijn verbonden aan de intermediation entity naar de facilitator. Indien data holders onvoldoende capaciteit en kennis hebben, kunnen intermediation entities aanvullende ondersteuning bieden bij het opstellen van de metadata zelf en ervoor zorgen dat ze voldoen aan de vereiste normen (bv. opmaak volgens de [HealthDCAT-AP standaard](#)).
- **Datacatalogus aanbieden (optioneel):** Het creëren en onderhouden van een gestructureerde catalogus van beschikbare gezondheidsgegevens van de data holders die verbonden zijn aan de intermediation entity. De datacatalogus omvat informatie omtrent welke gegevens beschikbaar zijn, welke standaarden worden gebruikt, en hoe privacy en beveiliging worden gewaarborgd. De opmaak van dergelijke datacatalogus op lokaal niveau lijkt aangewezen om een overzicht te hebben van de (meta)gegevens waarover de intermediation entity beschikt. Dergelijke lokale datacatalogi kunnen vervolgens gekoppeld worden met de datacatalogus van de facilitator.

Technische bouwstenen

- **Interne IAM:** De interne IAM-component (Identity & Access Management) zorgt ervoor dat de organisatie achter de gebruiker wordt herkend en het juiste certificaat of token kan worden meegeleverd aan de externe IAM-component. Deze interne IAM-component is steeds partij-

afhankelijk, wat betekent dat de implementatie van deze component kan variëren per organisatie.

- **Externe IAM:** *De externe IAM-component zorgt voor identificatie, authenticatie en machtiging van alle gemachtigde partijen op basis van het certificaat of token van de gebruiker dat door de interne IAM-component wordt meegeleverd. Concreet zorgt de externe IAM-component dat gebruikers van alle gemachtigde partijen kunnen inloggen op o.a. de metadata management tool, het aanvraagplatform, ... en rechten bepaald worden via het eHealth platform, zodat ze toegang hebben tot de benodigde tools.*
- **Metadata management tool:** *In deze tool kunnen gebruikers metadata aanvullen, aanpassen, toevoegen en onderhouden. De metadata moet ervoor zorgen dat registers en de beschikbaar gestelde gezondheidsgegevens vindbaar, toegankelijk, interoperabel en herbruikbaar (FAIR) zijn. De metadata wordt eerst gedocumenteerd bij de IE en wordt daarna opgehaald en aangevuld bij de facilitator.*
- **Datacatalogus (optioneel):** *De datacatalogus is een centrale inventaris van de beschikbare gegevens. Het biedt functionaliteiten zoals het zoeken en filteren hiervan, waardoor deze eenvoudig vindbaar en toegankelijk zijn.*

3. FEDERALE INSTANTIE ALS FACILITATOR REGISTERS

Omschrijving rol

De federale instantie als facilitator ondersteunt het **gebruik** van registers, en zorgt ervoor dat registers op een eenvoudige en geautomatiseerde wijze toegankelijk zijn. In zijn werking publiceert de facilitator onder meer een **datacatalogus** die informatie verstrekt over alle beschikbare registers. Verder werkt de facilitator nauw samen met de betrokkenen en het veld om vanuit gedeelde expertise tot **afspraken en richtlijnen** te komen met betrekking tot onder meer standaarden.

