Technische, juridische, ethische en privacy-gerelateerde randvoorwaarden voor (her)gebruik van gezondheidsgegevens voor onderzoek

Vlaamse overheid

FLANDERS CARE

zorgnet ICURO

Colofon

Redactie: Peter Raeymaekers, Tom Balthazar, Yvonne Denier

Met inhoudelijke bijdrage van: Filip Veldeman, Peter Berghmans

Gewaardeerde dank aan: de meer dan 200 stakeholders die in deze ontwerpfase hun ideeën en suggesties met ons hebben gedeeld. Deze tekst kwam tot stand met ondersteuning van Flanders' Care en de Vlaamse Overheid.

Eindredactie: Yvonne Denier, Lieve Dhaene

D/2020/12067/4
ISBN 9789491323362

Citeren als: Raeymaekers, Peter; Balthazar, Tom & Denier, Yvonne (2020), *Big data in de gezondheidszorg. Technische, juridische, ethische en privacy-gerelateerde randvoorwaarden voor (her)gebruik van gezondheidsgegevens voor onderzoek.* Brussel: Zorgnet-Icuro

Zorgnet-Icuro vzw
Guimardstraat 1
1040 Brussel
post@zorgneticuro.be
www.zorgneticuro.be

Big data in de gezondheidszorg

Technische, juridische, ethische en privacy-gerelateerde randvoorwaarden voor (her)gebruik van gezondheidsgegevens voor onderzoek

Inhoud

Woord vooraf

We kunnen er niet omheen. Big data spelen in toenemend tempo een steeds grotere rol in de samenleving. De hoeveelheid data die wordt opgeslagen groeit exponentieel. Dat komt doordat we zelf steeds meer data opslaan (in de vorm van bestanden, foto's, filmpjes), doordat overheden, organisaties en bedrijven steeds meer data over burgers opslaan (registratie van gegevens allerhande), en doordat veel apparaten zelf data verzamelen, opslaan en uitwisselen (*sensor data* of het zogenaamde *Internet of Things*).

Het bijzondere aan big data is dat we werken met datasets die te groot zijn om door reguliere datamanagementsystemen te worden onderhouden. In het Engels spreekt men ook wel over *The seven V's of Big Data*. Het gaat dan over: *volume* (enorme hoeveelheid), *velocity* (grote snelheid), *variety* (ongestructureerde diversiteit), *variability* (variatie in de data zelf), *veracity* (grote verschillen in kwaliteit), *visualization* (meestal via tabellen en grafieken) en *value* (welke meerwaarde haal je uit analyse). Die enorme hoeveelheden en vormen van data zijn een belangrijke bron van informatie voor onderzoek en ontwikkeling, innovatie, beleid en marketing.

Ook in het domein van de gezondheidszorg spelen data en big data een almaar grotere rol, gaande van de concrete zorgpraktijk naar organisatie en beleid van zorg, over onderzoek, ontwikkeling en zorginnovatie, tot ja zelfs ons eigen dagelijkse leven en de keuzes die we daarin op elk moment maken door de dingen die we registreren en opslaan via allerhande *lifestyle apps*.

Van op de zijlijn toekijken zit niet in het DNA van Zorgnet-Icuro. Analyse, bewustmaking en positionering daarentegen wel. Daar is vandaag ook alle reden toe. Hierbij stellen we heel concreet de vraag hoe we ons als mens, burger, patiënt, organisatie, beleidsmaker, onderzoeker, industrie, e.a. moeten verhouden tot het fenomeen van big data inzake gezondheidsgegevens. Dat is een belangwekkende en urgente vraag die een breed en grondig maatschappelijk debat verdient.

Het is tevens de uitgangspositie en doel van dit document, nl. maatschappelijke reflectie en discussie op gang brengen over de volgende vragen. Hoe kunnen we meer doen met wat er reeds bestaat aan geregistreerde gezondheidsgegevens? Hoe kunnen we het bestaande potentieel aan data aanboren en inzetten voor een betere kwaliteit van zorg? Hoe kunnen we dat doen op een gestructureerde, juridisch en ethisch verantwoorde wijze? Volgens de principes van verantwoord gebruik van gegevens, dus in het kader van het algemeen belang en het publieke goed? Hoe kunnen we dat doen op transparante wijze? Hoe kunnen we dat doen op een manier waarop er in het publieke debat op verantwoorde wijze over kan worden gediscussieerd? Hoe kunnen we het publieke vertrouwen ter zake garanderen en behouden? Die en andere vragen zijn van groot belang in onze samenleving vandaag.

Met voorliggende discussietekst wil Zorgnet-Icuro het initiatief nemen voor een breed maatschappelijk debat over de technische, juridische, ethische en privacy gerelateerde randvoorwaarden van het gebruik van gezondheidsgegevens. De tekst werd geschreven in de periode januari-november 2019, na overleg en aftoetsing met vele belanghebbenden. Patiënten en burgers, overheden, industriële spelers, zorgaanbieders, mutualiteiten, academici, zowel individuele personen als groepen, federaties en koepels werden betrokken via dialoog en overleg, rondetafelgesprekken, een stakeholdermeeting en tekstuele review.

Voorliggende tekst is geen consensustekst. Toch heeft dit document er mee voor gezorgd dat tijdens het ontwikkelingsproces van dit project meer dan 200 personen en organisaties hun

licht hebben laten schijnen op de thematiek, hun eigen standpunt hierover hebben verwoord en hun stem hebben laten horen. Het heeft alvast geleid tot voortschrijdend inzicht voor alle partijen, tot overleg en debat. De scène is gezet.

Maar hiermee stopt het niet. Zorgnet-Icuro wil verder blijven bijdragen aan de collectieve ontwikkeling van een duurzaam model voor het gebruik van gezondheidsgegevens. Een model dat onderzoek toelaat met maatschappelijke finaliteit en dat uiteindelijk leidt tot een betere kwaliteit van zorg, een efficiëntere werking van het systeem, en verantwoorde technologie en innovatie in de zorg. Een model met transparante en rechtvaardige spelregels voor iedereen. Kortom, een model dat in het voordeel is van alle betrokken partijen in het zorglandschap en de bredere samenleving.

Als we iets hebben geleerd uit de COVID-19 crisis die ons land en de wereld in de ban heeft gehouden de voorbije maanden, dan is het wel het belang van data. De aanpak ervan, elke mogelijke uitweg uit de pandemie en de toekomstige preventie van een nieuwe grootschalige outbreak zijn gebaseerd op data. Er zijn de cijfergegevens omtrent besmettingen, opnames, overlijdens. Discussies omtrent aanpak en organisatie van contactopsporing lopen volop. Ook in dit verband worden er ontzettend veel data geregistreerd en gedeeld. Het belang van een goed gebruik van data staat buiten kijf. Toch roept ook dit vele technische, juridische, ethische en privacy-gerelateerde vragen op. Hier moeten we antwoorden op kunnen bieden, in naam van het algemeen belang en de gezondheid van iedereen. Het debat gaat voort.

Peter Raeymaekers
Tom Balthazar
Yvonne Denier
Stafmedewerkers

Marc Geboers
Directeur Algemene Ziekenhuizen

Margot Cloet
Gedelegeerd bestuurder

Samenvatting

Regelmatig rijst in de Vlaamse ziekenhuizen de vraag hoe de klinische gegevens waarover zij beschikken, kunnen worden ontsloten voor maatschappelijk relevant onderzoek. Die vraag vormt de concrete aanleiding van dit initiatief van Zorgnet-Icuro. Wij gingen met deze vraag aan de slag in januari 2019 en kwamen na verschillende overlegrondes met diverse betrokken partners uit bij een voorstel dat verder gaat dan de ziekenhuiscontext alleen.

Conceptvoorstel voor een onderzoeksplatform

We stellen een concept voor waarbij gegevens afkomstig van verschillende zorgverstrekkers worden gecombineerd. Dat levert niet alleen waardevolle onderzoeksresultaten op maar heeft ook een klinische meerwaarde op het oog. Concreet willen we de verschillende achtereenvolgende contacten van de zorgvrager met het zorgsysteem in kaart brengen (de *whereabouts*) en die verrijken met klinische gegevens die verbonden zijn met die contacten. Op die manier kan men inzicht verwerven in het traject dat een patiënt aflegt doorheen het zorgsysteem en dit in relatie brengen tot zijn of haar klinische gegevens. Deze mogelijkheid moet het verschil maken ten opzichte van de mogelijkheden die men wereldwijd heeft om aan big-data-onderzoek te doen in de gezondheidszorg. Tegelijk zijn de gegevens over het traject van de patiënt ook klinisch relevant.

Doelstelling van het platform

Het mogelijk maken van onderzoek en innovatie door het ontsluiten van de data afkomstig van de Vlaamse ziekenhuizen en van andere Vlaamse zorgactoren, en dat op een ethisch en juridisch verantwoorde manier, met respect voor de privacy van de patiënt en beheerd door een transparante en rechtvaardige governance structuur waarin de belangrijkste betrokkenen vertegenwoordigd zijn.

Realisatie

Voor de realisatie hiervan willen we zoveel mogelijk voortbouwen op de systemen van het eHealth-platform waarvan zorgverstrekkers vandaag al gebruikmaken. Daarnaast moet het initiatief complementair zijn aan de reeds bestaande big-data-initiatieven. De *whereabouts* maken het mogelijk gradueel meer en meer klinische gegevens toe te voegen aan de analyse of de uitwisseling. Op die manier kunnen we vrij snel tot resultaten komen als men zich enkel op de logistieke gegevens baseert. Voor het capteren van de gegevens bij de verschillende zorgverstrekkers zullen connectoren moeten worden voorzien die naargelang de onderzoeksvraag de relevante gegevens via een *Trusted Third Party* (TTP) kunnen ontsluiten voor de onderzoekers van het onderzoeksplatform.

Juridische punten

Het hergebruik van gezondheidsgegevens voor onderzoek kan een verantwoorde uitzondering zijn op het beginsel dat gegevens alleen mogen gebruikt worden voor het doel waarvoor zij werden ingezameld, namelijk diagnose en behandeling. De Algemene Verordening Gegevensbescherming laat onderzoek op gezondheidsgegevens toe, maar wel onder een reeks essentiële voorwaarden. Zo moet het gaan om onderzoek met een publiek belang, de patiënten moeten worden geïnformeerd en het is essentieel dat er technische en organisatorische maatregelen worden genomen om te vermijden dat identificeerbare patiëntengegevens zouden worden verspreid. De gegevens moeten daarom worden geanonimiseerd of gepseudonimiseerd.

Indien er betrouwbare controle is op het veilig en gepseudonimiseerd gebruik van de gegevens en uitgebreide informatie wordt gegeven, kan het verantwoord worden dat de gegevens worden hergebruikt zonder uitdrukkelijke toestemming van de patiënt, maar met de mogelijkheid om bezwaar aan te tekenen tegen het gebruik van de gegevens voor onderzoek.

Bij het organiseren van het data-platform zullen zeker ook strikte overeenkomsten (*Data Transfer Agreements*) moeten worden gemaakt tussen de bronnen en het platform, en tussen het platform en de gebruikers.

Privacy-aspecten

De uitwerking van het onderzoeksplatform dient te gebeuren op een informatieveilige manier. Hiervoor hanteren we vier werkingscriteria.

(1) **Confidentialiteit:** het onderzoeksplatform wordt enkel gehanteerd door een geautoriseerde gebruiker (een individu, organisatie of een systeem), waarbij diens handelen in lijn ligt met vooraf bepaalde regels.
(2) **Integriteit**: alle informatie op het platform is actueel en correct.
(3) **Beschikbaarheid:** betreft het niveau van dienstverlening.
(4) **Verantwoording:** verwijst naar de vraag 'wie deed wat, wanneer en waarom?'

Het voorgestelde onderzoeksplatform is risicoavers. Dat houdt in dat elk initiatief tot innovatie wordt afgewogen, rekening houdend met de noodzakelijke en haalbare kost voor informatieveiligheid. Informatieveiligheid is een kwaliteitskenmerk dat moet worden beheerd volgens de *Deming Circle* (plan-do-check-act). Het is een continu proces vanaf de ontwerpfase (*Security by Design*) dat blijft doorlopen tijdens uitrol en operationalisering. Hiervoor presenteren we een reeks technische, organisatorische, wetgevende, politieke en normatieve maatregelen.

Ethische randvoorwaarden

Vanuit ethisch oogpunt is het noodzakelijk om een orgaan op te richten dat waakt over het verantwoord gebruik van de data en dat kan bevestigen dat de vragen tot gebruik van de data wel vallen onder de uitzonderingen voorzien voor onderzoek in publiek belang. Het is aangewezen dat binnen het onderzoeksplatform een (ethische) commissie wordt opgericht die de aanvragen juridisch en ethisch toetst. Die commissie kan eventueel ook de beleidslijnen voor de controle van het proces vastleggen en toezien op de uitvoering van die controle.

Inhoudelijk gezien moet de finaliteit van gegevensdeling vanuit ethisch oogpunt gestoeld zijn op vier overkoepelende principes:
(1) de maatschappelijke meerwaarde ervan
(2) een rechtvaardige verdeling van risico's, baten en lasten
(3) respect voor individuen en groepen
(4) de garantie van publiek vertrouwen en duurzaam engagement. Bijzondere aandacht dient hierbij te gaan naar de concrete vormgeving en/of uitzondering van het principe van vrije en geïnformeerde toestemming.

Positie van dit voorstel in het maatschappelijke debat

Aangezien verschillende stakeholders bijdragen tot het succes van dit initiatief lijkt het logisch dat het eigenaarschap in het vervolgtraject niet enkel bij Zorgnet-Icuro blijft maar dat ook de stakeholders hun maatschappelijke verantwoordelijkheid kunnen opnemen. In de eerstvolgende fase van uitwerking nodigt Zorgnet-Icuro de betrokken stakeholders dan ook uit om gezamenlijk een structureel overleg te organiseren om enerzijds tot de initiële realisatie te komen van het platform en anderzijds om de complementariteit tot en samenwerking met de reeds lopende initiatieven te garanderen.

Hoofdstuk 1
Situering van het conceptvoorstel

Het voorstel voor een onderzoeksplatform voor het (her)gebruik van gezondheidsgegevens is ontstaan vanuit een specifieke maatschappelijke context waarin verschillende noden – maatschappelijk, juridisch, ethisch, technisch… – op urgente wijze samenkomen. In dit hoofdstuk situeren we de context van het voorstel, concretiseren we de doelstelling ervan en geven we inzicht in het totstandkomingsproces.

1.1. Nood aan maatschappelijk debat

Er is nood aan een maatschappelijk debat over de wijze waarop burgers, zorgvoorzieningen en zorgverstrekkers in een bredere context kunnen omgaan met het 'gebruik', 'ter beschikking stellen' of 'delen' van gezondheidsgegevens en dit in functie van het optimaliseren van de kwaliteit en werking van de gezondheidszorg.

In een internationale context zien we dat hierrond heel wat initiatieven bestaan. We stellen vast dat we in Vlaanderen wat aarzelen over het voeren van dit debat, dat vele aspecten (ethische, economische, juridische, technische …) kent. Met dit project willen we een aanzet doen, het debat lanceren en de krijtlijnen ontwikkelen voor goede praktijken in een duurzaam model van gebruik van gezondheidsgegevens.

1.2. Nood aan structurele uitwisseling

Het delen van gegevens tussen zorgvoorzieningen en ondernemingen gebeurt in de praktijk nog te vaak op individuele basis (met uitzondering van groepen voorzieningen die met hetzelfde elektronisch dossier werken).

Nochtans zijn er veel voordelen verbonden aan een meer structurele uitwisseling. Ondernemingen kunnen gegevens in de zorgvoorzieningen gebruiken om nieuwe producten en diensten te ontwikkelen die de zorggebruiker en/of de zorgvoorzieningen en/of het zorgsysteem ten goede komen. Zorgverstrekkers kunnen beter zicht krijgen op de aard en de eventuele gevolgen van de onderlinge interactie door gegevens te delen voor analyse. Ook de overheid heeft gegevens nodig voor het uitzetten van een zinvol en duurzaam beleid.

Algemeen kan men stellen dat een optimaal gebruik van de beschikbare gegevens aangewezen is om het juiste antwoord te kunnen vinden op de grote uitdagingen waarmee de samenleving wordt geconfronteerd, zo ook in de gezondheidszorg.

1.3. Nood aan verantwoorde gegevensdeling

Uiteraard dienen zorgverleners en zorgvoorzieningen privacyregels te respecteren ten aanzien van het individu, maar zij hebben evenzeer een plicht tot *accountability* ten aanzien van de overheid wanneer het aankomt op het ter beschikking stellen van gegevens die nuttig zijn om het beleid te onderbouwen. Van hen mag met andere woorden worden verwacht dat zij ten aanzien van de overheid en de samenleving verantwoording kunnen afleggen over de aanwending van overheidsmiddelen op basis van meetbare resultaten.

Dat geldt zeker wanneer de gedeelde gegevens een hulp kunnen zijn bij het uitbouwen van een verantwoord gezondheidsbeleid. Vaak knelt hier echter het schoentje. Zorgverleners vrezen immers dat de overheid de verkregen gegevens tegelijk ook voor controle en/of ongenuanceerde besparingsmaatregelen zal aanwenden. Ook hier is er nood aan transparantie, juiste garanties en wederzijds vertrouwen over de finaliteit van de gegevensdeling.

1.4. Nood aan juridische duidelijkheid

De GDPR of Algemene Verordening Gegevensbescherming is bedoeld om de privacy van het individu en dus ook van de persoon met een zorgnood te beschermen. Ook vroeger al konden medische gegevens worden gedeeld met dien verstande dat zij waar nodig worden geanonimiseerd of gepseudonimiseerd. In België heeft de federale overheid de toegang van zorgverleners tot het globaal medisch dossier wettelijk gereglementeerd. Dat is belangrijk vanuit het oogpunt van de vertrouwensrelatie tussen de patiënt en zijn zorgverlener.

De GDPR wil wetenschappelijk onderzoek bevorderen en laat uitzonderingen toe in het belang van het onderzoek. De Belgische Kaderwet Gegevensbescherming van 30 juli 2018 heeft deze *research exemption* verder uitgewerkt.

We hebben in dit rapport onderzocht hoe het onderzoeksplatform kan worden ontwikkeld op basis van de thans geldende Europese en nationale wetgeving.

We gingen daarbij ook in op belangrijke discussiepunten zoals de betrokkenheid van de patiënten (zowel individueel als in groep), de begrenzing van wetenschappelijk onderzoek met publiek belang en de mogelijkheid om (big-data)-onderzoek mogelijk te maken waarvan de doeleinden niet vooraf kunnen worden beschreven.

1.5. Ondersteuning door de Vlaamse overheid

Dit document kon tot stand komen door ondersteuning van de Vlaamse overheid via het 'Besluit van de secretaris-generaal tot toekenning van een subsidie aan Zorgnet-Icuro vzw voor het project 'Big Data Platform: verkenning en blauwdruk' dd. 10/12/2018.

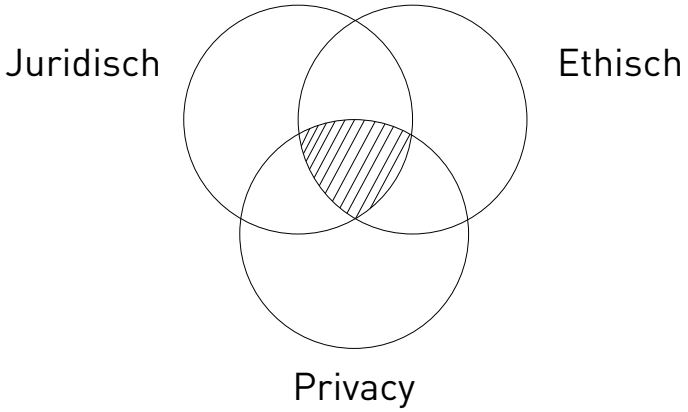
Omdat de samenleving er baat bij heeft dat collectief onderzoek op klinische gegevens in de gezondheidszorg snel tot resultaten kunnen leiden in de aanpak van de grote uitdagingen van deze tijd, is het belangrijk voor de Vlaamse overheid en voor alle stakeholders om over een gedegen visie hierover te beschikken.