Kardinaliteit: Eén

Taken en verantwoordelijkheden

- **Registers definiëren:** *Gegevens van registers worden waar mogelijk maximaal opgehaald uit het **elektronisch patiëntendossier (EPD)**. De facilitator overlegt met de data user(s) van het register welke gegevensvelden nodig zijn voor de opmaak van het register in functie van de gebruiksdoelinden. Hierbij wordt steeds gesteund op een wettelijke basis voor de opmaak van een register.*
- **Metadata onderhouden:** *Het opmaken en onderhouden van informatie over de gegevensvelden die de registers uitmaken volgens de **metadata standaard HealthDCAT-AP**. Dit omvat onder meer het definiëren van beschrijvende informatie over de gegevens, zoals hun betekenis, bron, formaat, toegangsrechten, gehanteerde standaarden en kwaliteit van de gegevens. Concreet ontvangt de facilitator de metadata van de data holders en intermediation entities voor de beschikbare registers en zal deze aggregeren. **Het onderhouden en documenteren van metadata volgens de HealthDCAT-AP standaard is een verantwoordelijkheid van de coordinating HDAB volgens de EHDS-verordening.***
- **Afspraken semantische interoperabiliteit beheren:** *Het beheren, bijwerken en onderhouden van de terminologie, classificaties voor secundair gebruik en die worden gebruikt voor het vastleggen van registergegevens. Dit zorgt ervoor dat het duidelijk is welke betekenis en definitie aan gegevens wordt toegekend. **Dit vocabularium wordt verder aangevuld door de coordinating HDAB voor de gegevensaanvragen, om alignering overheen secundair gebruik en alignering met het Europese niveau te waarborgen.** Verder steunt men hierbij ook op het beheer van semantische interoperabiliteit op technisch gebied door eHealth en semantische standaard (bv. SNOMED CT, ICD-10, etc.) door FOD VVVL.*
- **Afspraken technische interoperabiliteit hanteren:** *Het toepassen van afspraken die technische interoperabiliteit bevorderen, zoals het definiëren van welke technische uitwisselingsstandaarden (bv. FHIR) gebruikt moeten worden om een vlotte en efficiënte gegevensuitwisseling te garanderen. Ook hier steunt men verder op het beheer van dergelijke uitwisselingsstandaarden door eHealth.*
- **Datacatalogus aanbieden:** *Het creëren en onderhouden van een gestructureerde catalogus van beschikbare registergegevens. De datacatalogus omvat informatie omtrent welke gegevens beschikbaar zijn en onder welke voorwaarden, welke standaarden worden gebruikt, en hoe privacy en beveiliging worden gewaarborgd. De facilitator aggregereert de datacatalogi van de data holders en intermediation entities voor de beschikbare registers.*
- **Aanvraagplatform coördineren voor registers (optioneel):** *Het coördineren van het aanvraagplatform waarin data users van registers verschillende bouwstenen zoals de*

datacatalogus, het vocabularium en het gebruiksbeleid kunnen raadplegen en via een eenvoudige en automatische aanvraag registers kunnen ophalen.

- **Gebruik rapporteren:** *Het rapporteren over de activiteiten van de facilitator en het effectieve gebruik (en opmaak) van de registers door (voor) de data users van registers. Dit is conform de wettelijke bepalingen waarbij men moet kunnen rapporteren over het gebruik van gegevens voor secundaire doeleinden. Zowel volgens bepalingen binnen EHDS als nationale wetgeving.*

Technische bouwstenen

- **Interne IAM:** *De interne IAM-component (Identity & Access Management) zorgt ervoor dat de organisatie achter de gebruiker wordt herkend en het juiste certificaat of token kan worden meegeleverd aan de externe IAM-component. Deze interne IAM-component is steeds partij-afhankelijk, wat betekent dat de implementatie van deze component kan variëren per organisatie.*
- **Externe IAM:** *De externe IAM-component zorgt voor identificatie, authenticatie en machtiging van alle gemachtigde partijen op basis van het certificaat of token van de gebruiker dat door de interne IAM-component wordt meegeleverd. Concreet zorgt de externe IAM-component dat gebruikers van alle gemachtigde partijen kunnen inloggen op o.a. de metadata management tool, het aanvraagplatform, ... en rechten bepaald worden via het eHealth platform, zodat ze toegang hebben tot de benodigde tools.*
- **Metadata management tool:** *In deze tool kunnen gebruikers metadata aanvullen, aanpassen, toevoegen en onderhouden. De metadata moet ervoor zorgen dat registers en de beschikbaar gestelde gezondheidsgegevens vindbaar, toegankelijk, interoperabel en herbruikbaar (FAIR) worden. De metadata wordt eerst gedocumenteerd bij de intermediation entity (IE) indien van toepassing, en wordt daarna opgehaald en aangevuld bij de facilitator.*
- **Datacatalogus:** *De datacatalogus is een centrale inventaris van de beschikbare gegevens en registers die ontsloten zijn. Het biedt functionaliteiten zoals het zoeken en filteren hiervan, waardoor deze eenvoudig vindbaar en toegankelijk zijn. Deze datacatalogus dient alle informatie beschikbaar uit catalogussen bij data holders en intermediation entities te combineren en consolideren zodat één nationale catalogus bestaat waarin informatie geconsolideerd aangeboden wordt. Dit is dezelfde catalogus zoals later ook beschreven in “7. Coordinating HDAB als facilitator gegevensaanvragen binnen EHDS”*
- **Aanvraagplatform registers (optioneel):** *Het aanvraagplatform biedt een omgeving waar data users nieuwe registers kunnen aanvragen kunnen indienen, en waarin deze aanvragen beheerd kunnen worden. Data users van registers verkrijgen toegang op basis van een wettelijke basis. Wanneer een aanvraagplatform wordt aangeboden, wordt idealiter gebruik gemaakt van dezelfde bouwsteen zoals vermeld bij “7. Coordinating HDAB als facilitator gegevensaanvragen binnen EHDS”.*

4. CODERINGS-TTP

Omschrijving rol

Deze Trusted Third Party (TTP) is verantwoordelijk voor de codering van **direct identificeerbare gegevens** (bv. rijksregister, naam, ...) veld per veld door middel van versleuteling met sleutels die de TTP beheert, en biedt de mogelijkheid om andere gegevens als geheel te versleutelen. Dit is in lijn met hoe de activiteiten vandaag omschreven worden voor de Coderings-TTP en eerste stap in de IVC-nota eerder vermeld het glossarium.

Kardinaliteit: Meerdere

Taken en verantwoordelijkheden

- **Sleutelbeheer:** *Het veilig beheren van sleutels en het coderen van gegevens om de vertrouwelijkheid en integriteit van uitgewisselde gezondheidsgegevens te waarborgen. Deze verantwoordelijkheid wordt opgenomen door de Coderings-TTP die in staat voor het bewaren van de sleutels die de koppeling mogelijk maken tussen de oorspronkelijke gegevens en de gegevens die ter beschikking worden gesteld aan data users.*

Technische bouwstenen

- **Codering service:** *De codering service is verantwoordelijk voor het versleutelen van direct identificeerbare gegevens (bv. rijksregisternummer, ...) op veldniveau met sleutels die door de Coderings-TTP worden beheerd. Daarnaast biedt de service de mogelijkheid om andere gegevenssets in hun geheel te versleutelen, wat bijdraagt aan de beveiliging en vertrouwelijkheid van de data.*

5. UITVOERDER SCRA-CONTROLE

Omschrijving rol

De uitvoerder van de SCRA-controle beoordeelt het risico op identificatie van een individu door het uitvoeren van een SCRA-controle en voorziet richtlijnen voor het vermijden hiervan door middel van het gebruik van technieken om waarden te vervangen (zoals via aggregaties in categorieën, abstracties, tijdsverschuivingen, ...) van **indirect identificeerbare gegevens** (bv. adres, geboortedatum, ...) en gevoelige gegevens (bv. gewicht, BMI, ...). Deze actor heeft voor het uitvoeren van zijn verantwoordelijkheden geen toegang tot de eigenlijke gegevens die worden uitgewisseld maar maakt louter gebruik van de nodige metagegevens (zie SCRA-controle in het glossarium).