Gezien de tweevoudige impact, namelijk een verbetering van de kwaliteit van zorg en de economische ontwikkeling die ermee gepaard gaat, past het initiatief perfect in de doelstellingen van Flanders' Care. Flanders' Care is het programma van de Vlaamse overheid dat inzet op innoveren en ondernemen in zorg met als missie 'op aantoonbare wijze en door innovatie het aanbod van kwaliteitsvolle zorg verbeteren en verantwoord ondernemerschap in de zorgeconomie stimuleren'. (www.flanderscare.be).

1.6. Doelstelling van dit document

In dit document worden de randvoorwaarden voor een onderzoeksplatform met de hierboven omschreven doelstelling op juridisch en ethisch vlak uitgewerkt alsook op het vlak van de privacy. Daarnaast wordt suggestie gegeven voor een technische realisatie van het platform. De technische suggestie is een mogelijkheid, maar er bestaan meerdere andere, die ook in ogenschouw kunnen worden genomen.

Het document geeft dus naast een concrete piste voor realisatie vooral de randvoorwaarden aan waarbinnen men gegevens op grote schaal en afkomstig van verschillende zorgactoren kan ontsluiten op een maatschappelijk verantwoorde wijze. Het is dan aan de deelnemers van het initiatief om te kijken wat binnen deze voorwaarden de technische mogelijkheden zijn en die te laten aansluiten bij de vraag.



Randvoorwaarden voor (her)gebruik van gezondheidsgegevens voor onderzoek

1.7. Totstandkoming van het document

Consultatieronde

Een nog belangrijke randvoorwaarde is dat het initiatief gedragen moet zijn door een zo breed mogelijke groep stakeholders. Om de posities en belangen van eenieder in kaart te brengen organiseerden we tussen januari en juni 2019 een maatschappijbrede consultatieronde. We danken iedereen die ons te woord heeft willen staan voor de medewerking en voor de vele constructieve reacties.

Technische analyse

Voor de uitwerking van het scenario voor de technische realisatie van het platform werd niet alleen gespecialiseerde expertise ingewonnen, maar is er ook afstemming gebeurd met een aantal experten op het terrein. Op die manier hebben we een inschatting kunnen maken van de praktische uitvoerbaarheid van het voorliggend scenario. Het concept werd ook voorgelegd aan de werkgroep ICT van Zorgnet-Icuro. Die werkgroep brengt de ICT-managers van de Vlaamse ziekenhuizen op geregelde tijdstippen samen.

Literatuurstudie

Een groot aantal randvoorwaarden kunnen worden afgeleid uit wetteksten of uit de academische literatuur. Een grootschalige literatuurstudie zorgde voor de uitgebreide juridische en ethische afbakeningen in dit document.

Workshop

Op 30 april 2019 organiseerden we in samenwerking met Agoria, BeMedtech en VOKA een workshop waarin de leden van deze organisaties hun vragen en noden op het vlak van onderzoek kenbaar konden maken. Via de methode van rondetafeloverleg kon iedereen uitgebreid aan bod komen. Plenair werd alles samengevoegd en meegenomen in de verdere tekstontwikkeling.

Stakeholderoverleg

Op 20 juni 2019 organiseerde Zorgnet-Icuro een bijeenkomst waarop alle stakeholders de gelegenheid kregen om hun feedback te geven op het conceptvoorstel en de respectieve randvoorwaarden. Ook hier werd er voldoende ruimte geboden voor iedere stem. De deelnemers aan het stakeholderoverleg zijn terug te vinden in bijlage 1.

Review & feedback

De voorliggende ontwerptekst werd in de periode september-oktober 2019 voorgelegd aan alle stakeholders voor review en feedback. Hierop werd actief en constructief gereageerd door meer dan 200 actoren en organisaties. De tekst werd onderworpen aan een uitgebreid scala aan perspectieven. Daar waar mogelijk werd de tekst aangepast op basis van de bedenkingen en suggesties. Aangezien de feedback op verschillende punten diametraal was, was het niet altijd mogelijk om het in de tekst te integreren. Wel hebben we alle reacties verzameld en samenvattend gebundeld. U kan ze terugvinden in bijlage 3. Op die manier kunnen ze het voortgaande debat mee blijven stofferen.

Hoofdstuk 2
Wat is de doelstelling van het onderzoeks-platform?

Hoe kunnen we bestaande of toekomstige gezondheidsgegevens van burgers, zorgvoorzieningen en zorgverstrekkers zo optimaal mogelijk delen binnen een brede maatschappelijke context? Dat wil zeggen, op een manier dat het ten goede komt aan iedereen: zorggebruikers, zorgvoorzieningen, het zorgsysteem, zorgondernemers, de burgers en de samenleving? Dat is onze startvraag én doelstelling. Om die verder te verhelderen specifiëren we in dit hoofdstuk het werkdomein, met name het maatschappelijk verantwoord onderzoek, ontwikkeling en overheidsbeleid, het type en de finaliteit van onderzoek, type gebruikers en soorten gegevens. We staan ook stil bij enkele sterktes en uitdagingen van dit project.

2.1. Kerndoelstelling

Het mogelijk maken van onderzoek en innovatie door het ontsluiten van de data afkomstig van de Vlaamse ziekenhuizen en van andere Vlaamse zorgactoren en dit op een ethisch en juridisch verantwoorde manier, met respect voor de privacy van de patiënt en beheerd door een transparante en rechtvaardige governance structuur waarin de belangrijkste betrokkenen vertegenwoordigd zijn.

Over welk type onderzoek gaat het?

Het betreft onderzoek op bevolkingsniveau oftewel 'collectief onderzoek' dat inzicht biedt in patiëntenstromen en het effect op patiënten nagaat van onder meer de volgende elementen:

- omgevingsfactoren
- geneesmiddelen
- medische technologie
- verstrekte zorgen

Dit door de analyse van de gegevens van patiënten die voortkomen uit hun interactie over een langere periode met verschillende zorgverstrekkers (ziekenhuizen, huisartsen…).

Wat is de finaliteit van het onderzoek?

De finaliteit kan verschillend zijn:

- wetenschappelijk: het creëren van nieuwe inzichten;
- beleidsmatig: het ontwikkelen van nieuw beleid;
- terugbetaling: het al dan niet kunnen aantonen van bedoelde of onbedoelde effecten van geneesmiddelen, implantaten of andere technologie die voor terugbetaling in aanmerking komen.

De finaliteit is zeker niet:

- controle van artsen, ziekenhuizen of andere zorgverstrekkers;
- controle van patiënten;
- informatie over kwaliteit van ziekenhuis/zorgverstrekker/behandeling;
- commercieel onderzoek naar bv. voorschrijfgedrag.

Voor het monitoren van kwaliteit en voor de noodzakelijke controle op zorgenverstrekkers en zorginstellingen bestaan thans reeds andere mechanismen. Deze kunnen mogelijk worden verbeterd en ook gebruik maken van moderne data-analyse-technieken, maar dat kan niet het doel zijn van het voorgestelde onderzoeksplatform.

Wie kan van het platform gebruikmaken?

Mogelijke gebruikers van het platform zijn alle actoren die onderzoek verrichten op gezondheidsgegevens. Het kan zowel gaan om zorgvoorzieningen, welzijnsactoren, universiteiten en kennisinstellingen, overheden als commerciële partijen (geneesmiddelenproducenten, producenten van *medical devices* enz.).

De bepalende factor voor toelaatbaarheid van het gebruik van gezondheidsgegevens ligt niet zozeer in het antwoord op de vraag *wie* van het onderzoeksplatform gebruik wil maken, dan wel in het antwoord op de vraag wat de eigenlijke *finaliteit* van het onderzoek is en welk type gegevens daarvoor nodig zijn.

2.2. Onderzoek op collectief niveau

Het voorliggend conceptvoorstel voor een onderzoeksplatform komt niet in het vaarwater van klinisch onderzoek zoals dat in de ziekenhuizen wordt uitgevoerd. Ons voorstel is gericht op **big data** (cf. de in het woord vooraf vermelde *Seven V's of Big Data* – groot volume, hoge snelheid, combinatie van gegevens, grote diversiteit en variatie aan gegevens, grote kwaliteitsverschillen enz.)

Het aanboren van een groot volume data en de combinatie van data afkomstig van verschillende zorgverstrekkers zal omwille van de datakwaliteit en complexiteit de onderzoeksmogelijkheden beperken. Vandaar dat het onderzoek zich veeleer op het niveau van de bevolking of van grote groepen zal situeren dan wel zich zal richten op groepen van veeleer beperkte omvang.

2.3. Vlaamse ziekenhuizen en andere Vlaamse zorgactoren

De regionale scope van dit initiatief is **Vlaanderen**. Dat houdt niet zozeer verband met de projectsponsor, maar is vooral ingegeven uit overwegingen in verband met complexiteit en snelheid. Het aantal organisaties die als stakeholder kunnen betrokken worden stijgt aanzienlijk in aantal indien we de actieradius zouden verbreden naar België. Bovendien is de technische uniformiteit in Vlaanderen groter (binnenkort zijn er bijvoorbeeld nog slechts drie of vier EPD-leveranciers actief op de Vlaamse markt).

Niettemin moet het op termijn toch de ambitie zijn om dit uit te breiden naar een **nationale schaal**. Daarmee zou niet alleen de hoeveelheid gegevens toenemen die voor onderzoek beschikbaar wordt, maar het zou ook beter aansluiten bij de werking van de stakeholders die op nationaal niveau actief zijn, bijvoorbeeld de ziekenfondsen. Het onderzoek kan ook raken aan federale bevoegdheden zoals bijvoorbeeld de terugbetaling van geneesmiddelen, waarvoor gegevens uit alle landsdelen nodig zijn.

De technische uitwerking van het voorliggend conceptvoorstel moet daarom rekening houden met de uitbreiding naar het nationaal niveau.

2.4. Data afkomstig van verschillende zorgactoren

Zoals eerder gezegd gaat het voorliggend voorstel verder dan de ziekenhuiscontext alleen. Indien het initiatief zich zou beperken tot het ontsluiten van de gegevens waarover de algemene ziekenhuizen in Vlaanderen beschikken, dan zou het vanuit internationaal perspectief

nauwelijks meerwaarde bieden. Gegevens afkomstig van EPD's zijn commercieel en in grote hoeveelheden verkrijgbaar.

Wat daarentegen het verschil kan maken is het **combineren van gegevens afkomstig van verschillende zorgactoren**. In de combinatie zit informatie over het traject dat de patiënt volgt. Dat levert longitudinale inzichten op. Dergelijke inzichten kunnen enerzijds belangrijke indicatoren zijn voor de effectiviteit van een bepaalde behandeling of hulpmiddel; anderzijds kunnen de patronen die worden waargenomen indicatoren zijn van goede zorg(paden).

Door de vergevorderde digitalisering van de meeste zorgactoren en het bestaan van een aantal gemeenschappelijke platformen en basisdiensten is Vlaanderen ook een geschikte regio om die gegevens te combineren.

Het niet beperken tot de eigen gegevens heeft een belangrijke weerslag op het eigenaarschap van het initiatief. Zorgnet-Icuro kan dan wel de initiatiefnemer zijn, het zullen de deelnemende zorgactoren zijn die het (gedeeld?) eigenaarschap zullen moeten opnemen en het initiatief mee zullen moeten sturen en vormgeven.

2.5. Waarom nog een big-data-initiatief in de gezondheidszorg?

Er werden in Vlaanderen en in België reeds een aantal initiatieven genomen. We moeten ons dus terdege de vraag stellen: wat kan de **meerwaarde** zijn van een bijkomend initiatief zoals het voorliggende voorstel? Kan het aansluiten bij reeds bestaande initiatieven? Wat voegen we toe?

2.5.1. Homogenisering in de ziekenhuissector

Eerst een vooral is er het element van homogenisering. Momenteel is er geen eenduidige benadering om klinische gegevens te ontsluiten. Niet alleen is de mate waarin ziekenhuizen hun gegevens ontsluiten verschillend over de ziekenhuizen heen, ook de manier waarop die gegevens worden ontsloten is niet voor alle ziekenhuizen dezelfde.

Het preciseren van de randvoorwaarden in dit document zou moeten kunnen leiden tot een veel meer uniforme aanpak, wat tot meer duidelijkheid zal leiden voor de zorgverstrekkers die hun gegevens aanleveren, voor de patiënten wiens gegevens worden gebruikt, voor de gebruikers van de gegevens en voor de samenleving in haar geheel.

2.5.2. Klinische meerwaarde

De combinatie van gegevens afkomstig van verschillende zorgverstrekkers heeft niet enkel een meerwaarde voor onderzoek maar kan ook een klinische meerwaarde hebben. Ook ziekenhuizen hebben interesse in patiëntenstromen vanuit kwaliteitsoogpunt of om het klinisch aanbod te optimaliseren. Als je bijvoorbeeld het traject bij verschillende zorgverstrekkers kent dat de patiënt heeft afgelegd, dan heb je een beter zicht op het voortraject van de patiënt op het moment dat die zich aandient bij een voorziening.

Het is die klinische meerwaarde die zorgverstrekkers uiteindelijk zal moeten motiveren om deel te nemen aan het initiatief en hun gegevens ter beschikking te stellen. Ze krijgen er beter en doeltreffender inzicht voor in ruil. In principe moet het initiatief hierdoor zelf rekruterend zijn.

2.5.3. Aansluiting bij bestaande initiatieven

Het objectief moet zijn om zoveel mogelijk aansluiting te vinden bij bestaande initiatieven en zoveel mogelijk gebruik te maken van de infrastructuur die reeds aanwezig is.

Vermits de doelstelling maatschappelijk is geïnspireerd, is het logisch dat gekeken wordt naar de meest efficiënte weg naar realisatie en de meest duurzame verankering. Daarenboven ligt het eigenaarschap bij verschillende stakeholders, met als gevolg dat men de drempel voor deelname zo laag mogelijk moet houden. Maakt men onvoldoende gebruik van bestaande systemen, technische standaarden enz., dan is de kost voor deelname aan het initiatief voor de verschillende types van zorgverstrekkers te hoog.

Bijlage 2 bevat een overzicht van de ons bekende Belgische initiatieven.

2.6. Wat zijn sterktes en wat zijn de belangrijkste uitdagingen?

2.6.1. Sterktes

Door de onafgebroken inspanningen van alle stakeholders in de Belgische gezondheidszorg (bv. in het kader van het plan eGezondheid, maar ook ver daarbuiten) kunnen we, zonder hiervoor over een precieze meetlat te beschikken, vaststellen dat de digitalisering van de Belgische gezondheidszorg zich het voorbije decennium echt heeft doorgezet. In zoverre zelfs dat Vlaanderen bij de regio's kan worden gerekend die geschikt zijn voor het big-data-initiatief zoals geformuleerd in deze tekst. We benadrukken drie belangrijke sterktes.

Betere klinische software

Ziekenhuizen, huisartsen, thuisverpleging, apothekers... beschikken allemaal over klinische software die verder in kwaliteit toeneemt. Tegelijk neemt het aantal aanbieders van medische software af. Door die consolidatie worden de resterende software *vendors* groter in omvang en hebben zij meer mogelijkheden om aan ontwikkeling te doen.

Hoewel vrije tekst nog bij vele zorgverstrekkers de norm is, kunnen deze systemen steeds meer gestructureerde gegevens registreren.

Het eHealth platform

Het eHealth-platform heeft ervoor gezorgd dat men voor een aantal basisdiensten op de systemen van de overheid kon terugvallen. Dat heeft het Belgische systeem in zijn geheel overzichtelijk gehouden en de actoren hebben efficiëntiewinsten kunnen realiseren. Het heeft met kmehr als berichtenstandaard ook voor een gestructureerde manier van gegevens-uitwisseling gezorgd. De hub/metahub-structuur speelt een cruciale rol in het voorstel voor de technische uitwerking van het onderzoeksplatform. Het voorstel voorziet in een maximale aansluiting bij de reeds aanwezige systemen. Een belangrijke kanttekening hierbij is dat het klinisch gebruik van de eHealth systemen nog verre van optimaal is, wat een belangrijke beperking betekent in termen van datakwaliteit.

Codering

De overheid heeft de laatste jaren sterk ingezet op codering. Zo is er bijvoorbeeld een nieuwe versie van de SAM databank voor geneesmiddelen aangeboden en investeert men in de vertaling van Snomed codes voor de ziekenhuizen. Het gebruik van de kluizen heeft er ondertussen ook voor gezorgd dat heel wat taalproblemen tussen systemen en types zorgverstrekkers zijn opgelost. Het probleem is nog niet helemaal van de baan, maar de ontwikkelingen zijn zeer hoopgevend. Hier geldt dezelfde opmerking als voor de eHealth systemen: de basis is gelegd, maar er is nog een lange weg te gaan in termen van gebruik, met ook hier in tussentijd de overeenkomstige beperkingen inzake datakwaliteit.

2.6.2. Uitdagingen

De uitdagingen zijn verbonden met de manier waarop we de digitalisering in België hebben georganiseerd, maar zijn tegelijk eigen aan elk big-data-initiatief. We vermelden er drie.

Datakwaliteit

In België is steeds de filosofie gehanteerd de systemen te optimaliseren voor klinisch gebruik en niet voor een harmonisering van de systemen. Op zich is dat een te verdedigen keuze, maar het heeft ertoe geleid dat de gegevens moeilijk uitwisselbaar zijn tussen verschillende systemen en dat men telkens tot afspraken moet komen over de structuur van de gegevens die men wenst uit te wisselen. Dat is meestal geen gemakkelijke oefening.

Daarenboven wordt nog maar weinig gebruik gemaakt van de mogelijkheid die de pakketten bieden om gestructureerd te registreren. *Natural Language Processing* kan hier wel een positieve rol spelen, maar dat neemt niet weg dat vooral de datakwaliteit bepalend zal zijn voor de onderzoeksmogelijkheden.

Het probleem van de datakwaliteit inspireert sommigen tot visies over één patiëntendossier dat wordt gedeeld tussen alle zorgverstrekkers. Dat is echter niet de visie van Zorgnet-Icuro. EPD's of andere systemen zijn immers niet louter gegevensbanken maar sturen ook de klinische processen doorheen de voorziening. Het is daarom noodzakelijk dat een dergelijk systeem is geoptimaliseerd voor de interne werking dan wel voor externe uitwisseling.

Expertise en ontwikkelingscapaciteit

Zelfs al stijgt de ontwikkelingscapaciteit van de Belgische ICT-leveranciers, dan nog is de mate waarin zij nieuwe projecten kunnen aanvatten beperkt en is de *roadmap* voor de komende periode al goed gevuld. Daarnaast is er ook bij hun klanten zorgverstrekkers geen, nauwelijks of onvoldoende expertise inzetbaar, niet enkel wegens ontoereikende budgetten, maar ook omdat dergelijke profielen moeilijk aan te trekken zijn. Ook het aantrekken van de gepaste expertise voor gegevensanalyse en voor de technische realisatie in het algemeen vormt een grote uitdaging.

Verwachtingen

De mogelijkheden van big data zijn natuurlijk enorm en onder ideale omstandigheden kan veel worden gerealiseerd. Maar zoals hierboven beschreven zijn de omstandigheden niet ideaal en kunnen zelfs kleine tekortkomingen een grote hypotheek leggen op de onderzoeksmogelijkheden. Hoge verwachtingen houden dus een risico in. We moeten onze verwachtingen altijd toetsen aan wat realistisch, haalbaar en duurzaam mogelijk is.