Kardinaliteit: Eén

Taken en verantwoordelijkheden

- **Richtlijnen formuleren:** *Het formuleren van richtlijnen voor de data holder en SPE-provider om in het anonimiseren en pseudonimiseren van ter beschikking gestelde gezondheidsgegevens te voorzien. De uitvoerder van de SCRA-controle treedt op als controlerend toezichtsorgaan, waarbij de data holder aan de bron (voor individuele gegevens) en de SPE-provider in de SPE (voor geaggregeerde gegevens) instaan voor de betreffende activiteiten.*
- **SCRA-controle uitvoeren:** *Het evalueren en identificeren van potentiële beveiligingsrisico's en data-integriteitsteksties met betrekking tot kleine gegevenscellen binnen gezondheidsgegevens die ter beschikking worden gesteld aan data users. Concreet zal de uitvoerder van de SCRA-controle een SCRA-controle uitvoeren bij de data ontsluiting, ter validatie van de anonimisatie/pseudonimisatie uitgevoerd door de data holder, Coderings-TTP en/of SPE-provider. Indien de SCRA-analyse een negatief advies geeft, dan zal een nieuwe pseudonimisering bij de data holder vanaf de bron opnieuw uitgevoerd worden.*

Technische bouwstenen

- **SCRA-service:** *Bij de SCRA-service wordt gecontroleerd of heridentificatie van kleine groepen wordt voorkomen. Dit kan gebeuren door een theoretische SCRA (met behulp van de theoretische waarden per variabele een risicovoorspelling maken) of een kwantitatieve SCRA (aan de hand van de verschillende, reële waarden per variabele een risicovoorspelling maken). De focus van de uitvoerder van de SCRA-controle zal quasi enkel liggen op de theoretische SCRA wanneer de data ontsloten wordt in een SPE. Dit omdat hiervoor geen toegang tot de eigenlijke gegevens vereist is.*

6. DATA USER REGISTERS

Omschrijving rol

Data users van registers zijn **gemachtigde partijen** binnen het netwerk die toegang hebben tot het **aanvraagplatform** om registers aan te vragen. Ze krijgen enkel toegang tot de registers waarvoor ze de nodige wettelijke basis hebben en op een veilige manier kunnen ontvangen ter verwerking voor de vastgelegde doeleinden. Registers dienen dus te allen tijde te worden opgezet binnen een **wettelijk kader**. Toegang tot een register is mogelijk zodra een data user aan de **vereiste voorwaarden** voldoet.

Voorbeelden van entiteiten die in de praktijk optreden als een data user van registers zijn onder meer het RIZIV, de FOD VVVL, het IMA, Sciensano en de gefedereerde entiteiten. In bepaalde gevallen kunnen ook wetenschappelijke verenigingen of universiteiten optreden als data user van een register indien deze een mandaat toegewezen krijgen door een overheidsgezondheidsinstelling.

Kardinaliteit: Meerdere

Taken en verantwoordelijkheden

- **Registers definiëren:** *Gegevens van registers worden waar mogelijk maximaal opgehaald uit het **elektronisch patiëntendossier (EPD)**. De data user definieert welke gegevens nodig zijn om het vooropgestelde doel of doelen te bereiken. De facilitator kan de data user(s) van het register ondersteunen door aan te geven welke gegevensvelden reeds ter beschikking zijn voor de opmaak van het register in functie van de gebruiksdoeleinden. Hierbij wordt beoordeeld of een wettelijke basis vanuit de Belgische regelgeving of vanuit andere Europese wetgeving wordt gebruikt.*
- **Verwerkingsomgevingen operationaliseren:** *Het ontvangen van registers door data users geschiedt in een eigen verwerkingsomgeving, die de data user van het register lokaal uitbaat. Deze verwerkingsomgevingen zijn beveiligde omgevingen op het terrein van de data user zelf, om veilig gebruik en verwerking van registers te waarborgen. Data landt in de verwerkingsomgevingen in versleutelde (geëncrypteerde) vorm, waarbij decryptie slechts plaatsvindt na geautomatiseerde validatie van de theoretische SCRA door de uitvoerder van de SCRA-controle.*