Al deze uitdagingen nopen tot bescheidenheid en voorzichtigheid bij de verdere concretisering. De datakwaliteit moet onder controle zijn door in eerste instantie te kiezen voor eenvoudig te uniformiseren gegevens of voor gegevens die al in een standaardformaat beschikbaar zijn. De ontwikkelingscapaciteit van leveranciers en de ICT-expertise van de zorgverstrekkers mag niet al te zeer worden aangesproken. De verwachtingen mogen niet onrealistisch zijn. Het aanspreken van onze sterktes en het technisch concept op zich (zie verder) moeten voldoende basis bieden voor zinvol onderzoek en voor klinische meerwaarde.

Hoofdstuk 3
Hoe ziet het concept er precies uit?

Op basis van de bovenvermelde inzichten zijn dit de uitgangspunten van het voorgestelde concept.

- *We beogen een **combinatie** van gegevens van verschillende zorgverstrekkers;*
- *Er dient een **klinische meerwaarde** voor zorgverstrekkers en patiënten uit voort te komen;*
- *We steunen op **maximaal hergebruik** van bestaande systemen;*
- *We beogen **weinig tot geen drempels** voor **deelname** door zorgverstrekkers;*
- *We zetten in op **maximale privacy-garantie**.*

In dit hoofdstuk geven we meer inzicht in de zorgtrajecten die we op het oog hebben, de soorten van data die daarvoor nodig kunnen zijn en de mogelijke scenario's die we hiervoor kunnen aanwenden.

3.1. Traject van zorgcontacten

Het basisidee bestaat erin om het zorgcontact tussen patiënt en zorgverstrekker te registreren, de zogenaamde *whereabouts* van de patiënt. Het in kaart brengen van die *whereabouts* geeft informatie over het **traject** dat de **patiënt** heeft afgelegd binnen het **zorgsysteem**. Worden de *whereabouts* aangevuld met klinische gegevens van de patiënt, dan kan die combinatie niet alleen worden gebruikt om logistieke informatie te genereren, maar ook om klinische inzichten te bekomen.

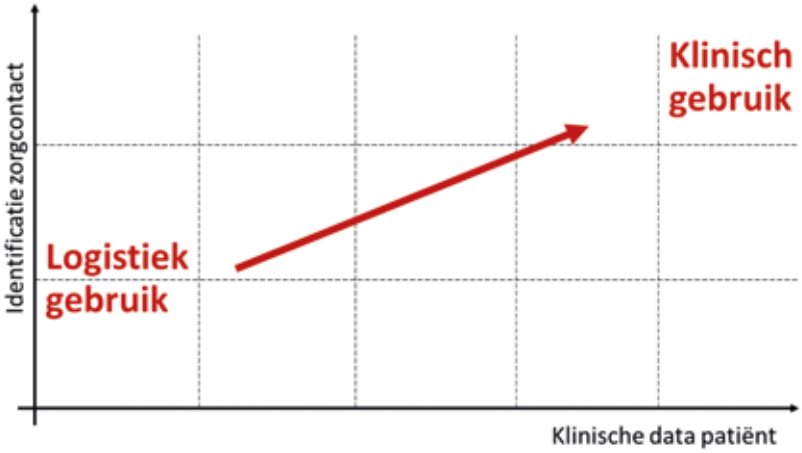
We willen met de *whereabouts* dus vertrekken van een goed gedefinieerd gegeven dat nu al in de software van de zorgverstrekker wordt geregistreerd en dat met relatief beperkte inspanningen op uniforme wijze kan worden verzameld. Hierbij kunnen we ervan uitgaan dat de **datakwaliteit** van dit logistiek gegeven hoog is en geschikt voor logistiek gebruik. Waar het bij de *whereabouts* om goed gedefinieerde en relatief eenvoudig te standaardiseren gegevens gaat, is dat bij klinische gegevens veelal niet het geval. Tenzij voor gegevens die al volgens een bepaalde codering worden geregistreerd (zoals bijvoorbeeld vandaag het geval is voor labo-resultaten) is de datakwaliteit van de beschikbare klinische gegevens meestal beperkt.

Vermits het combineren van logistieke gegevens en klinische gegevens pas zin heeft bij voldoende hoge datakwaliteit gaat het concept uit van een **gradueel toenemend gebruik** van klinische gegevens, naargelang de inspanningen die nodig zijn om een voldoende hoge datakwaliteit te bekomen en naargelang de meerwaarde van de verwachte conclusies van het gewenst onderzoek.

Onderstaande figuur geeft een overzicht van de data die kunnen worden ontsloten en in welke mate die data geanonimiseerd zijn.

- Op de **horizontale as** gaat het over **patiëntgegevens**: van links naar rechts is steeds meer informatie beschikbaar.
- Op de **verticale as** gaat het over de **zorgverstrekkers**: van onder naar boven is steeds meer informatie beschikbaar.

Op die manier ontstaan een aantal **scenario's** die het mogelijk maken om het project te faseren, alsook de bijkomende juridische en ethische aspecten in kaart te brengen (*cf.* §3.3.)



Graduele toename gebruik klinische gegevens

Ziekenhuizen en andere zorgverstrekkers hebben in het verleden reeds interesse getoond om over de *whereabouts* van de patiënt te beschikken. Hoewel niet kwantificeerbaar bestaat er dus vanuit klinisch oogpunt een **vraag** naar die gegevens. Niet enkel de gegevens uit het **verleden** kunnen van nut zijn door inzage in het gelopen zorgtraject, maar ook de (quasi-) **real-time-informatie** kan van belang zijn. Zo is het voor de huisarts of GMD-houder bijvoorbeeld belangrijk te weten of de patiënt al dan niet is opgenomen in het ziekenhuis en in welk ziekenhuis dat dan is. Hierin verschilt het concept van de big-data-analyses die de overheden en mutualiteiten op hun gegevens kunnen uitvoeren. Per definitie zijn die laatste niet real-time vermits zij de gegevens vaak vele maanden na het genereren ervan ontvangen. Hierdoor verdwijnt de klinische relevantie.

Essentie van het concept

De combinatie van de klinische informatie die vervat zit in de *whereabouts* en de maatschappelijke meerwaarde die het onderzoek kan opleveren zouden voor zorgverstrekkers voldoende motivatie moeten zijn om de beoogde gegevens te delen (*whereabouts*/klinisch) mits slechts beperkte inspanning vereist is en mits deelname geen meerkosten met zich meebrengt.

3.2. Soorten data

3.2.1. Patiëntenbewegingen

Patiëntenbewegingen (of *whereabouts*) geven een longitudinaal beeld van de patiëntencontacten binnen een bepaald **zorgtraject**. Bv. een patiënt gaat naar de huisarts, wordt doorverwezen naar de praktijk van een specialist, wordt een tijdje opgenomen in het ziekenhuis, krijgt nadien thuiszorg en een aantal beurten kinesitherapie en gaat naar één of enkele controleraadplegingen ter opvolging.

Ook uitbreiding naar de welzijnssector is mogelijk. Eveneens bij uitbreiding kunnen ook contacten in het kader van **preventie** worden geregistreerd (bezoek aan zwembad, fitness, natuurvoedingswinkel…) of *mobile health* gegevens van de patiënt zelf (stappenteller, sportapps…), maar dat is momenteel niet de prioriteit.

3.2.2. Administratieve gegevens

Daarnaast kan het ook gaan over administratieve gegevens van de patiënt (die gaan al meer in de richting van 'patiëntidentificatie'). Afhankelijk van het specifieke onderzoeksscenario

(*cf.* §3.3.) kunnen die gegevens (rijksregisternummer, naam, voornaam, geboortedatum, woonplaats…) geheel of gedeeltelijk ter inzage zijn, ofwel geaggregeerd, ofwel gepseudonimiseerd zijn (door een *Trusted Third Party*) waardoor patiëntnummers door onderzoekers niet terug te voeren zijn naar individuele patiënten (zie hiervoor ook hoofdstuk 5 'Juridische analyse' en hoofdstuk 6 'Informatieveiligheid).

3.2.3. Klinische data

Hier betreft het klinische gegevens van de patiënt (bv. labo, radiologie, patiëntendossier…). In dit geval kan het gaan om eenvoudige klinische data-elementen (reden van opname, bepaald type pathologie, bepaalde medicatie…).

Het kan ook gaan om meer uitgebreide, gestructureerde informatie, bijvoorbeeld een SUMEHR (*Summarised Electronic Health Record*) waarmee op een gestructureerde manier kan worden verwezen naar een kerndossier met reden van opname, voorgeschiedenis, huidige medicatie, allergieën enz.

3.2.4. Gegevens zorgverstrekkers

Een vierde mogelijke datastroom betreft de gegevens over de zorgverstrekkers. Ook over de verschillende 'haltes' in het regionale zorgtraject van de patiënt kan informatie worden verzameld (huisarts, ziekenhuis, thuiszorg, …) die in meerdere of mindere mate ter beschikking kan worden gesteld in functie van de noden en doelstellingen van het onderzoek.

3.2.5. Andere gegevens

Het kan ook interessant zijn andere gegevens te ontsluiten, bv. andere administratieve gegevens dan die van de patiënt of kostgegevens.

3.3. Drie scenario's

3.3.1. Scenario 'Workflow onderzoek'

In dit scenario (de linkerkolom uit figuur 2) wordt van de **patiënt** geen klinische informatie verzameld, enkel de *whereabouts*. Er is van de patiënt enkel een gepseudonimiseerd patiëntnummer beschikbaar (aangemaakt via een *Trusted Third Party*, *cf.* hoofdstuk 5 en 6).

Van de **zorgcontacten** wordt alle informatie verzameld, maar die kan – in functie van de onderzoeksvraag – in mindere of meerdere mate ter beschikking worden gesteld. Bv. enkel type contact (ziekenhuis, huisarts, …), of ook locatiegegevens (postnummer van ziekenhuis of huisarts), of de volledige informatie (naam/nummer van het ziekenhuis, naam/rizivnummer van de huisarts).

Dit is een goed scenario om mee te starten. De uitdaging in dit scenario is om zoveel mogelijk zorgcontacten en types zorgcontacten te laten aansluiten op het systeem, zodat er **regionaal** en **longitudinaal onderzoek** mogelijk is. Dat kan gaan over ziekenhuizen, huisartsen, apothekers, kinesisten, paramedici, niet-zorgpartijen enz.

3.3.2. Scenario 'Populatieonderzoek'

In dit scenario worden aan de *whereabouts* van de patiënt één of meerdere klinische data-elementen toegevoegd: bv. reden van opname, type pathologie of medicatie. Informatie over de zorgcontacten kan geanonimiseerd blijven of worden ontsloten zoals in het scenario *workflow* onderzoek.

Op die manier is het mogelijk om te **segmenteren** in functie van een bepaalde **pathologie** of **medicatie** en aan **populatieonderzoek** te doen.

Technisch en organisatorisch bestaat de extra uitdaging in dit scenario erin de klinische data-elementen op een gestructureerde en gecodeerde manier te verzamelen, bv. met gebruik van Snomed (voor diagnoses), of ATC-codes (voor medicatie).

In dit scenario start men best met een **piloot**, waarna de *lessons learned* in een breder kader kunnen worden toegepast.

3.3.3. Scenario 'Big data'

In dit scenario wordt aan de *whereabouts* van de patiënt een geanonimiseerde SUMEHR toegevoegd (*Summarized Electronic Health Record*), zoals nu gebruikt door de huisartsen. Die bevat gestructureerde informatie over het kerndossier van de patiënt (huidige medicatie, voorgeschiedenis, reden van contact enz.) en laat toe om complexer onderzoek te doen. Naast de mogelijkheid om longitudinaal onderzoek te doen (dankzij de *whereabouts*), biedt de SUMEHR ook bij elk contact een gepseudonimiseerde 'snapshot' van het kerndossier (*continuity of care record*) dat een synthese geeft van de klinische informatie van de patiënt.

Hoofdstuk 4
Hoe zouden we dat technisch kunnen realiseren?

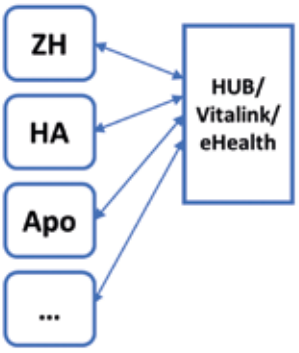
In dit document werken we de randvoorwaarden uit voor een conceptvoorstel van onderzoeksplatform voor gegevensdeling op juridisch, ethisch en privacy-gerelateerd vlak. Maar niet alleen conceptueel, ook technisch willen we bekijken hoe we dat kunnen realiseren. In dit hoofdstuk presenteren we een mogelijk concept voor de technische realisatie van het onderzoeksplatform. Hierbij houden we maximaal rekening met de bovenvermelde randvoorwaarden voor maatschappelijk verantwoorde gegevensdeling.

Een mogelijkheid

We willen benadrukken dat het technisch voorstel een mogelijkheid is. Er bestaan meerdere andere mogelijkheden voor technische realisatie, die we ook in ogenschouw kunnen nemen. Zo willen we de mogelijkheid tot aansluiting bij bestaande platformen te maximaliseren.

4.1. Huidige infrastructuur

Laat ons starten met de bestaande infrastructuur. We beschikken vandaag in België over een goed georganiseerde hub- en meta-hubstructuur, aangevuld met de kluizen, om gegevens uit verschillende bronnen toegankelijk te maken voor zorgverleners die een therapeutische relatie hebben met de patiënt.



De hubs, vitalink en het eHealth platform in het algemeen zijn in Vlaanderen/België de systemen van voorkeur voor het veilig uitwisselen van zorggegevens. Documenten van de ziekenhuizen worden ter beschikking gesteld via de hub en de eerstelijnszorgverstrekkers gebruiken vitalink voor het delen van gegevens. Ook de eHealthBox is een vaak gebruikt systeem, maar dan voor punt-tot-punt communicatie.

De meest gestructureerde en best gecodeerde gegevens zijn onder meer:

- Medicatieschema: actueel overzicht van de medicatie die de patiënt neemt;
- SUMEHR: snapshot met de belangrijkste medische informatie over de patiënt op dat moment;
- Laboresultaten;
- Vaccinatiegegevens

Dat wil nog echter nog niet zeggen dat die gegevens in de praktijk optimaal gecodeerd en gedeeld worden, wel integendeel. Maar het raamwerk waarbinnen dat kan gebeuren is wel al aanwezig en verwacht wordt dat de datakwaliteit verder zal stijgen. We merken hierbij ook op dat zich eveneens veel gegevens bevinden bij niet-klinische actoren die niet kunnen worden gedeeld via deze kanalen, bijvoorbeeld bij de overheid en bij de mutualiteiten.

4.2. Gegevenscaptatie

Aangezien de *whereabouts* ook in de klinische praktijk zullen worden gebruikt, is het maximaal aanwenden van de huidige infrastructuur zoals hierboven omschreven de enige realistische optie om de gegevens te ontsluiten. Via de diensten van het eHealth-platform kan naar analogie met het delen van andere gegevens via hubs en kluizen de therapeutische relatie worden vastgesteld en kan de geïnformeerde toestemming worden gecontroleerd (voor de juridische en ethisch aspecten zie hoofdstuk 5 en 7).

Wie toegang krijgt tot de *whereabouts* kan worden vastgelegd in de toegangsmatrix die wordt beheerd door de werkgroep Toegang onder het eHealth-platform. Toegang tot de klinische gegevens gebeurt uiteraard via dezelfde bestaande kanalen.

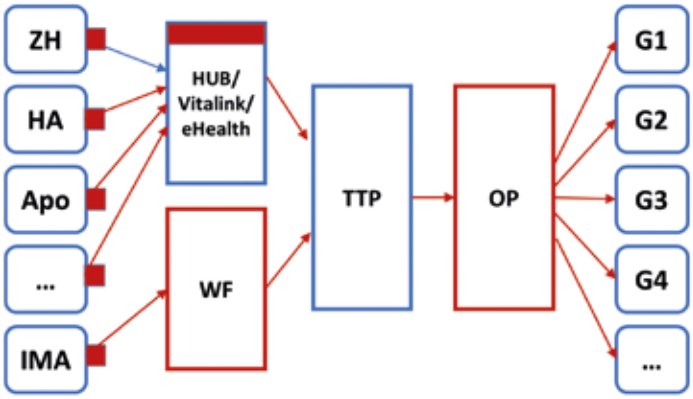
Om gebruik te kunnen maken van de huidige infrastructuur is het nodig dat de *whereabouts* kunnen worden gecapteerd in de systemen van de verschillende zorgverstrekkers. Dat kan gebeuren door het installeren van een connector in de softwaresystemen van de zorgverstrekkers (de rode blokjes in de figuur). Idealiter wordt zo'n connector centraal ontwikkeld en ter beschikking gesteld van de softwareleveranciers. De connector moet ook in staat zijn om de nodige klinische gegevens te verbinden aan de gecapteerde logistieke informatie. De complexiteit van de ontwikkeling en het gebruik van de connector is afhankelijk van de aard van die klinische gegevens. In het begin is het vooral zaak die complexiteit tot het minimum te reduceren of zelfs enkel onderzoek te doen op basis van de *whereabouts*. Gaandeweg kan de connector dan worden uitgebouwd om meer en meer klinische gegevens te capteren die via het eHealth-platform toegankelijk zijn (medicatieschema, SUMEHR...). Nog verder in de toekomst kan men denken aan het gebruik van gegevens die zich in de softwaresystemen van de zorgverstrekkers bevinden.

Wenst men gebruik te maken van gegevens die afkomstig zijn van niet-klinische actoren (zoals het IMA), dan moet een apart kanaal worden voorzien. Niettegenstaande een aantal van deze actoren ook gebruikmaken van de basisdiensten van het eHealth-platform hebben zij geen toegang tot de hubs en tot de kluizen, en kunnen die dan ook niet worden gebruikt voor het delen van deze gegevens. Deze gegevens zullen dus via een aparte omgeving (WF op de figuur) moeten worden gecapteerd omdat deze actoren geen therapeutische relatie hebben met de patiënt.

Het is uiterst belangrijk dat de zorgverstrekkers geen extra inspanning moeten leveren om de connector te installeren of te gebruiken. Ook de inspanningen van de softwareleveranciers moeten zo beperkt mogelijk zijn. Het is immers de bedoeling dat een zo groot mogelijk aantal zorgverstrekkers deelneemt aan het platform en dus moet ook de drempel voor de softwareleveranciers zo laag mogelijk zijn. Een centrale ontwikkeling en centraal beheer van de connector zijn dus de aangewezen piste.

4.3. Gegevensverwerking

Onderstaande figuur visualiseert het proces van gegevenscaptatie naar gegevensverwerking. Een centrale tussenrol wordt vervuld door de *Trusted Third Party* (TTP) en het onderzoeksplatform (OP).



4.3.1. Anonimisering en pseudonimisering

Het onderzoeksplatform krijgt uiteraard geen toegang tot individuele patiëntengegevens. Bovendien laat de mate waarin de gebruikte gegevens geanonimiseerd of gepseudonimiseerd zijn een betere verwerking van de gegevens toe (zie hoofdstuk 5).

Aangezien de gegevens van de patiënt afkomstig zijn van verschillende bronnen is een volledige anonimisering bij de authentieke bronnen echter niet mogelijk. Bijgevolg is het nodig om te werken met een *Thrusted Third Party* (TTP) die de gegevens van de verschillende zorgverstrekkers over dezelfde patiënt kan combineren zonder dat de identiteit van de patiënt moet worden doorgegeven aan het onderzoeksplatform. De TTP moet instaan voor garanties op dat vlak.

Men kan ook denken aan het initieel verwerken van de gegevens bij de zorgverstrekkers i.p.v. bij de *Trusted Third Party*. Op die manier wordt de privacy nog beter gegarandeerd. Nadelen hiervan zijn echter de bijkomende complexiteit en bijhorende inspanningen aan de kant van de zorgverstrekker (terwijl die zo minimaal mogelijk zouden moeten worden gehouden) en een mogelijk verlies aan relevante gegevens.