Technische bouwstenen

- **Interne IAM:** *De interne IAM-component (Identity & Access Management) zorgt ervoor dat de organisatie achter de gebruiker wordt herkend en het juiste certificaat of token kan worden meegeleverd aan de externe IAM-component. Deze interne IAM-component is steeds partij-afhankelijk, wat betekent dat de implementatie van deze component kan variëren per organisatie.*
- **Externe IAM:** *De externe IAM-component zorgt voor de identificatie, authenticatie en machtiging van alle gemachtigde partijen op basis van het certificaat of token van de gebruiker dat door de interne IAM-component wordt meegeleverd. Concreet zorgt de externe IAM-component dat gebruikers van alle gemachtigde partijen kunnen inloggen op o.a. de metadata management tool, aanvraagplatform, ... en rechten bepaald worden via het eHealth platform, zodat ze toegang hebben tot de benodigde tools.*
- **Verwerkingsomgeving:** *De verwerkingsomgeving bij de data user zelf laat toe om een verwerkingsomgeving ter beschikking te hebben voor het veilig ontvangen en verwerken van*

registregegevens. Per data user, m.a.w. organisatie(s) die een aanvraag indienen, zal er zo'n verwerkingsomgeving worden opgesteld. Data users van registers zullen deze dus zelf dienen te hosten. Dergelijke verwerkingsomgeving zal het mogelijk maken om wanneer nodig via de data gateways bij de data holders, nieuwe gegevens op te vragen en verwerken in de eigen omgeving.

7. COORDINATING HDAB ALS FACILITATOR GEGEVENSAANVRAGEN BINNEN EHDS

Omschrijving rol

De coordinatie HDAB als facilitator ondersteunt het **tijdelijk gebruik** van gezondheidsgegevens, en coördineert de gegevensaanvragen via het aanvraagplatform. In zijn werking publiceert de coordinatie HDAB onder meer een **datacatalogus** die informatie verstrekt over alle beschikbare gezondheidsgegevens. *De coordinatie HDAB binnen het registerbeleid is dezelfde entiteit als de coordinatie HDAB onder de EHDS-verordening en werkt zodoende overkoepelend, waarbij deze beroep kan doen op gemeenschappelijke bouwblokken.*

Kardinaliteit: Eén

Taken en verantwoordelijkheden

- **Metadata publiceren:** *Zoals eerder aangegeven dienen data holders metadata op te maken en te onderhouden voor de ter beschikking gestelde gegevensvelden volgens de metadata standaard HealthDCAT-AP. De coordinatie HDAB als facilitator publiceert de metagegevens vervolgens in het aanvraagplatform in functie van het opvragen van tijdelijke gegevens. Daarnaast is er een faciliterende rol voor de coordinatie HDAB weggelegd om de opmaak van metadata bij de data holders te ondersteunen, zoals het formuleren van richtlijnen en best practices in verband met de opmaak van metadata.*
- **Vocabularium onderhouden:** *Het bijwerken en onderhouden van de terminologie, classificaties en coderingssystemen die worden gebruikt voor het documenteren, inventariseren en ter beschikking stellen van gezondheidsgegevens. Dit vocabularium wordt verder aangevuld door de coordinatie HDAB als facilitator voor de gegevensaanvragen, om alignering overheen het secundair gebruik en alignering met het Europese niveau te bevorderen.*
- **Datacatalogus aanbieden:** *Het creëren en onderhouden van een gestructureerde catalogus van beschikbare gezondheidsgegevens. De datacatalogus omvat informatie omtrent gegevens die beschikbaar zijn en onder welke voorwaarden, welke standaarden worden gebruikt, en hoe privacy en beveiliging worden gewaarborgd. De coordinatie HDAB als facilitator voor gegevensaanvragen voorziet een gefedereerde catalogus die informatie bevat over alle beschikbare gezondheidsgegevens. Dit gebeurt door aggregatie van gegevens uit de catalogus van de data holders en intermediation entiteiten. Deze datacatalogus zit ingebed in de algemene, centrale datacatalogus van de coordinatie HDAB.*
- **Aanvraagplatform coördineren voor gegevensaanvragen binnen EHDS:** *Het coördineren van het aanvraagplatform waarin data users van gegevensaanvragen verschillende bouwstenen zoals de datacatalogus, het vocabularium en het gebruiksbeleid kunnen raadplegen en via een manuele aanvraag, op basis van een gedetailleerd informatieformulier, gezondheidsgegevens kunnen opvragen.*
- **Meldingsplicht nakomen:** *Het publiek melden van alle ontvangen en verwerkte aanvragen binnen het aanvraagplatform, inclusief de besluiten voor het al dan niet verstrekken van gegevens. Deze informatie wordt aangevuld met het gebruik dat wordt gerapporteerd door de facilitator voor de registers. De verantwoordelijkheid betreffende de meldingsplicht berust op de verplichting die HDAB's hebben in overeenstemming met de EHDS-verordening waarbij gesteld wordt dat de HDAB om de twee jaar dient te rapporteren over alle ontvangen aanvragen.*

Technische bouwstenen

- **Metadata management tool:** *In deze tool kunnen gebruikers metadata aanvullen, aanpassen, toevoegen en onderhouden. De metadata moet ervoor zorgen dat registers en de ter beschikking gestelde gezondheidsgegevens vindbaar, toegankelijk, interoperabel en herbruikbaar (FAIR) worden. De metadata wordt eerst gedocumenteerd bij de data holder of intermediation entity (IE) indien van toepassing, en wordt daarna opgehaald en aangevuld bij de facilitator.*
- **Datacatalogus:** *De datacatalogus is een centrale inventaris van de beschikbare gezondheidsgegevens en registers die ontsloten zijn. Het biedt functionaliteiten zoals het zoeken en filteren hiervan, waardoor deze eenvoudig vindbaar en toegankelijk zijn. Deze datacatalogus dient alle informatie beschikbaar uit catalogussen bij data holders en intermediation entities te combineren en consolideren zodat één nationale catalogus bestaat waarin informatie geconsolideerd aangeboden wordt.*
- **Aanvraagplatform:** *Het aanvraagplatform biedt een omgeving waar data users gegevensaanvragen kunnen indienen, en waarin deze aanvragen beheerd kunnen worden. Data users van gegevensaanvragen ontvangen de gevraagde gegevens per aanvraag. Indien het gaat over individuele gegevens, dan worden deze gegevens via de SPE omgeving voor gegevensaanvragen ter beschikking gesteld gedurende de periode vermeld in de gegevensvergunning.*

8. DATA USER GEGEVENSAANVRAAG

Omschrijving rol

Data users van gegevensaanvragen nemen **niet rechtstreeks deel** aan het gefedereerde netwerk. Ze dienen een **gegevensaanvraag (conform EHDS)** in via het aanvraagplatform, waarna de aanvraag wordt behandeld door de coordinating HDAB. In de aanvraag dienen de data users onder meer duidelijk te **motiveren** voor welke specifieke doeleinden zij de gegevens wensen te gebruiken, alsook of aan de vastgestelde voorwaarden wordt voldaan.