4.3.2. Patiëntselectie

Op basis van het onderzoek dat de gebruiker (G1, G2...) van het onderzoeksplatform (OP) wil uitvoeren, zal een selectie van patiënten moeten worden gemaakt. Dat kan gaan om patiënten die passeerden in een bepaalde regio, bij een specifieke zorgverlener of - via bevraging van de bijhorende klinische informatie - om patiënten met een bepaalde pathologie, medicatie, allergie..., afhankelijk van de kwaliteit van de klinische gegevens die voorhanden zijn. De connector zal in staat moeten zijn om in de gegevens van de zorgverstrekkers op zoek te gaan naar de patiënten die aan de criteria van de onderzoeksvraag voldoen.

4.3.3. Genereren van onderzoeksresultaten

Van zodra de geschikte patiënten zijn geselecteerd geeft de TTP per patiënt de gecombineerde gegevens door aan het onderzoeksplatform. De TTP doet dat proportioneel, d.w.z. dat enkel gegevens die noodzakelijk en relevant zijn voor het onderzoek worden doorgegeven. Immers, niet elke onderzoeksvraag vergt dezelfde graad van detaillering van de gegevens. Gewenste onderzoeksresultaten kunnen variëren naar aggregatieniveau (bv. aantal gevallen van een bepaalde pathologie per regio), waardoor het onderzoeksplatform niet over gegevens van individuele patiënten hoeft te beschikken.

4.4. Suggestie voor een technische implementatie via XDW

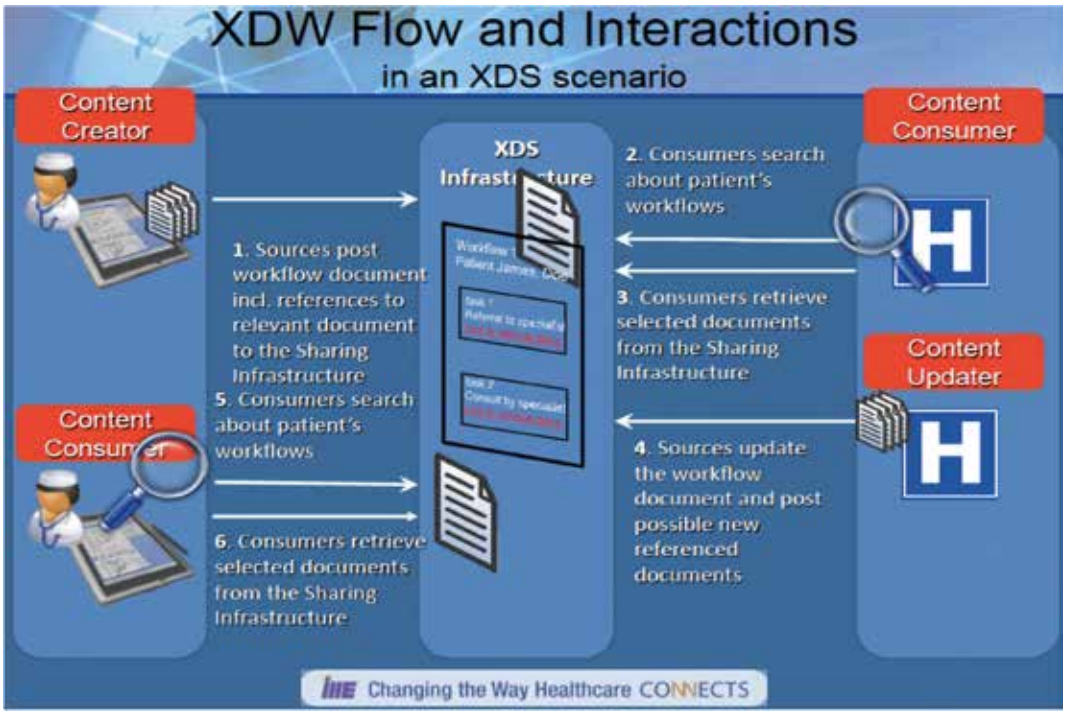
4.4.1. Opzetten van een workflow context

Het hierboven geschetste systeem is realiseerbaar via XDW (*Cross Enterprise Document*

Workflow). Dat is een technische standaard die voortbouwt op en complementair is aan XDS (*Cross Enterprise Document Sharing*), de technologie die onder meer UZ Leuven gebruikt voor het implementeren van zijn hub-infrastructuur.

Die technologie laat toe om regionale workflows op te zetten (en op een gestandaardiseerde manier uit te wisselen) in een workflowdocument. De standaard is ontwikkeld voor de ondersteuning van transmurale samenwerking maar kan ook de basis vormen voor gefilterde en/of stapsgewijze toegang tot workflowgegevens voor onderzoek.

Onderstaande figuur geeft een schematische voorstelling van het werkingsprincipe van XDW. Voor meer info, zie: https://wiki.ihe.net/index.php/Cross_Enterprise_Workflow.



4.4.2. Ervaringen met implementatie van XDW

Veneto

XDW wordt al met succes toegepast in de Regio Veneto in Italië. Vorig jaar (2018) was er een bezoek met IHE België (onder de vleugels van Agoria) aan de IHE Connectathon in Den Haag, waar de succesvolle implementatie werd toegelicht door Claudio Saccavini: 3800 huisartsen, 4300 ziekenhuisartsen en 1330 apotheken zijn op het systeem aangesloten en genereren 40 miljoen ePrescriptions en 20 miljoen eReferrals per jaar.

België

In België werd ervaring opgedaan bij Abrumet waar een XDW implementatie werd gedaan voor het opzetten van eRefferals. Op 22 en 23 februari 2019 organiseerde Abrumet samen met IHE Belgium en Agoria een eHealth Connectathon waar leveranciers integratietesten konden opzetten naar dit platform.

Nederland

Ook Nederland kijkt in de richting van XDW, zoals blijkt uit een recent document van NICTIZ en de Regionale SamenwerkingsOrganisaties.[1]

4.4.3. Hoe ziet zo'n workflow document eruit?

We geven hier meer info over de inhoud van een workflow document. De toepassingsmogelijkheden voor de inzet in het kader van een big-data-architectuur wordt verder toegelicht.

Elke workflow die wordt opgezet krijgt een specifieke workflow ID (*cf. infra*, illustratie). De workflow wordt gedocumenteerd in een workflowdocument waarin op een gestandaardiseerde manier informatie wordt vastgelegd over de patiënt, de zorgverlener en het workflowproces (een verzameling van taken en acties).

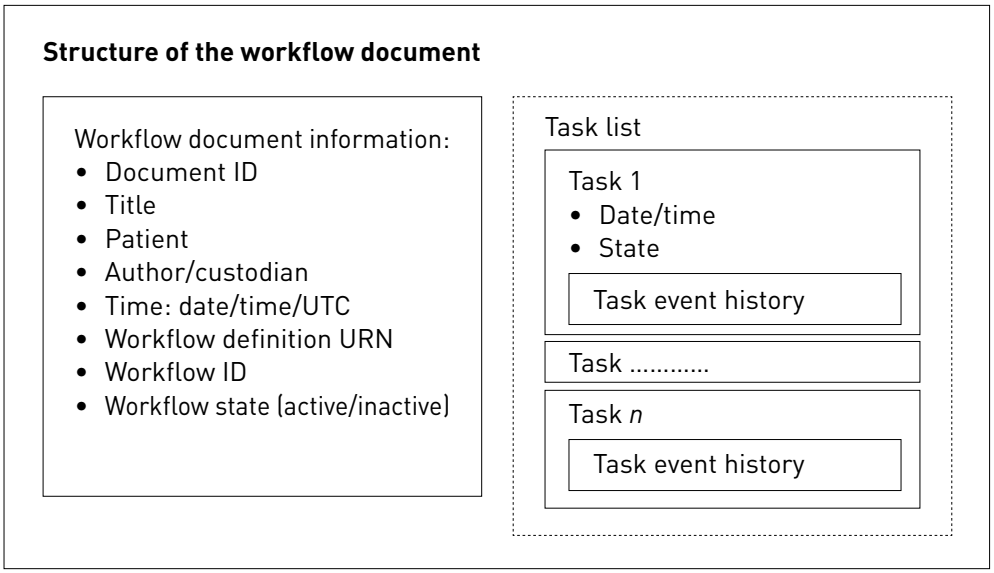
De workflow kan op twee manieren werken:

1. Men kan **taken toewijzen** wanneer de uitvoerders vooraf bepaald zijn.
2. Men kan ook kiezen voor een **publish/subscribe** systeem om taken kenbaar te maken (*publish*) aan een doelgroep zonder vooraf vast te leggen wie ze precies zal uitvoeren. Deelnemers aan het proces kunnen dan intekenen op bepaalde taken (*subscribe*) zonder vooraf te weten welke opdrachtgever de workflow heeft opgezet.

Taken en acties kunnen ook vergezeld zijn van verwijzingen naar klinische of administratieve documenten. Het kan gaan om inputinformatie ter voorbereiding van een taak (bv. een verwijsbrief) of outputinformatie met de resultaten van een taak (bv. een verslag van een onderzoek).

Klinische informatie wordt dus enkel toegevoegd via referentie aan een extern document (input/ter voorbereiding of output/als resultaat), niet in het workflowdocument zelf). Dat maakt het gemakkelijker om indien nodig de workflowinfo over *whereabouts* en de toegang tot klinische informatie apart te beheren.

Wanneer een deelnemer een update doet van het workflowdocument (door een taak af te werken en te documenteren of een nieuwe taak te starten) wordt een nieuwe actieve 'snapshot' van het workflow document gemaakt die de vorige versie vervangt. De historiek van de verschillende versies van die workflowdocumenten wordt bewaard.



Bright L. & Goderre J. (Eds.), Underlying Standards That Support Population Health Improvement, CRC Press, 2017.

4.4.4. Hoe verloopt big-data-onderzoek via XDW?

Voor elke patiënt kan een gepseudonimiseerd workflowdocument worden aangemaakt, waarbij elk patiëntencontact met een zorgverlener (bij de huisarts, in het ziekenhuis…) aanleiding geeft tot een update van het workflowdocument met een extra workflowstap (een taak/gebeurtenis) die de *whereabouts* vastlegt met (indien van toepassing) ook een referentie aan een extern document met bijhorende klinische informatie (zie verder).

Die workflowcontext kan worden aangevuld met **administratieve gegevens** van patiënt en zorgverstrekker.

- **Patiënt**: unieke identificatie (rijksregisternummer) te anonimiseren via *Trusted Third Party* (webservices van eHealth-platform).
- **Zorgverstrekker**: via CoBRHA (*Common Base Registry for HealthCare Actor*), de gemeenschappelijke database van de openbare instellingen die bevoegd zijn voor de erkenning van de actoren in de gezondheidszorg in België.

Daarnaast kan de workflowcontext ook worden aangevuld met **klinische gegevens**.

Klinische informatie wordt enkel toegevoegd via referentie aan **externe documenten** (input/ter voorbereiding, of output/als resultaat), niet in het workflowdocument zélf). Als voorbeeld nemen we de Sumehr.[2]

Concreet: de SUMEHR

De Sumehr is (net zoals het workflowdocument) een **snapshot**. Die informeert op een gestructureerde manier over de gezondheidstoestand van de patiënt, gevalideerd door de auteur, op een bepaald moment, relevant, en ter ondersteuning van continuïteit van zorg. De Sumehr werd aanvankelijk gebruikt in de context van niet-geplande zorg, maar kan ook worden gebruikt bij geplande zorg, bijvoorbeeld als aanvulling bij een verwijsbrief voor een hospitalisatie of consultatie.

De **patiëntinformatie** in de Sumehr kan via dezelfde **pseudonimisering** passeren als de patiëntinformatie van het workflowdocument. De **zorgverstrekker** in de SUMEHR (hcparty element) loopt via dezelfde manier als de auteur van het workflowdocument. Verder biedt de SUMEHR de vereiste **structuur** om allergieën, risico's, problemen/diagnoses, behandelingen, medicatie op een gestructureerde manier weer te geven.

De tools om Sumehrs aan te maken en te tonen zijn al in alle huisartsenpakketten beschikbaar. Er is technisch al behoorlijk veel ervaring met het aanmaken en tonen van SUMEHRS. Er is dus **bestaande infrastructuur** en **ervaring**.

De Sumehr laat toe om informatie in te geven via **vrije tekst** en/of via **codeersystemen** (bv. ICD-10). Er wordt gewerkt aan verdere richtlijnen voor de representatie van de nationale referentieterminologie Snomed CT in de SUMEHR. Bijvoorbeeld:

Vrije tekst:	Buikpijn
Snomed CT:	21522001 | Abdominal pain (finding)

Waar nodig kunnen ook andere aanvullende documenten worden toegevoegd (in Kmehr, HL7 FHIR, of HL7 CDA) zoals gedocumenteerd op de standaarden pagina van het eHealth-platform.

Hoofdstuk 5
Technisch kan het, maar mag het ook? Juridische analyse

In de vorige hoofdstukken situeerden we het concept van het onderzoeksplatform tegen een bredere maatschappelijke horizon, formuleerden we de doelstellingen en concretiseerden we het platform in een conceptueel en technisch voorstel. Nu is het tijd voor een gedegen juridisch perspectief. We stellen ons de vraag of het (her)gebruik van gezondheidsgegevens juridisch gezien allemaal wel mag. Kan het verlopen op rechtsgeldige en rechtszekere wijze? En zo ja, waarmee dienen we dan allemaal rekening te houden? Op die vragen probeert dit hoofdstuk een antwoord te bieden.

5.1. Probleemstelling vanuit juridisch perspectief

5.1.1. Centrale vragen

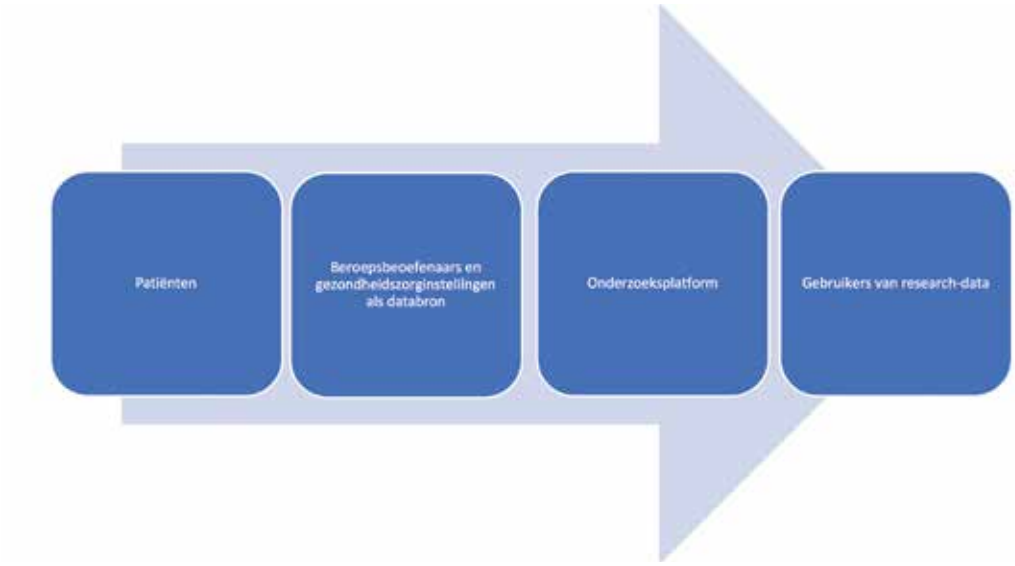
In dit onderdeel maken we een eerste analyse van de mogelijkheden om op rechtsgeldige en voldoende rechtszekere wijze het beoogde platform op te richten en te laten functioneren. Hierbij gaat het vooral om de mogelijkheden voor de verschillende databronnen (verzorgingsinstellingen, artsenpraktijken, apothekers enz.) om de door hen beheerde gezondheidsgegevens op geoorloofde, veilige en betrouwbare wijze ter beschikking te stellen aan het platform.

Het platform zal immers pas de nodige meerwaarde voor het wetenschappelijk onderzoek kunnen bieden indien meerdere actoren uit verschillende sectoren van de gezondheidszorg bereid worden gevonden om de door hen beheerde data ter beschikking te stellen van het onderzoeksplatform en zijn gebruikers. Dat kan en mag enkel indien het juridisch toegelaten is en indien dat het vertrouwen van patiënten en burgers niet aantast.

Naast de vraag of de actoren in de gezondheidszorg gegevens ter beschikking mogen stellen van het platform, is er de vraag of een dergelijk platform eigenlijk wel mag worden opgericht, welke regels daarbij moeten worden gerespecteerd en hoe het dient te worden beheerd.

Tot slot rijst de vraag onder welke juridische voorwaarden de onderzoekers als 'gebruikers' van de data die kunnen opvragen en ontvangen en wat ze er na ontvangst mogen mee doen.

Onderstaand schema visualiseert de stappen in het proces en de gegevensstroom die we juridisch willen onderzoeken.



5.1.2. Variant model

Een variante met belangrijke juridische implicaties is de mogelijkheid dat de bronnen van de data (de zorgverstrekkers en zorginstellingen) géén data overdragen, ook in niet-geanonimiseerde of gepseudonimiseerde vorm, maar enkel toelaten dat bijzondere big-data-analysetechnieken worden verricht *binnen* hun eigen bestanden en systemen, waarna **enkel de algemene conclusies van die analyses** worden overgedragen. Op die wijze gebeurt geen overdracht van persoonsgegevens en zal in belangrijke mate buiten het dwingend kader van de GDPR kunnen worden gewerkt. Het feit dat geen persoonsgegevens worden overgedragen aan derden neemt niet weg dat sommige interne analyses ook als verwerking kunnen worden beschouwd zodat de verwerkingsverantwoordelijke moet kunnen verantwoorden op grond waarvan dat gebeurt.

Een andere variante is dat er geen data worden overgedragen, maar dat aan onderzoekers wordt toegelaten om toegang te krijgen tot bestaande databanken. In dergelijke gevallen blijft de GDPR onverkort van toepassing

5.1.3. Situering voorliggende analyse: work in progress

Deze tekst vormt een eerste analyse, in het kader van de initieel beoogde haalbaarheidsstudie in 2019, en houdt rekening met de opmerkingen en suggesties die mondeling werden geformuleerd op het stakeholderplatform van 20 juni 2019, en met de opmerkingen die nadien schriftelijk werden doorgegeven.

Het spreekt voor zich dat met het oog op een daadwerkelijke realisatie van het beoogde onderzoeksplatform een meer doorgedreven en gedetailleerd juridisch onderzoek noodzakelijk zal zijn. Juridische analyse op dit domein is dus te begrijpen als *work in progress*.

Het zal ook noodzakelijk zijn dat het uitgewerkte kader wordt voorgelegd aan de vereiste advies- en toetsingsorganen, zoals de Gegevensbeschermingsautoriteit, de Vlaamse Toezichtscommissie en het Informatieveiligheidscomité. Voor de individuele gezondheidszorgbeoefenaars zal een advies van hun deontologisch advies- of toezichtsorgaan (zoals de Orde der Artsen of de Psychologencommissie) aangewezen zijn.

We analyseren de mogelijkheden vanuit het **momenteel geldende wettelijk kader**, en dus vanuit de hypothese dat er voor de oprichting van het onderzoeksplatform geen bijzonder wettelijk of decretaal initiatief wordt genomen. Indien het noodzakelijk of aangewezen wordt geacht, zullen wij dat signaleren.

We analyseren de situatie vanuit de **bestaande praktijk**, waarbij het niet gebruikelijk is dat aan patiënten die zich voor diagnose en/of therapie aanbieden bij een arts of een andere zorgverstrekker of verzorgingsinstelling toestemming wordt gevraagd voor het gebruik van hun gegevens voor wetenschappelijk onderzoek. We gaan dus na of het geoorloofd is dat eerder ingezamelde ('historische') klinische gegevens worden gebruikt voor onderzoek. Er wordt ook onderzocht of het in de toekomst noodzakelijk en/of wenselijk is dat er wel om een dergelijke toestemming zou worden gevraagd.