Data users van gegevensaanvragen dienen voor iedere gegevensvraag **een nieuwe aanvraag** in te dienen bij de coordinating HDAB. Voor elke aanvraag zal men de data pas kunnen raadplegen of ontvangen na het verkrijgen van een **positieve beslissing door de HDAB**. Indien er nood is voor een vergunning voor het gebruik van individuele gegevens, zal deze vergunning geëvalueerd binnen de permitting werking van de HDAB (zie verder) en verleend conform een wettelijk kader. **Dit kader is in principe de EHDS-verordening, die geldt als verfijning ("lex specialis") van GDPR**, maar alternatieven kunnen ook specifiek wettelijke kaders zijn die via koninklijke besluiten (federaal), decreten (Vlaams/Waals), ordonnances of verordeningen (Brussels) zijn. Gegevensvergunningen en dus ook -aanvragen zijn daarbij steeds **beperkt in de tijd**.

Elke natuurlijke persoon of organisatie kan in principe optreden als een data user gegevensaanvraag, op voorwaarde dat zij voldoen aan de vastgestelde criteria. **In de praktijk** zullen veel voorkomende dergelijke gebruikers onder andere onderzoekers, beleidsmakers, private bedrijven en zorgvoorzieningen zijn.

Kardinaliteit: Meerdere

Taken en verantwoordelijkheden

- **Gegevensaanvragen definiëren:** *Om tijdelijke toegang te verkrijgen tot gezondheidsgegevens, dient de data user een aanvraag voor toegang tot gezondheidsgegevens of verzoek om gezondheidsgegevens – naargelang de aard van de gewenste data, zie de definitie van gegevensaanvraag binnen EHDS in Hoofdstuk B. hierboven – in te dienen via het aanvraagplatform. Indien gewenst en wanneer relevant, kunnen gegevensaanvragen opgesteld worden vertrekkend vanuit de gegevens die in een bestaand register zijn opgenomen, bv. aangevuld met een aantal extra gegevensvelden, al dan niet uit andere databronnen.*

Technische bouwstenen

- /

9. PERMITTING ROL BINNEN WERKING HDAB

Omschrijving rol

Een HDAB dient de beslissing te nemen of de aanvrager toegang tot gegevens kan verkrijgen. Wanneer dit gaat over toegang tot individuele gegevens zal een vergunning of 'permit' verleend moeten worden. Daarom heeft de HDAB ook een rol als 'permitting' entiteit. Binnen deze permitting rol zal men gegevensaanvragen van gezondheidsgegevens mee verwerken door de **besluitvorming** betreffende het al dan niet verlenen van een (permanente/tijdelijke) **vergunning** te ondersteunen. Momenteel speelt het **Informatieveiligheidscomité (IVC)** in België een belangrijk rol bij het adviseren over permits. *De instantie die zal instaan voor de permitting activiteiten binnen de werking van de HDAB binnen het registerbeleid is dezelfde entiteit als deze onder de EHDS-verordening, en werkt zodoende overkoepelend, waarbij deze kan beroepen op gemeenschappelijke bouwblokken.*

Kardinaliteit: Eén of meerdere

Taken en verantwoordelijkheden

- **Gegevensaanvragen evalueren en verlenen:** *Het beoordelen van aanvragen en de daaropvolgende besluitvorming over het verlenen of weigeren van toegang tot het gebruik van gezondheidsgegevens voor secundair gebruik. Dit omvat onder meer de controle op de naleving van geldende regelgeving en de controle op de naleving van ethische normen.*

Technische bouwstenen

- **Permit management tool:** *De permit management tool beoordeelt en verleent gegevensvergunningen voor het aanvragen van gezondheidsgegevens met persoonlijke data. Bij data users van registers wordt dit zoveel mogelijk geautomatiseerd aan de hand van het gebruiksbeleid van de registers. Bij data users voor gegevensaanvragen zal er steeds een manuele tussenkomst zijn.*

10. SPE-PROVIDER BINNEN WERKING HDAB

Omschrijving rol

Het voorzien van een SPE voor gegevensaanvragen en dus binnen de werking van de HDAB betreft het faciliteren en ter beschikking stellen van een **Secure Processing Environment** zodat data users gezondheidsgegevens binnen een veilige omgeving kunnen ontvangen en verwerken. Binnen de SPE wordt een afgescheiden en beveiligde werkruimte voorzien specifiek voor een bepaalde aanvraag en begrenst in de tijd. De SPE zelf wordt opgezet zonder einddatum en is aldus continu van aard. Afhankelijk van de wijze waarop deze rol wordt opgenomen binnen de werking van een HDAB is er nood aan de nodige segregatie/scheiding van teams, functies en toegangen voor het verwerken van data en gegevensaanvragen zoals gesteld in de EHDS verordening⁹.