5.1.4. Uitwerking

Deze analyse is als volgt uitgewerkt:

- Wij geven eerst een overzicht van de toepasselijke wetgeving (§5.2.);
- We beschrijven nadien de voor de problematiek toepasselijke regels en principes van de privacywetgeving en in het bijzonder de wijze waarop de Algemene Verordening Gegevensbescherming (AVG of GDPR) wetenschappelijk onderzoek mogelijk wil maken (§5.3.);

- We passen deze principes vervolgens toe:
    - Op de data-bronnen (§5.4.);
    - Op het op te richten onderzoeksplatform (§5.5.);
    - Op de gebruikers (§5.6.).
- We formuleren een kort besluit dat de basis kan vormen voor politieke besluitvorming, maatschappelijk debat en verder onderzoek (§5.7.).

5.2. Toepasselijke wetgeving

5.2.1. Centraal toetsingskader: de AVG

De gegevens waarover de met het onderzoeksplatform mogelijk samenwerkende gezondheidsactoren beschikken, zijn zonder enige twijfel **persoonsgegevens**, zelfs indien die met het oog op het (her-) gebruik voor onderzoek nadien worden geanonimiseerd. Ze vallen dan ook (minstens tot bij hun anonimisering) onder het toepassingsgebied van de **Algemene Verordening Gegevensbescherming (AVG)**, vooral bekend onder het Engelstalige acroniem **GDPR** (afkorting van de General Data Protection Regulation).[3] De AVG vormt dan ook het centrale toetsingskader voor dit onderzoek.

5.2.2. Andere relevante wetgeving

Naast de AVG als centraal toetsingskader zijn ook nog relevant:

- De '**kaderwet'** van 30 juli 2018[4], waarbij de *research exemption* werd uitgevoerd in het Belgisch recht;
- De bestaande regelgeving over de uitwisseling van gezondheidsgegevens, zijnde de **eHealth-wet**[5] en het **Vlaams decreet over de uitwisseling van gezondheidsgegevens**[6];
- De nieuwe **Kwaliteitswet**[7], die pas in 2021 in werking zal treden, maar waarmee toch best rekening wordt gehouden;
- De **Patiëntenrechtenwet.**[8]

Bij de analyse werd ook rekening gehouden met de **resolutie betreffende het gebruik van big data in de gezondheidszorg**, zoals aangenomen op 28 maart 2019 in de Kamer van Volksvertegenwoordigers.[9]

5.3. De AVG wil wetenschappelijk onderzoek bevorderen en mogelijk maken

5.3.1. Algemeen

De Algemene Verordening Gegevensbescherming bevestigde en verscherpte het bestaande kader over de bescherming van de privacy bij de verwerking van persoonsgegevens. Dat heeft evident gevolgen voor het gebruik van persoonsgegevens voor wetenschappelijk onderzoek. Toch bevat de AVG meerdere bepalingen waaruit blijkt dat de Europese wetgever het wetenschappelijk onderzoek en het gebruik van persoonsgegevens bij **wetenschappelijk onderzoek** wil bevorderen en faciliteren. Dat blijkt vooreerst uit de overwegingen bij de AVG. We kunnen o.m. verwijzen naar de overwegingen of '**consideransen'**:

- Overweging 33, waarbij het concept van de **brede toestemming** (*broad consent*) wordt toegelicht[10];
- Overweging 50, waarbij het principe wordt toegelicht dat de **'verdere verwerking' voor wetenschappelijk onderzoek** (onder voorwaarden) kan worden beschouwd als een met de aanvankelijke doeleinden verenigbare verwerking. Dat is een belangrijke uitzondering op het beginsel van de 'doelbinding' of *purpose limitation* van art. 5.b. AVG[11];
- Overweging 156, waarin de mogelijke **afwijkingen op de rechten van de betrokkenen** in het belang van wetenschappelijk onderzoek, worden toegelicht[12];
- Overweging 157, waarin de **potentiële voordelen** van de koppeling tussen registers wordt toegelicht, in het bijzonder in wetenschappelijk onderzoek op gezondheidsgegevens.[13]

Maar ook in de tekst zelf van de AVG zijn een aantal **bepalingen** opgenomen ter bevordering van het gebruik van persoonsgegevens bij wetenschappelijk onderzoek.

Wij lichten hierna kort de bepalingen toe die relevant kunnen zijn voor de toetsing van de mogelijkheden om op rechtsgeldige en geoorloofde wijze het onderzoeksplatform uit te bouwen en passen die nadien toe op:

- De mogelijkheden voor de actoren in de gezondheidszorg om als 'data-bronnen' samen te werken met het onderzoeksplatform en in functie van de goedgekeurde aanvragen gegevens over te dragen aan het onderzoeksplatform (§5.4.);
- De mogelijkheden om het onderzoeksplatform uit te bouwen (§5.5.);
- De mogelijkheden om de gegevens ter beschikking te stellen van onderzoekers (§5.6.).

5.3.2. Uitzondering op het beginsel van doelbinding

Een van de belangrijke beginselen van de AVG is de '**doelbinding'** of *purpose limitation*. Persoonsgegevens moeten *voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.* Toegepast op de actoren in de gezondheidszorg houdt dat in dat gegevens die werden ingezameld voor diagnose en therapie in beginsel niet nadien voor een ander doeleinde mogen worden verwerkt.

Daar wordt evenwel aan toegevoegd dat *de verdere verwerking met het oog op archivering in het algemeen belang, **wetenschappelijk** of historisch onderzoek of statistische doeleinden (..) overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden (wordt) beschouwd*.

Het kan dus geoorloofd zijn dat gegevens die initieel werden ingezameld voor een ander doel nadien worden verwerkt voor **wetenschappelijk onderzoek**. Dat dient wel te gebeuren overeenkomstig art. 89, lid 1 en dus met zogenaamde 'passende waarborgen' om het beginsel van de minimale gegevensverwerking te garanderen. Dat betekent vooral dat de nodige maatregelen moeten worden genomen om identificatie van de betrokkenen te vermijden en dat er dus moet worden overgegaan tot **anonimisering** of **pseudonimisering** (cf. §5.3.5.).

5.3.3. Welke zijn de rechtmatige grondslagen voor verwerking van persoonsgegevens?

Voor elke verwerking – en dus ook voor de 'verdere verwerking' bij hergebruik van gegevens voor wetenschappelijk onderzoek – is altijd een **rechtmatige grondslag** nodig.

Voor de verwerking van gezondheidsgegevens geldt bovendien een principieel verbod tot verwerking van die gegevens. Om dergelijke gevoelige gegevens te mogen verwerken moet men zich kunnen beroepen op de uitzonderingen voorzien in art. 9.2. (waaronder de toestemming van de betrokkene (a), de noodzaak voor diagnose of therapie (h), of de noodzaak voor wetenschappelijk onderzoek (j)).

De verschillende mogelijke grondslagen voor de verwerking zijn vermeld in art. 6.1. AVG. Het gaat om mogelijke voorwaarden waar niet noodzakelijk cumulatief moet aan voldaan zijn. Artikel 6.1. bepaalt: *De verwerking is alleen rechtmatig indien en voor zover aan **ten minste één** van de onderstaande voorwaarden is voldaan*.

Nadien volgt een opsomming van mogelijke **rechtmatigheidsgrondslagen**, waaronder:

- De toestemming van de betrokkene (a);
- De noodzaak voor de uitvoering van een overeenkomst (b);
- Een wettelijke verplichting (c);
- De bescherming van vitale belangen (d);
- De vervulling van een taak van algemeen belang (e);
- De behartiging van de 'gerechtvaardigde belangen van de verwerkingsverantwoordelijke' (f).[14]

Belangrijk: **De toestemming van de betrokkene kan dus één van de rechtmatige grondslagen zijn, maar is niet steeds de enige basis om persoonsgegevens te mogen verwerken.** Er zijn gevallen waarin persoonsgegevens kunnen en mogen worden verwerkt zonder dat hiervoor voorafgaand de toestemming van de betrokkene diende te worden gevraagd. Dat neemt niet weg dat de betrokkene alle rechten (zoals het recht op informatie, inzage en correctie) behoudt.

Om misverstanden hierover te vermijden is het zeker voor de gezondheidszorg belangrijk om te beklemtonen dat er een **verschil** bestaat tussen de toestemming die nodig is voor de **medische handeling** en de toestemming voor de **verwerking van persoonsgegevens** die worden ingezameld om die handeling mogelijk te maken.

- Zo zal een patiënt op grond van het *Informed Consent*-beginsel en de Wet Patiëntenrechten onbetwistbaar toestemming moeten geven om een operatie uit te voeren, maar is voor het aanleggen van het patiëntendossier naar aanleiding van die operatie niet noodzakelijk een afzonderlijke toestemming nodig.

Dat werd ook aanvaard en toegelicht in het ontwerp van GDPR- gedragscode voor zorgvoorzieningen.[15]

- Ook bij deelname aan een experiment of een geneesmiddelenproef moet eenzelfde onderscheid worden gemaakt. Een dergelijke proef kan en mag enkel worden uitgevoerd na geïnformeerde toestemming van de patiënt of proefpersoon.[16] Voor de verwerking van persoonsgegevens bij een geneesmiddelenproef is niet altijd een afzonderlijke toestemming nodig.

Dat werd uitdrukkelijk aanvaard in de opinie die hierover op 23 januari 2019 werd uitgebracht door de European Data Protection Board. In *opinion 3/2019 concerning the Questions and Answers on the interplay between the Clininical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)* wordt besloten dat bij verwerking in het kader van wetenschappelijk onderzoek drie rechtmatigheidsgronden mogelijk zijn, namelijk:

- Een taak van **algemeen belang** in de zin van art. 6.1.e AVG, samen te lezen met art. 9.2.i of 9.2.j AVG;
- De **gerechtvaardigde belangen** van de verwerkingsverantwoordelijke in de zin van art. 6.1.f. AVG, samen te lezen met art. 9.2.j AVG;
- in bijzondere omstandigheden, wanneer aan alle voorwaarden voldaan is, de **toestemming** van de betrokkene in de zin van art. 6.1.a en art. 9.2.a AVG.

Hoewel het advies is uitgebracht naar aanleiding van vragen over de toepassing van verordening 536/2014 over geneesmiddelenproeven[17], heeft het toch een bredere draagwijdte. Het ondersteunt de stelling die reeds in de eerste doctrine werd ingenomen dat toestemming geen noodzakelijke voorwaarde is voor wetenschappelijk onderzoek op gezondheidsgegevens en dat het ook niet de aangewezen rechtmatigheidsgrond is.[18] In de Opinion 3/2019 wijst de European Data Protection Board o.m. op het feit dat toestemming niet steeds volwaardig vrij kan worden gegeven, gelet op de onvermijdelijke *imbalance of power*. Tot op heden heeft dit advies wel nog niet geleid tot een uniforme visie over de noodzaak van toestemming om gegevens te kunnen verwerken voor wetenschappelijk onderzoek. Lidstaten zoals het Verenigd Koninkrijk en België vinden dat niet nodig en (mits de nodige waarborgen) ook niet wenselijk. In Frankrijk, Duitsland en Italië wordt het toch wenselijk geacht.[19.]

Zonder toestemming:

De mogelijkheid dat er zonder uitdrukkelijke toestemming van de patiënt in het belang van wetenschappelijk onderzoek kan worden overgegaan tot hergebruik van gezondheidsgegevens houdt absoluut geen vrijbrief in voor de gezondheidszorginstellingen die de gegevens beheren.

Vooreerst is het enkel mogelijk mits de (hierna besproken) 'passende waarborgen' om de identificatie van de patiënt maximaal te vermijden.

Bovendien moet zeker informatie over deze verwerking worden gegeven en behoudt de patiënt in beginsel alle rechten voorzien door de AVG, zoals het recht op inzage, op gegevenswissing, op beperking en op bezwaar. Het recht op bezwaar (dat enkel vervalt indien de verwerking is gebaseerd op een 'taak van algemeen belang' [20]) kan ook inhouden dat er een vorm van opt-out-systeem wordt ontwikkeld en gepromoot.

Met toestemming:

Indien wel beroep wordt gedaan op toestemming, sluit overweging 33 bij de AVG niet uit dat gebruik wordt gemaakt van een zogenaamde ruime toestemming of *broad consent*.

Het is immers zeer moeilijk om gedetailleerd en voor langere termijn het onderzoeksdoel te omschrijven omdat de resultaten mogelijk nieuwe onderzoeksvragen en onvoorziene hypotheses kunnen genereren en omdat bij big-data-analyse met *machine learning* wordt gewerkt, waarbij de systemen op auto-adaptieve wijze de data onderzoeken.[21]

Het gebruik van *broad consent* veronderstelt volgens de aanbevelingen van de World Medical Association (de 'Tapei'-declaration'[22]) en de zogenaamde CIOMS-guidelines[23] wel een gepast *governance* systeem over het gebruik van de data en degelijke informatie over dat *governance* systeem.[24]

5.3.4. Noodzaak van transparante communicatie & informatie

De mogelijkheid om zich voor de verdere verwerking van gegevens te beroepen op een andere grondslag dan de toestemming van de patiënt neemt niet weg dat het recht op informatie van de patiënt en de verplichting van de verwerkingsverantwoordelijke om in die informatie te voorzien onverkort blijven bestaan.

Belangrijk: **Patiënten moeten weten dat verdere verwerking voor wetenschappelijk onderzoek mogelijk is.** Transparantie is cruciaal. Naast de juridisch noodzakelijke informatie beschreven in de artikelen 12, 13 en 14 AVG is het aangewezen dat proactief, helder en positief wordt gecommuniceerd om het vertrouwen in wetenschappelijk onderzoek te doen groeien.

- Dat kan op algemeen maatschappelijk niveau: door publiekscampagnes rond verantwoord hergebruik van gezondheidsgegevens;
- Alsook op niveau van de gezondheidszorginstellingen die zowel bij de opname als tijdens het verblijf actief kunnen informeren over wat er kan gebeuren met data, wat hiervan de voordelen zijn en welke waarborgen voorzien zijn. Zij zijn doorgaans ook de formele 'verwerkingsverantwoordelijke' die moeten kunnen verantwoorden wat er met de persoonsgegevens gebeurt.

De noodzaak van transparantie is ook een van de belangrijke aanbevelingen in het 'Big-data-rapport' dat in 2017 uitgebracht werd door de toenmalige *privacy* commissie.[25]

5.3.5. Noodzaak van 'passende waarborgen'

Zoals gezegd zijn de uitzonderingen in het kader van wetenschappelijk onderzoek onderworpen aan zogenaamde 'passende waarborgen'.

> *Art. 89.1 AVG bepaalt hierover: De verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met deze verordening voor de rechten en vrijheden van de betrokkene. Die waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.*

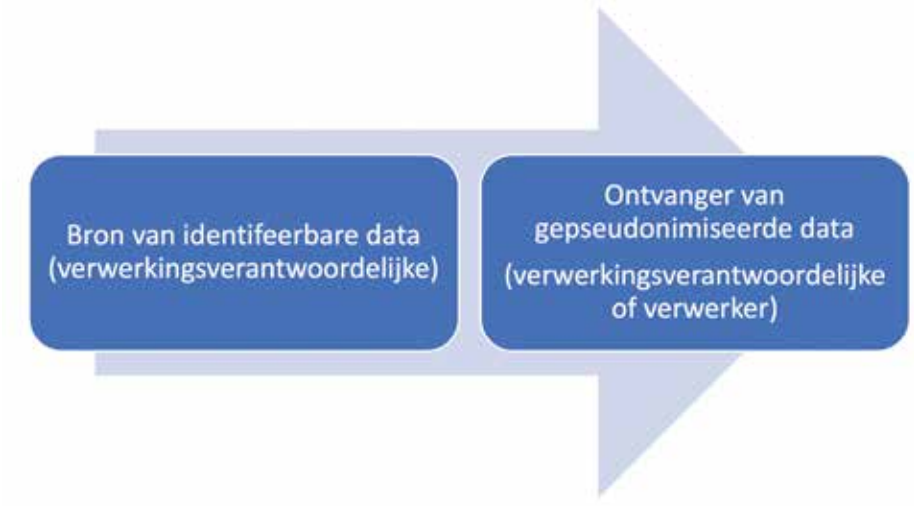
Die 'passende waarborgen' zijn niet precies beschreven in de AVG. Het gaat zowel om **organisatorische** (*governance*) als om **technische** maatregelen die vooral gericht zijn op het bewaken van het beginsel van minimale gegevensverwerking. Aangezien het voor het bereiken van het doel van het wetenschappelijk onderzoek slechts bij uitzondering noodzakelijk is om de identiteit van de betrokkene te kennen, strekken die maatregelen dus vooral op het maximaal vermijden van de identificatie van de patiënt. Dat kan gebeuren door anonimisering of pseudonimisering.

Deze processen worden soms ten onrechte als synoniemen gebruikt, maar zijn technisch sterk verschillend en hebben ook fundamenteel verschillende juridische gevolgen:

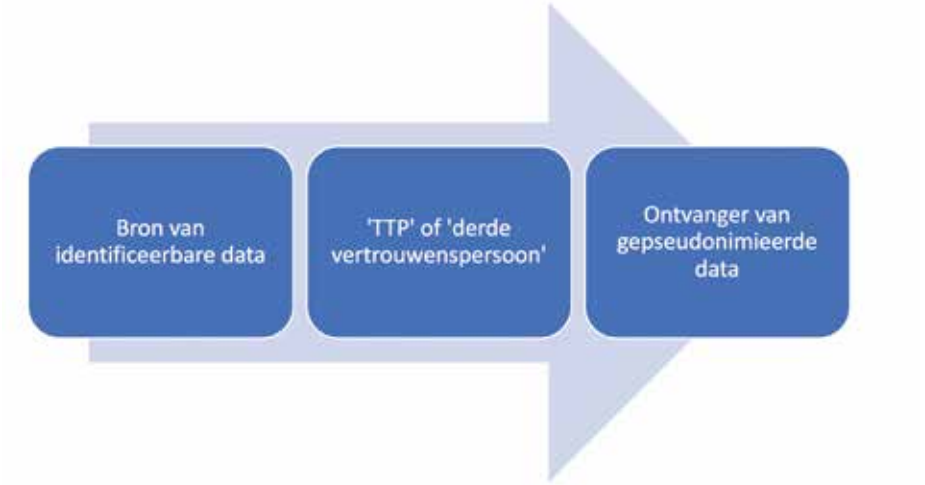
- Bij **anonimisering** worden alle identificerende gegevens definitief en onherroepelijk verwijderd op een wijze die nadien niet meer toelaat om tot re-identificatie te komen;
- Bij **pseudonimisering** worden de identificerende gegevens via een algoritme (of een sleutel) vervangen door een versleutelde en onherkenbare, maar wel unieke combinatie van letters en cijfers (het pseudoniem).[26] Re-identificatie is nog mogelijk, maar enkel door de houder van de sleutel.[27]

Het juridische verschil is belangrijk. Na anonimisering, waarbij heridentificatie met alle 'redelijkerwijze te verwachten' technieken onmogelijk is geworden, verliezen de gegevens het statuut van persoonsgegeven. Na het proces van anonimisering is de AVG dan ook niet meer van toepassing op die gegevens.[28] Gelet op de enorme vooruitgang van de ICT-technologie, de koppelingsmogelijkheden tussen databanken en het uniek identificerend karakter van DNA en van vele andere (fysieke) kenmerken, wordt meer en meer getwijfeld aan de mogelijkheid om tot daadwerkelijke anonimisering over te gaan.[29] Sommigen omschrijven anonimiteit zelfs als een mythe.[30]

Gepseudonimiseerde gegevens blijven persoonsgegevens en blijven dus onder het toepassingsgebied van de AVG.[31] Indien persoonsgegevens tussen verschillende verwerkingsverantwoordelijken of tussen een verwerkingsverantwoordelijke en een verwerker worden overgedragen, moet de pseudonimisering ***vóór* de overdracht** gebeuren. Anders zal de ontvanger zonder rechtmatige grondslag kennis kunnen nemen van identificeerbare data. Schematisch is dat als volgt:



Om de data-transfer veilig en optimaal te laten verlopen en om het proces van pseudonimisering te bewaken en te professionaliseren wordt vaak gebruik gemaakt van een zogenaamde **TTP** of ***Trusted Third Party***, in de Belgische kaderwet omschreven als 'derde vertrouwenspersoon'.[32] Schematisch ziet de plaats van de TTP in de gegevensstroom er als volgt uit, al kan de TTP ook een rol spelen in de omgekeerde richting (bijvoorbeeld als de onderzoeker gegevens wil opvragen bij de oorspronkelijke bron).



Belangrijk is ook dat de pseudonimisering tot gevolg moet hebben dat de *persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt* en dat die aanvullende gegevens *apart worden bewaard en technische en organisatorische maatregelen worden genomen om te waarborgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.*[33] Na pseudonimisering blijft het dus wel mogelijk om de gegevens te herleiden tot één persoon (de zogenaamde *singling out*), maar dat mag niet mogelijk zijn voor wie de 'aanvullende gegevens' (de sleutel) niet kent. Dat kan zeer moeilijk te waarborgen zijn bij zeldzame ziekten, bij zeer specifieke ziektebeelden of bij gegevens van beperkte populatiestalen die op andere wijze (bv. door de band met een regio of een tewerkstellingsplaats) tot herkenbaarheid kunnen leiden. Grote voorzichtigheid is dus gepast indien de herkenning op die wijze wel mogelijk is.

5.3.6. Mogelijke uitzonderingen op de rechten van betrokkenen

De AVG waarborgt in het belang van de betrokkene meerdere rechten, zoals het recht op inzage, gegevenswissing of rectificatie.

Het is mogelijk dat het **in het belang van het onderzoek** nodig is om af te wijken van bepaalde beginselen of een (eventueel tijdelijke) uitzondering te voorzien op de uitoefening van individuele rechten. Een klassiek voorbeeld is het dubbelblind, placebo gecontroleerd, gerandomiseerd geneesmiddelenonderzoek. Bij een dergelijk onderzoek wordt aan sommige proefpersonen een geneesmiddel toegediend, terwijl andere (door het toeval bepaalde) personen enkel een placebo krijgen. Noch de onderzoekers noch de proefpersonen mogen weten wie het werkzame middel krijgt en wie enkel het placebo ontvangt. Het recht van inzage zou het (wetenschappelijk noodzakelijk) 'blind' karakter van het onderzoek kunnen doorbreken. Het kan dus in het belang van het onderzoek minstens tijdelijk verantwoord zijn om geen volledige inzage toe te laten.

De AVG voorziet daarom de mogelijkheid om uitzonderingen te voorzien op sommige rechten van de betrokkene. Voor sommige rechten voorziet de AVG die uitzonderingen zelf. Zo is het recht op gegevenswissing niet van toepassing bij **wetenschappelijk onderzoek** indien de

gegevenswissing het onderzoek 'dreigt onmogelijk te maken of ernstig in het gedrang dreigt te brengen'.[34] Voor andere is 'lidstatelijk' recht nodig. De zogenaamde *research exemption* van art. 89. 2. voorziet de mogelijkheid dat een nationale wet afwijkingen op artikelen 15 (recht van inzage), 16 (recht van rectificatie), 18 (recht op beperking) en 21 (recht van bezwaar) toelaat.

In België werd deze *research exemption* uitgevoerd door de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, doorgaans omschreven als de 'Kaderwet Gegevensbescherming'. Deze kaderwet voorziet een aantal voorwaarden om te mogen afwijken van de rechten opgesomd in art. 89.2 AVG. Samengevat gaat het om:

- De noodzaak van een **overeenkomst** (*Data Transfer Agreement*) tussen de verwerkingsverantwoordelijke en de verdere verwerker. Dus meer concreet tussen de bron van de data en de onderzoeker (of het onderzoeksplatform);
- Het respecteren van het zogenaamde **cascadestelsel** en de noodzakelijke verantwoording in het verwerkingsregister voor de keuze tussen anonieme, gepseudonimiseerde of niet-gepseudonimiseerde gegevens;
- Voorschriften over het **moment** waarop de anonimisering of de pseudonimisering moeten gebeuren en de uitvoerder van die processen.

De overeenkomst

Bij verdere verwerking schrijft art. 194 Kaderwet Gegevensbescherming voor dat een overeenkomst moet afgesloten worden tussen de verwerkingsverantwoordelijke (voor het onderzoek) en de verantwoordelijke voor de oorspronkelijke verwerking. Concreet dus tussen de bron van de onderzoeksgegevens en het onderzoeksinstituut of in dit project het onderzoeksplatform.

De **inhoud** van de overeenkomst is omschreven in art. 195 Kaderwet Gegevensbescherming:

- De contactgegevens van beide partijen;
- De redenen waarom de uitoefening van de rechten van betrokkene de verwezenlijking van de doeleinden (van het onderzoek) 'onmogelijk dreigen te maken of ernstig dreigen te belemmeren'.

De afgesloten overeenkomsten moeten ook bij het verwerkingsregister worden gevoegd.

Het cascademodel

De kaderwet omschrijft in art. 197 het zogenaamd **cascademodel** en bevestigt op dat vlak de regeling vervat in het uitvoeringsbesluit van de 'oude' (Belgische) privacywet.[35]

- In beginsel gebruikt de verantwoordelijke voor de verwerking met het oog op onderzoek anonieme gegevens;
- Indien het onderzoeksdoel niet kan worden bereikt met anonieme gegevens, gebruikt de verwerkingsverantwoordelijke gepseudonimiseerde gegevens;
- Indien het onderzoeksdoel niet kan worden bereikt met gepseudonimiseerde gegevens, gebruikt de verwerkingsverantwoordelijke niet-gepseudonimiseerde gegevens.

De **verantwoording** voor de keuze dient te worden opgenomen in het register voor de verwerkingsactiviteiten (art. 191, 1° Kaderwet Gegevensbescherming). Een afzonderlijk advies van de functionaris voor gegevensbescherming (DPO) is hierbij niet nodig. De DPO dient wel advies uit te brengen over de verschillende methodes van pseudonimisering en anonimisering.[36] Ook bij de-pseudonimisering is het advies van de DPO vereist.[37]

Persoon en moment

De artikelen 198 tot en met 204 van de Kaderwet Gegevensbescherming behandelen de anonimisering en pseudonimisering van gegevens voor onderzoeksdoeleinden. Zij zijn vooral relevant voor de vraag wie en op welk moment moet instaan voor anonimisering of pseudonimisering.

5.3.7. Uitzonderingen enkel voor wetenschappelijk onderzoek (met publiek belang)

Het is zeer belangrijk dat de uitzonderingsregeling **enkel** wordt toegepast voor **daadwerkelijk wetenschappelijk onderzoek**. Het concept wetenschappelijk onderzoek is niet gedefinieerd in de AVG. Overweging 159 bij de AVG stelt: *Voor de toepassing van deze verordening moet de verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek ruim worden opgevat en bijvoorbeeld technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek omvatten.* Dezelfde overweging maakt ook duidelijk dat voorzichtigheid gepast is bij publiceren van onderzoeksresultaten en bij het nemen van maatregelen op basis van het onderzoek.[38]

De Article 29 Working Party (thans vervangen door de European Data Protection Board) wees in een advies van 2017 (gereviseerd in 2018) nog op het belang van overeenstemming van het onderzoek met de relevante methodologische en ethische normen van de sector.[39]

Essentieel: publiek belang

Het is duidelijk dat niet de hoedanigheid van de opdrachtgever of de gebruiker essentieel zijn, maar het **doel** en het **publiek belang** van het onderzoek. Zeker indien men zich ook beroept op het algemeen belang als rechtmatigheidsgrond. Het moet niet noodzakelijk enkel gaan over klassiek medisch of farmacologisch onderzoek. Alle vormen van onderzoek die bijdragen tot de verbetering van de werking van het stelsel van gezondheidszorg zijn ook van publiek belang. Een belangrijk en niet beslecht discussiepunt is of research door farmaceutische bedrijven kan worden beschouwd als wetenschappelijk onderzoek in de zin van de uitzonderingsregeling van de AVG. Grote voorzichtigheid zal in elk geval gepast zijn om het publiek vertrouwen niet te aan te tasten door gebruik van onderzoeksgegevens voor commerciële motieven.

Juridische en ethische toetsingscommissie

In essentie zijn het de verwerkingsverantwoordelijken die moeten beslissen wanneer en onder welke voorwaarden de door hen beheerde gegevens mogen worden gebruikt voor wetenschappelijk onderzoek. Zij moeten dus uitmaken of de uitzonderingen ter bevordering van wetenschappelijk onderzoek kunnen worden toegepast. Niettemin kan het voor een georganiseerde samenwerking tussen een groot aantal databronnen, het beoogde onderzoeksplatform en een groot aantal gebruikers, sterk aangewezen zijn dat een **orgaan** wordt opgericht dat op onafhankelijke en deskundige wijze oordeelt of de gegevens inderdaad opgevraagd worden voor onderzoek in het publiek belang. Binnen het onderzoeksplatform wordt dus best een commissie opgericht die de aanvragen juridisch en ethisch toetst en bevestigt dat het gaat om onderzoek met publiek belang. Die commissie kan eventueel ook de beleidslijnen voor de controle van het proces vastleggen en toezien op de uitvoering van deze controle. De praktijk van de Data Acces Committees (DAC's) voor de regeling van toegang tot databases met genetische gegevens kan daarbij zeer inspirerend zijn.[40.]

Publiek vertrouwen

Dergelijke vormen van toetsing en controle kunnen ook zeer belangrijk zijn voor het **publiek vertrouwen**. Een zeer recent (in 2019) in *Health Policy* gepubliceerd artikel maakt een meta-analyse van een reeks studies over de aanvaarding van *re-use of health data* bij patiënten en

de brede bevolking. Uit de conclusie blijkt dat men doorgaans zeer positief en aanvaardend staat tegenover hergebruik van gezondheidsgegevens op voorwaarde dat er voldoende waarborgen zijn voor gebruik in het algemeen belang. De conclusie van de *attitude review* luidt als volgt:

> *Health data are used for still more purposes and policies are enacted to facilitate data reuse within the European Union. This literature synthesis explores attitudes among people living in the European Union towards the use of health data for purposes other than treatment. Our findings indicate that while a majority hold positive attitudes towards the use of health data for multiple purposes, the positive attitudes are typically conditional on the expectation that data will be used to further the common good. Concerns evolve around the commercialization of data, data security and the use of data against the interests of people providing the data. Studies of these issues are limited geographically as well as in scope. We therefore identify a need for cross-national exploration of attitudes among people living in the European Union to inform future policies in health data governance.*[41]

5.4. Voorwaarden voor de zorgactoren

5.4.1. Wie is er in welke zin betrokken?

Om na te gaan in hoeverre de voorgenomen overdracht van patiëntengegevens voor onderzoeksdoeleinden geoorloofd kan zijn, zal het in de eerste plaats nodig zijn dat een analyse wordt gemaakt van de verhoudingen tussen de verschillende actoren. Voor de toepassing van de AVG zal het daarbij erg belangrijk zijn wie wordt beschouwd als betrokkene, verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke en eventueel als verwerker.

Het is vrij evident dat de patiënt (en mogelijk ook diens familielieden) de betrokkene is in de zin van de AVG.

De gezondheidszorginstellingen en de onafhankelijke zorgverstrekkers zijn verwerkingsverantwoordelijken. Binnen de gezondheidszorginstellingen is de omschrijving van de hoedanigheid van de betrokken zorgenverstrekkers doorgaans vrij complex. Verpleegkundigen en zorgkundigen worden doorgaans als 'bewerkers' beschouwd. 'Bewerkers' zijn personen die onder het rechtstreeks gezag van de verwerkingsverantwoordelijke gemachtigd zijn om persoonsgegevens te verwerken.[42] Artsen zijn in sommige ziekenhuizen 'gezamenlijk verwerkingsverantwoordelijken'. In de mate dat artsen voor de door hen beheerde gegevens als verwerkingsverantwoordelijke worden beschouwd, zullen zij ook een overeenkomst moeten sluiten met het onderzoeksplatform. Het zal minstens nodig zijn dat het ziekenhuis over de door haar voorgenomen overeenkomst met het onderzoeksplatform advies vraagt aan de medische raad. Het gaat immers over een overeenkomst met een derde die een weerslag kan hebben op de medische activiteit.[43]

Het onderzoeksplatform zal ten opzichte van de databronnen geen verwerker, maar een autonome verwerkingsverantwoordelijke zijn. Het onderzoeksplatform werkt immers niet in opdracht en 'ten behoeve van' de databronnen.

Ook de onderzoekers zijn als 'gebruikers' van de gegevens in de relatie met het onderzoeksplatform geen verwerkers, maar autonome verwerkingsverantwoordelijken.

In de relatie tussen het onderzoeksplatform en de databronnen en de datagebruikers zal het – zoals hierna onder nr. 5.4.7. nader wordt toegelicht - aangewezen zijn dat overeenkomsten worden opgesteld. Indien zij als gezamenlijk verwerkingsverantwoordelijken zouden worden beschouwd, is dat zelfs voorgeschreven door art. 26 AVG. Indien gebruik wordt gemaakt van de uitzonderingsregeling voorzien in de Kaderwet, is een dergelijke overeenkomst ook verplicht.

Binnen een ziekenhuis zal ook advies moeten gegeven worden door de hoofdarts als algemeen verantwoordelijke voor het medisch dossier en door de DPO. Het kan ook aangewezen zijn om de overeenkomsten of minstens het algemeen beleid voor advies voor te leggen aan het ethisch comité.

5.4.2. Is er sprake van overdracht of niet?

Er is geen overdracht

Zoals toegelicht onder 1, is het denkbaar dat de bronnen van de data (de zorgverstrekkers en gezondheidszorginstellingen) géén data overdragen, ook niet in geanonimiseerde of gepseudonimiseerde vorm, maar enkel toelaten dat bijzondere big-data-analysetechnieken worden verricht **binnen** hun eigen bestanden en systemen, waarna **enkel de algemene conclusies van die analyses** worden overgedragen. Op die manier gebeurt geen overdracht van persoonsgegevens en zal mogelijk in belangrijke mate buiten het dwingend kader van de AVG kunnen worden gewerkt. De verwerkingsverantwoordelijke zal enkel moeten kunnen verantwoorden dat deze analyse wordt uitgevoerd op de data. Dat kan mogelijk onverenigbaar zijn met het doel waarvoor zij initieel werden ingezameld, maar in het belang van het wetenschappelijk onderzoek kan die uitzondering op het beginsel van doelbinding worden verantwoord.[44]

Er is wel overdracht

Indien er wel gegevens worden overgedragen is het een essentieel verschil of de gezondheidsgegevens op geanonimiseerde, gepseudonimiseerde of herkenbare wijze worden overgedragen van de oorspronkelijke verwerkingsverantwoordelijke (de zorgbeoefenaar of de gezondheidszorginstelling) naar het onderzoeksplatform.

- Indien zij geanonimiseerd worden, verliezen zij vanaf het moment van de anonimisering het statuut van persoonsgegeven.
- Indien zij gepseudonimiseerd worden, moet de pseudonimisering gebeuren voorafgaand aan de overdracht. Een TTP of 'derde vertrouwenspersoon' kan instaan voor een betrouwbaar proces van pseudonimisering.

5.4.3. Werken zonder uitdrukkelijke toestemming

Zoals hierboven onder nr. 3.3 toegelicht, kan het hergebruik van gezondheidsgegevens in het belang van wetenschappelijk onderzoek verantwoord worden zonder bijzondere toestemming van de betrokkene. Dat kan enkel indien de 'passende waarborgen' aanwezig zijn en het nodige ondernomen is om de gegevens veilig over te dragen en de identificatie van de patiënt te vermijden door anonimisering of pseudonimisering. Het is absoluut nodig dat de patiënt hierover wordt geïnformeerd.

5.4.4. Noodzaak van degelijke informatie

Het is nodig dat er zowel op het niveau van de verwerkingsverantwoordelijken (de gezondheidszorginstellingen of de gezondheidszorgbeoefenaars) als breder, naar het algemeen publiek of naar bepaalde patiëntengroepen **volledige informatie** wordt gegeven over de verwerking en het hergebruik van de gezondheidsgegevens voor wetenschappelijk onderzoek. Die informatie dient betrekking te hebben op alle aspecten van het hergebruik (doel, beveiliging, aan wie wordt overgedragen, hoe dit gecontroleerd wordt…). Deze informatie moet transparant, duidelijk, begrijpbaar en gemakkelijk toegankelijk zijn. Schriftelijke communicatie mag zeker worden ondersteund met filmpjes of audiofragmenten.

Voor het publiek vertrouwen is het ook aangewezen dat de *governance*- en controlestructuren van het onderzoeksplatform worden toegelicht en dat ook wordt getoond welk soort resultaten kan worden bereikt met de onderzoeken die mogelijk worden gemaakt via het

onderzoeksplatform. Indien dit gericht mogelijk is, wordt ook de bekendmaking en toelichting van onderzoeksresultaten sterk geapprecieerd. Inspiratie kan eventueel gevonden worden in projecten zoals *My health, my data* waarbij blockchain-technologie wordt gebruikt om toegang tot onderzoeksgegevens te bevorderen.[45]

5.4.5. Noodzaak van betrouwbare beveiliging en 'passende waarborgen'

Hergebruik van gezondheidsgegevens voor onderzoek is enkel geoorloofd mits 'passende waarborgen'. Dat impliceert dat alle technische en organisatorische maatregelen moeten worden genomen om de identificatie van de patiënt vermijden. Het veronderstelt dat performante, betrouwbare en regelmatig bijgestuurde technieken voor de data-security worden ingezet, en dat gebruik wordt gemaakt van anonimisering of pseudonimisering, voorafgaand aan de overdracht van de gegevens. Het gebruik van een TTP of 'derde vertrouwenspersoon' is niet altijd verplicht, maar kan in het belang van het publiek vertrouwen aangewezen zijn.

5.4.6. Mogelijke toepassing van kaderwet

Indien het voor het onderzoek nodig is om een uitzondering te maken op de artikelen 15 AVG (recht van inzage), 16 (recht van rectificatie), 18 (recht op beperking) of 21 (recht van bezwaar), dan moet ook toepassing gemaakt worden van de Kaderwet. Zoals toegelicht onder 3.6. houdt dit o.m. in dat:

- Een overeenkomst (een *Data Transfer Agreement*) moet worden opgesteld tussen de verantwoordelijke voor de oorspronkelijke verwerking en de verantwoordelijke voor de verdere verwerking;
- Dat de keuze tussen geanonimiseerde, gepseudonimiseerde of herkenbare gegevens moet worden verantwoord in het verwerkingsregister;
- Dat een aantal voorschriften over de pseudonimisering moeten worden gevolgd.

5.4.7. Contractuele afspraken en overeenkomsten

Indien toepassing gemaakt wordt van de uitzonderingsregeling voorzien in de Kaderwet moet een overeenkomst (een *Data Transfer Agreement*) worden opgesteld tussen de verantwoordelijke voor de oorspronkelijke verwerking en de verantwoordelijke voor de verdere verwerking. Maar ook los daarvan is het sterk aangewezen dat de relaties tussen de data-bronnen en het onderzoeksplatform contractueel worden geregeld en dat voor de overdracht van de gegevens en alle waarborgen een *Data Transfer Agreement* wordt opgesteld.

5.5. Aan welke voorwaarden moet het onderzoeksplatform zelf voldoen?

Het is op dit moment niet duidelijk onder welk juridisch statuut het onderzoeksplatform zal worden opgericht. Het zou een nieuwe instelling met afzonderlijke rechtspersoonlijkheid kunnen worden. Het zou ook een nieuwe taak kunnen worden voor een bestaande instelling.