Kardinaliteit: Eén of meerdere

Taken en verantwoordelijkheden

- **Data koppelen en voorbereiden:** *Het voorbereiden van de gevraagde data om betrouwbare en bruikbare gegevens te creëren voor analyses, rapportage en beleidsvorming. Dit omvat onder andere het standaardiseren van gegevensformaten, het uitvoeren van gegevensvalidatie, het koppelen van gegevens uit diverse bronnen en het uitvoeren van bepaalde verdere anonimisatie of pseudonimisatie activiteiten hierop. Deze verantwoordelijkheden worden opgenomen als onderdeel van de processing taken van een HDAB.*
- **Data anonimiseren en/of pseudonimiseren:** *Het elimineren, transformeren of vervangen van identificerende informatie binnen de gezondheidsgegevens alvorens deze ter beschikking te stellen aan data users, om ervoor te zorgen dat de privacy van individuen wordt beschermd. Deze verantwoordelijkheid wordt opgenomen door de data holders op de individuele gegevensbronnen aan de bron, alsook door de HDAB als onderdeel van haar processing taken voor de aggregatie van verschillende gegevensbronnen. Dit is in lijn met het standpunt binnen de EHDS waarbij deze activiteiten zoveel mogelijk aan de bron moeten gebeuren*
- **SPE's voor gegevensaanvragen operationaliseren:** *Het ontvangen van gezondheidsgegevens door data users naar aanleiding van een gegevensaanvraag geschiedt in Secure Processing Environments (SPE's) die door een aangeduide SPE-provider worden uitgebaat. Er wordt minstens één SPE voorzien maar men houdt de mogelijkheid open om eventueel meerdere SPE's op te zetten (bv. per gegevensdomein). Binnen deze SPE's worden tijdelijke afgescheiden en beveiligde werkruimtes opgericht, die specifiek kaderen binnen de doeleinden van één gegevensaanvraag, teneinde veilig gebruik en verwerking van de gezondheidsgegevens te waarborgen. Data komt in versleutelde (geëncrypteerde) vorm binnen in de werkruimte, waarbij decryptie slechts plaatsvindt na geautomatiseerde validatie van de theoretische SCRA door de uitvoerder van de SCRA-controle.*

Technische bouwstenen

- **Service voor anonimiseren/pseudonimiseren:** *Deze service beperkt het risico op heridentificatie en voorziet de uitvoering van technieken om waarden te vervangen van indirecte identificeerbare gegevens (bv. adres, geboortedatum, ...) en gevoelige gegevens (bv. gewicht, BMI, ...). Zoals eerder aangehaald bij de rol van data holder, gebeurt dit zoveel mogelijk bij de data holder zelf in de data management tool. Enkel in het geval van de nood aan bijkomende*

⁹ EHDS-verordening artikel 55 (3)

anonimisering en/of pseudonimisering na het combineren van gegevens zal de SPE-provider bijkomende activiteiten uitvoeren.

- **SPE voor gegevensaanvragen:** *Een SPE voor gegevensaanvragen laat toe om gezondheidsgegevens veilig te ontvangen en te verwerken door data users voor tijdelijk gebruik. Dergelijke SPE's worden steeds opgezet door een aangewezen SPE-provider, waarbinnen een werkruimte wordt opgezet specifiek voor één bepaalde aanvraag.*