Voor de toepassing van de AVG is het vooral belangrijk om te weten of het onderzoeksplatform daadwerkelijk persoonsgegevens en meer in het bijzonder gezondheidsgegevens zal verwerken. Het is daarbij belangrijk om te beklemtonen dat gepseudonimiseerde gegevens hun statuut van persoonsgegeven behouden, en dat gepseudonimiseerde gegevens over de gezondheid gevoelige gegevens in de zin van art. 9 AVG blijven. Dat betekent dat het onderzoeksplatform aan alle voorwaarden voor de verwerking van gezondheidsgegevens zal moeten voldoen, en dat alle medewerkers gebonden zijn door het beroepsgeheim of een gelijkwaardige contractuele regeling.

Het is aangewezen dat de relaties met de data-bronnen en met de onderzoekers worden vastgelegd in controleerbare overeenkomsten waarbij zowel het doel, de modaliteiten, de veiligheidsmaatregelen als de controlemechanismen zijn vastgelegd.

Ook de *governance* van het onderzoeksplatform is erg belangrijk. Zoals toegelicht onder § 5.3.7. is het aangewezen dat binnen het onderzoeksplatform een (ethische) commissie wordt opgericht die de aanvragen juridisch en ethisch toetst en bevestigt dat het gaat om onderzoek met publiek belang. Die commissie kan eventueel ook de beleidslijnen voor de controle van het proces vastleggen en toezien op de uitvoering van die controle.

De concrete modaliteiten van de controle moeten ook worden uitgewerkt en contractueel vastgelegd in de overeenkomst met de bronnen en de gebruikers. De ethische commissie van het onderzoeksplatform kan ook in relatie staan met de ethische commissies van de ziekenhuizen die over de algemene beleidslijnen van het hergebruik van de patiëntendata best om advies worden gevraagd.

5.6. Welke zijn de voorwaarden voor gebruik van data beheerd door het onderzoeksplatform?

Als aan alle voorgaande voorwaarden voldaan is, zal het onderzoeksplatform geanonimiseerde of gepseudonimiseerde data ter beschikking kunnen stellen van onderzoekers die daarom vragen. Per project en per onderzoek zal moeten worden verantwoord welke gegevens men nodig heeft, wat het doel van het onderzoek is, waarom het van publiek belang is, welke methodologie zal worden gevolgd en hoe de resultaten zullen worden gerapporteerd. Het is aangewezen dat dit getoetst wordt door een onafhankelijk orgaan binnen het onderzoeksplatform.

Het is aangewezen dat tussen het onderzoeksplatform en de gebruikers een overeenkomst wordt afgesloten waarin het doel, de modaliteiten, de veiligheidsmaatregelen en de controlemechanismen zijn vastgelegd. Een dergelijke overeenkomst moet ook kunnen worden opgevraagd en gecontroleerd door de patiëntenvertegenwoordigers in de *governance* structuren.

5.7. Samengevat

Wij vatten hierna kort de bevindingen van onze juridische analyse samen. Voor de verantwoording en de argumentatie wordt naar de tekst hierboven verwezen, zonder die te hernemen.

AVG

De Algemene Verordening Gegevensbescherming en de toepasselijke wetgeving laten toe om dit project nader uit te werken.

Zonder gegevensoverdracht

Indien het mogelijk is om te vermijden dat er enige overdracht van persoonsgegevens moet gebeuren tussen de bronnen van de data (de gezondheidszorginstellingen en zorgbeoefenaars), het onderzoeksplatform en de onderzoekers, kan dit het proces juridisch veel eenvoudiger maken. Indien de bronnen van de data enkel moeten toestaan dat er op hun bestanden en **binnen hun systemen** big-data-analysetechnieken worden toegepast en dat enkel de algemene conclusies worden meegedeeld, dan worden er geen persoonsgegevens overgedragen. Op de overdracht van de algemene conclusies zal de AVG dan ook niet van toepassing zijn. Het zal enkel nodig zijn om uit te maken of de verwerkingsverantwoordelijke een analyse op de door hem beheerde gegevens zal mogen uitvoeren of laten uitvoeren. Indien die analyses gebeuren in het belang van wetenschappelijk onderzoek vallen zij onder de uitzondering op het beginsel van doelbinding.

Met overdracht van gegevens

Indien er wel data moeten worden overgedragen, moeten alle nodige organisatorische en technische maatregelen worden genomen om de gegevens maximaal te beveiligen en de identificatie van de patiënten te vermijden. Dat kan door anonimisering of pseudonimisering.

- Bij anonimisering verliezen de gegevens hun statuut van persoonsgegeven.
- Gepseudonimiseerde gegevens blijven persoonsgegevens. De pseudonimisering moet gebeuren voorafgaand aan de data-transfer, en op degelijke en betrouwbare wijze. Best via de interventie van een TTP of 'derde vertrouwenspersoon'.

Passende waarborgen

Indien de data gebruikt worden om onderzoek uit te voeren in het algemeen belang en alle 'passende waarborgen' voor veilig en onherkenbaar hergebruik aanwezig zijn, is het hergebruik mogelijk zonder bijzondere toestemming van de betrokken patiënt. Indien men zich niet kan beroepen op de bijzondere uitzondering van het algemeen belang, blijft het recht van bezwaar bestaan zodat een 'opt-out-stelsel' kan worden ontwikkeld.

Informatie en communicatie

Het is wel nodig dat volwaardige informatie gegeven wordt over alle aspecten van het hergebruik (doel, beveiliging, aan wie wordt overgedragen, beoordeling, rapportering en controle). Die informatie moet worden gegeven door de gezondheidszorginstellingen die als data-bron aan het project meewerken. Ze wordt ook best ondersteund door bredere campagnes naar het algemeen publiek en specifieke patiëntengroepen.

Toetsingsorgaan

Het is noodzakelijk om een orgaan op te richten dat waakt over het verantwoord gebruik van de data en dat kan bevestigen dat de vragen tot gebruik van data wel vallen onder de uitzonderingen voorzien voor onderzoek in publiek belang. Het is aangewezen dat binnen het onderzoeksplatform een (ethische) commissie wordt opgericht die de aanvragen juridisch en ethisch toetst. Die commissie kan eventueel ook de beleidslijnen voor de controle op het proces vastleggen en toezien op de uitvoering van deze controle.

Contractuele overeenkomsten

De relaties tussen de data-bronnen en het onderzoeksplatform, en het onderzoeksplatform en de onderzoekers, worden best vastgelegd in een overeenkomst waarin alle aspecten van de data-overdracht (doel, beveiliging, de-identificatie, rapportering) en de controle duidelijk geregeld zijn.

Hoofdstuk 6
Hoe kan het allemaal veilig gebeuren?

In het vorige hoofdstuk lichtten we de juridische criteria toe met het oog op een rechtsgeldige en rechtszekere werking van het beoogde platform. Op verschillende plaatsen wordt hierbij verwezen naar technische en organisatorische maatregelen om die doelstelling te bereiken. Dit hoofdstuk bespreekt deze technische en organisatorische maatregelen en vormt de basis voor een verdere concrete uitwerking van het onderzoeksplatform op een informatieveilige manier.

6.1. Informatieveiligheid als criterium voor het onderzoeksplatform

6.1.1. Confidentialiteit, integriteit, beschikbaarheid en verantwoording

Informatieveiligheid verwijst naar maatregelen met het oog op confidentialiteit, integriteit en beschikbaarheid. Naar die triade wordt ook vaak verwezen met de afkorting 'CIA', afkomstig van de Engelse vertaling van deze begrippen (*Confidentiality, Integrity, Availability*). Het principe van verantwoording is een vierde criterium. Dat principe heeft aan belang gewonnen sinds de komst van GDPR, die het expliciet benoemt en daardoor een wettelijke grond geeft.

Concreet betekenen de vier principes het volgende:

1. **Confidentialiteit:** het onderzoeksplatform wordt enkel gehanteerd door een geautoriseerde gebruiker (een individu, organisatie of een systeem), waarbij diens handelen in lijn ligt met vooraf bepaalde regels.
2. **Integriteit**: alle informatie op het platform is actueel en correct.
3. **Beschikbaarheid:** betreft het niveau van dienstverlening.
4. **Verantwoording** verwijst naar de vraag: wie deed wat, wanneer en waarom?

6.2.2. Ondersteunende, niet-functionele criteria

Zoals aangegeven zal de studie van informatieveiligheid resulteren in een set van maatregelen die, wanneer ze correct worden uitgevoerd, zorgen voor een rechtsgeldige en rechtszekere werking van het platform. Ze bepalen met andere woorden *niet* de functionaliteit van het platform, maar **ondersteunen** ze. We kunnen stellen dat informatieveiligheid zogenaamde 'niet-functionele criteria' vastleggen die de 'functionele criteria' ondersteunen.

De 'functionele criteria' die door informatieveiligheid worden ondersteund betreffen bv. de juridische (hoofdstuk 5) en de ethische criteria (hoofdstuk 7). Er is dus met andere woorden een belangrijk onderscheid tussen functionele (wat moet het platform allemaal kunnen?) en niet-functionele criteria hoe kan dat worden gegarandeerd?). Informatieveiligheid behandelt vooral die laatste criteria.

6.2. Hoe pakken we het organisatorisch aan?

6.2.1. Interne organisatiecomponent

Informatieveiligheid als continu proces (Security by Design)

In dit conceptvoorstel bespreken we vooral de functionele criteria (wat moet het onderzoeksplatform allemaal kunnen? Conceptueel, technisch, juridisch, ethisch). Die criteria zullen nog verder evolueren, zowel in de aanloop naar een eventuele uitrol van het platform, als daarna.

Informatieveiligheid als het **ondersteunend proces** hiervoor, moet die evolutie volgen. Dat maakt van informatieveiligheid een continu proces dat van bij de start van het project moet worden bekeken (*Security by Design*). De evolutie in functionele criteria betekent dat dit niet-functionele aspect van informatieveiligheid ook wordt opgenomen in de *governance* structuur van het onderzoeksplatform.

Noodzakelijke ondersteuning

In principe bepalen 'niet-functionele criteria' zoals informatieveiligheid niet de functies van het platform, maar ondersteunen ze. Door de snelle evolutie van technologie stellen we soms vast dat een functioneel criterium wenselijk en uitvoerbaar is, maar dat de noodzakelijke ondersteuning ervoor – waaronder informatieveiligheid – niet bestaat, onvoldoende of ontoereikend is (wegens te duur of te complex). In die gevallen is informatieveiligheid een rem op de ontwikkeling van het beoogde platform. Het is daarom belangrijk dat informatieveiligheid niet alleen deel uitmaakt van de *governance* van het project, maar ook voortdurend deel uitmaakt van de visie en strategie ervan.

Risicoavers onderzoeksplatform

Concreet moet in de missie en visie worden bepaald in welke mate het platform risicoavers is, dan wel risicozoekend, en hoe dat in verhouding staat met de wil en mogelijkheid om te investeren in informatieveiligheid. Die intentie moet ook kenbaar worden gemaakt aan alle actoren (bv. in de opdrachtsverklaring).

We nemen aan dat het beoogde platform veeleer **risicoavers** is en dat bijgevolg elk initiatief tot innovatie wordt afgewogen, rekening houdend met de noodzakelijke en haalbare **kost** voor **informatieveiligheid**.

Informatieveiligheid als kwaliteitskenmerk (Deming Circle)

Informatieveiligheid stopt trouwens niet bij de ontwerpfase. Eenmaal het platform operationeel is, moeten de genomen maatregelen worden gemonitord en waar nodig bijgestuurd. Informatieveiligheid is daarom ook een kwaliteitskenmerk dat moet worden beheerd volgens het **plan-do-check-act** principe (ook wel de kwaliteitscirkel van Deming genoemd).

In dit domein is het de gewoonte om het kwaliteitsproces te monitoren door een (operationeel) onafhankelijk individu. Conform de GDPR wetgeving kan die taak worden toevertrouwd aan een **Data Protection Officer** (functionaris voor de gegevensbescherming).

Op basis van voorgaande besluiten we dat de interne organisatie van informatieveiligheid best wordt opgezet volgens de ISO 27001 **standaard**. Die standaard beschrijft op welke manier een beheerssysteem voor informatieveiligheid moet worden ingericht (in het Engels spreken we over een *Information Security Management System* of ISMS).

De standaard, die bovendien **certificeerbaar** is (de nood van certificatie wordt verder besproken), omvat alle hierboven beschreven criteria, met name de *governance*, de binding met missie en visie, en het beheer van informatieveiligheid volgens de *Deming circle*.

6.2.2. Externe, maatschappelijk getoetste organisatiecomponent

Het beheer van informatieveiligheid is niet alleen een interne aangelegenheid. Het niveau van informatieveiligheid van een platform dat voornamelijk het maatschappelijk belang dient, heeft ook een **externe, maatschappelijk getoetste** component. Binnen die component wordt het niveau van informatieveiligheid bepaald door politieke, wetgevende en normatieve criteria.

Politiek

Wat kan de impact van politiek zijn op de organisatie van informatieveiligheid? De politieke dimensie is in de eerste plaats die waarbij **verantwoording** kan worden afgelegd over **het nagestreefde veiligheidsniveau**. Het betekent concreet dat het niveau van informatieveiligheid moet kunnen worden **gemeten**. Met andere woorden, informatieveiligheid moet voldoende **matuur** zijn om over de performantie verantwoording af te leggen. In het domein van informatieveiligheid betekent dat een **maturiteitsniveau 4**, dus **'beheerd'** (1 staat voor 'initieel ad hoc', 2 voor 'herhaalbaar', 3 voor 'gedefinieerd', 4 voor 'beheerd' en 5 voor 'geoptimaliseerd').[46]

Wetgevend
Naast politiek kan ook de wetgeving een impact hebben op de organisatie van informatieveiligheid. Zo kan wetgeving verplichten om externe actoren te betrekken in de organisatie van informatieveiligheid of om een bepaald niveau van informatieveiligheid na te streven.

In die context menen we dat de **eHealth-wet**[47] en de (Belgische vertaling van de) **NIS richtlijn**[48] (we verwijzen in wat volgt naar 'NIS') een impact hebben op de organisatie van informatieveiligheid en het na te streven veiligheidsniveau. Afhankelijk van de implementatie van het platform moet die lijst van wetgeving nog worden aangepast en/of aangevuld (zie ook hoofdstuk 5).

Wanneer diensten van het **eHealth-platform** worden gebruikt (bv. als *Trusted Third Party* voor pseudonimisering) zal volgens de eHealth-wet het beheerscomité van het eHealth-platform, inclusief zijn werkgroepen, een belangrijke bijdrage leveren aan het na te streven veiligheidsniveau.

Daarnaast zal moeten worden bepaald in welke mate de **NIS-regelgeving** van toepassing is voor het beoogde platform. Op het moment van schrijven is niet duidelijk wie wel en niet wordt aangeduid als zo'n dienst, noch zijn de criteria hiervoor bekend. Die criteria worden bepaald door sectorale overheden. Het is wenselijk dat de oprichting van het platform hierover wordt afgestemd. Hoewel het onderzoeksplatform zelf geen kritische maatschappelijke functie uitvoert of ondersteunt en dus meer dan waarschijnlijk niet onder het toepassingsgebied van NIS valt, koppelt het wel met organisaties die onder het toepassingsgebied van de NIS richtlijn vallen (bv. ziekenhuizen als data-bronnen of het eHealth-platform.

In elk geval dient men bij de organisatie van informatieveiligheid en meer in het bijzonder bij het uitwerken van een cyber security strategie het **Centrum voor Cyber Security** te betrekken. Dt orgaan, dat opgericht is krachtens het Koninklijk Besluit tot oprichting van het Centrum voor Cybersecurity België (KB van 10 oktober 2014) heeft (onder meer) als opdracht het opsporen, observeren en analyseren van online veiligheidsproblemen. Interne procedures voor het opsporen en afhandelen van incidenten waarbij het onderzoeksplatform betrokken is, dienen te worden opgesteld in nauw overleg met de dienst **Computer Emergency Response Team (CSIRT)** van het Centrum voor Cybersecurity.

Tot slot, ook op **Europees niveau** (**Cyber Security Act**) bestaat er regelgeving die de organisatie van informatieveiligheid van het onderzoeksplatform kan beïnvloeden. We denken hierbij voornamelijk aan de Cyber Security Certificatie. Dat is momenteel nog toekomstmuziek.

Normatief
De normatieve component ten slotte wordt bepaald door criteria die voor de markt wenselijk zijn of zelfs verplicht worden opgelegd. De markt in deze is de **leverancier** (patiënt en zorgorganisatie), de **sectorgenoot** (andere soortgelijke platformen) en de **consument** (de onderzoeksinstelling of overheid).

We denken in deze context ook aan **externe actoren**, zoals verzekeringsmaatschappijen (bv. in het geval men beslist om voor dit onderzoeksplatform een Cyber Security Polis af te sluiten). In dat geval moeten procedures binnen het informatieveiligheidsbeleid worden afgestemd op de samenwerking met de verzekeringsmaatschappijen.

Het is aangewezen om **afspraken** te maken met die actoren over de organisatie van informatieveiligheid, meer in het bijzonder de afspraken **over de na te leven normen**, zoals bv. de cirkels van vertrouwen die in de schoot van het eHealth-platform worden opgesteld, gedragscodes voor soortgelijke platformen zoals bepaald in GDPR regelgeving, certificaties en merktekens.

Voor de verdere uitrol van het onderzoeksplatform is het aanbevolen om actief met alle partners af te stemmen over normatieve criteria. Dit kan praktisch worden uitgewerkt in de *governance* van de overkoepelende projectstructuur door bv. een overlegplatform te voorzien met alle actoren.

6.3. Welke zijn de noodzakelijke technische maatregelen?

De organisatorische dimensie van informatieveiligheid beklemtoont de manier waarop informatieveiligheid de ondersteuning voor 'functionele criteria' garandeert. De technische dimensie zoomt in op de **effectieve technische maatregelen** die moeten worden genomen om het platform mogelijk te maken op een veilige manier. De technische maatregelen voor informatieveiligheid kan je op verschillende manieren catalogeren. Voor deze bespreking gebruiken we twee dimensies, met name de dimensie **'aard'** (soorten van technische maatregelen) en de dimensie **'toepassingsgebied'** (op wie de technische maatregelen van toepassing zijn).

6.3.1. Volgens aard

De **aard** van deze maatregelen voor informatieveiligheid is drievoudig: (1) maatregelen gerelateerd aan wetten en normen, (2) maatregelen die noodzakelijk zijn om het risico af te dekken, en (3) maatregelen die te maken hebben met de rechten van de betrokkene(n).

Wetten en normen

Vooreerst zijn er de maatregelen die te maken hebben met van toepassing zijnde wetten en normen (zie ook §6.6.2.). Normen kunnen van toepassing zijn omdat de organisatoren en stakeholders (waaronder ook patiënten en onderzoekers of onderzoeksinstellingen) hiernaar vragen. Die normen kunnen met name zorgen voor een vorm van vertrouwen in de technologie. De normen kunnen ook door wetten en regels worden opgelegd (zo wordt ISO 27001 voor informatieveiligheid opgelegd door de eerder vermelde NIS regelgeving).

Risico afdekken

Ten tweede zijn er de technische maatregelen die noodzakelijk zijn om de risico's af te dekken die impact kunnen hebben op de veiligheid van het platform. Die maatregelen zijn in de meeste gevallen een deelverzameling van de maatregelen die door wetten worden opgelegd. We benoemen ze apart omdat ze niet (alleen) het resultaat zijn van een norm, maar veeleer van een specifieke, op het platform toegepaste risicoanalyse.

Rechten van de betrokkene(n)

Ten derde zijn er maatregelen die te maken hebben met de rechten van de betrokkene(n), zoals besproken in hoofdstuk 5. Die maatregelen hebben de eigenschap dat ze, in tegenstelling tot de op risico gebaseerde maatregelen, resultaatsgebonden zijn. Het is evident dat de rechten die patiënten hebben, zoals bv. het recht op inzage of het recht om vergeten te worden, ook effectief kunnen worden uitgevoerd. De technische maatregelen die genomen worden, dienen hieraan te voldoen.

6.3.2. Volgens toepassingsgebied

Niet alle technische maatregelen zijn van toepassing op alle actoren. Daarom is het zinvol om naast de onderverdeling 'aard' van maatregelen ook aan te geven **voor wie** de maatregelen van toepassing zijn. We volgen hierbij de onderverdeling die al in de bespreking van de juridische randvoorwaarden werd gegeven, met name:

- Informatieveiligheid voor de 'databronnen' die samenwerken met het onderzoeksplatform en hiermee gegevens uitwisselen (kolom 1 van de matrix).
- Informatieveiligheid van het onderzoeksplatform zelf, inclusief de *Trusted Third Party* (TTP) (kolom 2 van de matrix).
- Informatieveiligheid toe te passen bij het gebruik van de gegevens van het onderzoeksplatform, meer in het bijzonder door de onderzoekers (kolom 3 van de matrix).

6.3.3. Samenvattende matrix van technische maatregelen

Rekening houdende met de dimensies 'aard' en 'toepassingsgebied' komen we tot onderstaande matrix van technische maatregelen voor informatieveiligheid voor het conceptvoorstel. In de daaropvolgende alinea's lichten we dit verder toe.

Aard/Toepassingsgebied	Databronnen	Platform en TTP	Onderzoek
Wetten en normen	Circle of Trust, eHealth wetgeving en Kaderwet AVG (regels pseudonimisering, anoniem verwerken).	ISO 27001, eIDAS, Certificatie volgens GDPR en NIS, logging. Aanstelling van een DPO.	Kaderwet AVG (regels rond pseudonimisering en anoniem verwerken).
Risk-based maatregelen	Toetsing bij het Informatieveiligheids- comité, identificatie en veilige communicatie.	Gegevensbescherming bij ontwerp en als standaardinstelling.	Data management plan.
Rechten van betrokkene(n)	Technische gevolgen van de rechten van de betrokkene(n) in functie van rechtmatigheid.	Onderlinge regeling of overeenkomst conform artikel 28 GDPR, Artikels 12-22 GDPR.	Eventueel beperkingen rechten volgens artikel 23 (zie kaderwet AVG).

Technische maatregelen voor databronnen (matrix, kolom 1)

De data-bronnen dienen bij de uitwisseling van gezondheidsgegevens te voldoen aan voorwaarden die vervat zitten in **de cirkels van vertrouwen**. Op het moment van de redactie van deze tekst was het eHealth-platform bezig met het opstellen van nieuwe criteria die zullen worden opgelegd aan alle actoren die deelnemen aan de uitwisseling van gezondheidsgegevens. Het is bijgevolg ook wenselijk die criteria als uitgangspunt te nemen voor het uitwisselen van gegevens met het onderzoeksplatform.

Hoewel de voorwaarden van de cirkels van vertrouwen een belangrijke basis zijn, volstaan de voorgeschreven maatregelen niet. Ze bieden immers te weinig bescherming voor het uitwisselen van gegevens voor onderzoeksdoeleinden. Zoals toegelicht in hoofdstuk 5 dienen persoonsgegevens die voor wetenschappelijke doeleinden worden uitgewisseld, in beginsel **geanonimiseerd** te verlopen. Het onderzoeksdoel kan echter vereisen dat pseudonimisering noodzakelijk is. Indien dat zelfs niet mogelijk is, dan pas zullen de uitgewisselde gegevens niet-**gepseudonimiseerd** verlopen.

De anonimisering en pseudonimisering dienen te gebeuren **in opdracht** en volgens de criteria van de **verzendende partij** (die als verwerkingsverantwoordelijke wordt beschouwd voor de oorspronkelijke verwerking). Hierbij wordt, zoals voorzien in de kaderwet AVG, het advies van de **Data Protection Officer (DPO)** gevraagd. We stellen voor dat er in ieder geval wordt gewerkt aan een **standaardset** van afspraken voor pseudonimisering. Het gebruik van de basisdiensten van het **eHealth-platform** voor anonimisering en pseudonimisering is hierbij zeker een optie. Hierbij kan het eHealth-platform optreden als *Trusted Third Party* (*cf. infra*).

Wanneer voor de uitwisseling van de gegevens gebruik wordt gemaakt van het eHealth-platform als TTP, zal daarenboven ook een principiële beraadslaging van het **Informatieveiligheidscomité** vereist zijn. Die principiële beraadslaging beschrijft onder meer de genomen technische maatregelen.

Net zoals alle communicatiepartners zullen de databronnen alle communicatie over een **veilige verbinding** moeten organiseren. Een degelijke **versleuteling** van het communicatiekanaal is hierbij noodzakelijk. Daarnaast is een duidelijke identificatie van zender en ontvanger op een unieke en betrouwbare manier eveneens noodzakelijk. In die context kan

worden nagedacht over een specifiek **eHealth-certificaat** dat onderzoekspartners uniek identificeert. Technisch kan een dergelijk certificaat op dezelfde eigenschappen gestoeld zijn als de huidige eHealth-certificaten. Maar het toepassingsgebied moet anders zijn. Bij voorkeur is er een **onderscheid** tussen de eHealth-certificaten voor **onderzoek** en die voor gegevensdeling in het kader van **zorg**.

Met het oog op de uitoefening van de rechten van de betrokkene(n) zal voorafgaandelijk aan de doorgifte van persoonsgegevens door de data-bronnen, nagedacht moeten worden over de rechtmatigheidsgrond en de hieraan gekoppelde rechten.

> *Ter illustratie: wanneer de rechtmatigheid de toestemming is, dan moet die toestemming in de volledige levenscyclus worden beheerd en dient op aangeven van de patiënt (al dan niet door de patiënt zelf) de toestemming worden aangepast of ingetrokken. Hierbij moet het daarenboven duidelijk zijn wie hiervoor het aanspreekpunt is (de databron dan wel het onderzoeksplatform). Bij een verwerking met als rechtmatigheidsgrond het algemeen belang (dat we als belangrijkste grond naar voren schuiven, zie ook de juridische analyse), zijn andere rechten van toepassing en moeten mogelijk ook de criteria uit de kaderwet mee in rekenschap worden genomen.*

Om ervoor te zorgen dat de rechten kunnen worden uitgevoerd zonder de integriteit van het onderzoek of de daaraan gekoppelde datasets te schaden, zal een goed **Data Management Plan** deel moeten uitmaken van de architectuur van het onderzoeksplatform.

Technische maatregelen voor onderzoeksplatform (matrix kolom 2)

We gaven reeds aan dat het hanteren van de **ISO 27001 standaard** een goede praktijk is voor het onderzoeksplatform. De selectie van maatregelen die men dient te nemen (de zogenaamde *Statement of Applicability*) komen bijgevolg zeker uit ISO 27002.

Afhankelijk van het al dan niet van toepassing zijn van de **NIS-regelgeving** (cf. *supra*), zal de norm niet alleen naar behoren moeten worden toegepast, maar is het ook noodzakelijk het **ISMS** te laten certificeren. Dat moet dan gebeuren door een geaccrediteerde instelling. Los van die wettelijke verplichting is een dergelijke **certificatie** wenselijk. We zien in Europa dat soortgelijke onderzoeksplatformen een dergelijke certificatie behaalden (bv. EBMT, een onderzoeksplatform verbonden aan *The European Society for Blood and Marrow Transplantation*).

Daarnaast verdient het **toegangsbeheer** de nodige aandacht. In de **kaderwet AVG** is in artikel 9 de verplichting opgenomen om voor de verwerking van gezondheidsgegevens de categorieën van personen die toegang hebben tot de persoonsgegevens aan te duiden, waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig wordt omschreven. Die personen zijn daarnaast ook onderworpen aan de **verplichting** om de gegevens **vertrouwelijk** te behandelen (door een wettelijke, statutaire of contractuele verplichting).

Om het toegangsbeheer af te dwingen dienen de gebruikers op een deugdelijke manier geïdentificeerd te worden. Dit betekent dat de **autorisatie** van de gebruikers dient te gebeuren via een **eIDAS-**conforme[49] benadering (cf. Verordening (EU) nr. 910/2014). De **FAS** (Federale Authenticatie Service), inclusief **Itsme** en **TOTP**, zijn gratis beschikbaar voor de actoren in de gezondheid en de diensten die ze aanbieden.

Als **authenticatieniveau** lijkt ons eIDAS niveau 'substantieel' gepast. Voor het eIDAS-niveau 'substantieel' zijn striktere methoden voor de identiteitsverificatie nodig. Dat betekent dat het authenticatiemiddel op een betrouwbare manier moet kunnen worden aangevraagd, inclusief een degelijke controle van de identiteit van de aanvrager.

Voor het type authenticatiemiddel is **tweefactorauthenticatie** vereist. Het middel moet zo ontworpen zijn dat het alleen onder controle van de gebruiker kan worden gebruikt. Het mag niet mogelijk zijn dat het per ongeluk of ongemerkt door een ander kan worden gebruikt. Ten slotte geldt voor eIDAS 'substantieel' een eis voor het authenticatiemechanisme zelf. Er moet sprake zijn van **dynamische authenticatie**: de (cryptografische) gegevens voor de authenticatie veranderen bij ieder gebruik. Dat biedt extra bescherming tegen fraudeurs die gegevens willen stelen en hergebruiken.

Ter verantwoording voor de omgang met de aan het platform verbonden **risico's** is het noodzakelijk dat bij het ontwerp van het platform en tijdens de realisatie ervan rekening wordt gehouden met **design principes voor gegevensbescherming en informatieveiligheid**. De gehanteerde principes dienen te worden gedocumenteerd en eventuele risico-acceptatievoorwaarden dienen formeel te worden vastgelegd. Als methodologie kunnen de ontwerpprincipes van ENISA[50] als kader worden gebruikt. Het geheel aan risico's en maatregelen dienen bovendien te worden opgenomen in een **Gegevensbeschermingseffectbeoordeling**. Een belangrijk aspect hierbij is uiteraard ook het **monitoren** van de vastgelegde veiligheidsprincipes voor en tijdens de productiefase. Bij de **ontwikkeling** moet rekening worden gehouden met veilige **methodes** (bv. het handteren van OWASP (*Open Web Application Security Project*), **richtlijnen** en het testen van die principes in zogenaamde **penetratietesten**, waarbij *ethical hackers* het platform testen op veiligheid.

Al die maatregelen dienen voor het onderzoeksplatform onder toezicht en advies van een **DPO of functionaris voor de gegevensbescherming** te worden geplaatst.

Voor alle systeemcomponenten, maar zeker ook voor het onderzoeksplatform zelf, is het noodzakelijk dat elke verwerking die plaatsvindt, kan worden verantwoord. Naast toegangsbeveiliging is met andere woorden een degelijke **logging** vereist, die alle transacties logt (wie? wat? waarom? wanneer?). Die logging moet betrouwbaar zijn conform de CIA-maatregelen. Noodzakelijke eigenschappen zijn:

- **Confidentialiteit**: uiteraard bevatten deze logbestanden persoonsgerelateerde data en is de confidentialiteit (*wie* mag de loggegevens raadplegen), van essentieel belang.
- **Integriteit**: we moeten zeker kunnen zijn dat de logbestanden niet zijn aangepast. Hiervoor is een eerlijke weergave van wie wat deed, wanneer en waarom cruciaal.
- **Beschikbaarheid**: daarnaast moet de logging te allen tijde beschikbaar zijn, ook bijvoorbeeld na een inbraak op het systeem. Dat betekent dat de logging op een andere plaats dan het productiesysteem wordt bewaard.

Belangrijk**: logging voor de patiënt.** De loggegevens beschikbaar stellen voor een patiënt in een leesbare, begrijpbare en (mogelijk) in een geaggregeerde vorm, kan de **transparantie** van de werking van het platform bevorderen. Ook moet dat op eenvoudige en toegankelijke wijze opvraagbaar zijn. Zoals ook omschreven in de toelichting van het ethisch kader (hoofdstuk 7) is dat een vorm van **distributieve rechtvaardigheid** die deel uitmaakt van de criteria om de werking van het platform te rechtvaardigen.

Voor wat betreft de rechten van de betrokkene dienen, zoals reeds eerder besproken bij de technische maatregelen met betrekking tot de databronnen, de hoedanigheid worden bepaald en vervolgens, afhankelijk van de kwalificatie (verwerker of (gezamenlijke) verwerkingsverantwoordelijke) een **GDPR-conform handvest** worden opgesteld. In geval van een relatie van een verwerker betreft dit een verwerkersovereenkomst. In geval van (gezamenlijke) verwerkingsverantwoordelijke is dit een onderlinge regeling. In geval van een transfer tussen derden kan een *Data Transfer Agreement* (DTA) worden overwogen. Telkens dienen de veiligheidsmaatregelen te worden opgenomen, alsook de uitoefening van de rechten van de betrokkene.

Bij het verder uittekenen van de architectuur kan worden nagedacht over het opbouwen van een portaal voor de patiënt/betrokkene waarop rechten kunnen worden uitgeoefend. Dat **patiëntenportaal** biedt elke patiënt de mogelijkheid om rechten uit te oefenen (zoals voor welke doeleinden wordt mijn data gebruikt, geven of intrekken van een toestemming, uitoefenen van het recht om vergeten te worden).

Technische maatregelen voor de 'Trusted Third Party' (TTP) (matrix kolom 2)

Bovenop de technische maatregelen voor het onderzoeksplatform dient ook voor de *Trusted Third Party* (TTP) een veiligheidsniveau te worden bepaald. De TTP dient hierbij als verwerker te worden beschouwd van de verzendende partij, die de modaliteiten bepaalt voor de anonimisering en/of pseudonimisering.

Volgens artikel 203 van de kaderwet AVG is de TTP:

1. Onderworpen aan het **beroepsgeheim** in de zin van artikel 458 van het Strafwetboek, onder voorbehoud van andere bepalingen van die wet en van GDPR.
2. **Niet afhankelijk** van de persoon die verantwoordelijk is voor de oorspronkelijke en de verdere verwerking.

Een mogelijke TTP is het eHealth-platform, dat voldoet aan de vereisten van de eIDAS verordening, voldoet aan de onafhankelijkheidsvoorwaarden én gratis ter beschikking is.

Let wel, bij het gebruik van deze diensten is het Informatieveiligheidscomité bevoegd om beraadslagingen te formuleren. Die beraadslagingen gaan na of de beginselen van GDPR worden gerespecteerd en of de adequate technische en organisatorische veiligheidsmaatregelen zijn genomen alvorens de diensten van het eHealth-platform kunnen worden gebruikt. Die beraadslagingen zijn met betrekking tot deze technische en organisatorische maatregelen eerder generiek. Ze vertrekken van algemene goede praktijken en generieke risico's.

Technische maatregelen voor onderzoeksinstellingen (matrix kolom 3)

De onderzoeksinstellingen tot slot, dienen verantwoording af te leggen over de identificeerbaarheid van de gegevens. Daarnaast is het noodzakelijk dat de onderzoeksinstellingen hun technische en organisatorische veiligheidsmaatregelen vastleggen in een **Data Management Plan.**[51]

Hierin moet onder meer (ook) aandacht zijn voor het gebruik van persoonsgegevens bij de publicatie van de onderzoeksresultaten. Het Data Management Plan moet op een transparante manier garanties bieden dat de onderzoekers op een veilige en betrouwbare manier omgaan met de gegevens van het onderzoeksplatform. Het plan moet daarom volgens een vast format worden opgesteld en nagekeken door de *Data Protection Officer* (DPO) van het platform. Diens advies moet mee worden geëvalueerd, bijvoorbeeld door een ethisch comité.

Opgelet: Voor deze doelgroep zijn de eisen voor identificatie naar alle waarschijnlijkheid het meest lastig te realiseren. Onderzoeksinstellingen nemen vandaag zelden actief deel aan big-data-projecten van die orde. Ze hebben niet de ervaring met het uitwisselen van gezondheidsgegevens zoals de databronnen, laat staan dat ze over authenticatietokens zoals eHealth-certificaten beschikken. Om hen een plaats te geven in dit project moet worden nagedacht over de manier waarop deze organisaties of individuen zichzelf op een betrouwbare manier kunnen identificeren (cf. eIDAS 'substantieel' als authenticatieniveau).

Voor elke studie dient te worden vastgelegd in welke mate de rechten van de betrokkene(n) kunnen worden nageleefd en dienen technische voorzieningen te worden geïmplementeerd om die te garanderen.

6.4. Verantwoording inzake gegevensbescherming en informatieveiligheid

Zoals vermeld in hoofdstuk 5 dienen in het kader van **GDPR verantwoordingsprincipes** te worden gerespecteerd. We herhalen die hieronder en duiden telkens aan welke de verantwoordingsverplichtingen inzake **informatieveiligheid** zijn.

6.4.1. Een gegevensbeschermingsbeleid

Elke verwerkingsverantwoordelijke dient een gegevensbeschermingsbeleid uit te werken (zie ook AVG artikel 24.2). Dat beleid omvat onder meer de technische en organisatorische maatregelen die van toepassing zijn. Voor het onderzoeksplatform is dus een uitgeschreven informatieveiligheidsbeleid noodzakelijk.

6.4.2. Een register van verwerkingsactiviteiten

Elke verwerker én verwerkingsverantwoordelijke dient een register voor verwerkingsactiviteiten aan te leggen. De verwerkingsverantwoordelijke beschrijft in dit register de technische en organisatorische maatregelen, waaronder de pseudonimisering.

6.4.3. De gegevensbeschermingseffectbeoordeling

Een verwerkingsverantwoordelijke dient voor elke risicovolle verwerking zoals beschreven in AVG artikel 35, een gegevensbeschermingseffectbeoordeling te maken.

Het is een aanbeveling, met het oog op een praktische uitwerking, die beoordeling op het niveau van het onderzoeksplatform te maken, evenals voor elk type van onderzoeksactiviteit. Hierin moet duidelijk zijn op welke manier de technische en organisatorische maatregelen de risico's op rechten en vrijheden afschermen.

6.4.4. Beheer van verwerker en personeel

Conform artikel 28 AVG dienen de overeenkomsten met verwerkers (ook) elementen rond informatieveiligheid te bevatten. Daarnaast moeten alle personeelsleden (van zowel verwerkingsverantwoordelijke als verwerker) de noodzakelijke instructies krijgen inzake vertrouwelijkheid en informatieveiligheid.

6.4.5. Verantwoording betreffende de uitwisseling: bijkomende verplichtingen

Bij de uitrol van het onderzoeksplatform dient men rekening te houden met bijkomende verantwoordingsprincipes. Welke principes finaal zullen moeten worden toegepast zal pas duidelijk zijn wanneer dit platform verder vorm krijgt. Voornamelijk het juridische opzet heeft hierop een belangrijke invloed, alsook de keuze om al dan niet met diensten van het eHealth-platform te werken. Hieronder geven we enkele belangrijke elementen mee die bijkomend mee in rekening moeten worden gebracht.

Verantwoording aan de gegevensbeschermingsautoriteit of Vlaamse toezichtcommissie

Het onderzoeksplatform en de aangesloten instanties kunnen, indien ze voldoen aan de hieronder opgesomde criteria, worden beschouwd als een instelling met een publieke taak van artikel I.3, 6° bestuursdecreet (en vallen dus onder toezicht van de Vlaamse Toezichtcommissie) indien:

- Het wordt opgericht met het specifieke doel te voorzien in behoeften van algemeen belang die niet van industriële of commerciële aard zijn.
- Het een rechtspersoonlijkheid bezit.
- En dit in drie mogelijke gevallen (niet cumulatief):
    - > Ofwel wordt het platform voor meer dan de helft gefinancierd door de Vlaamse overheid, een lokale overheid of een andere instelling met een publieke taak;
    - > Ofwel hebben de Vlaamse overheid, een lokale overheid of een andere instelling met een publieke taak meer dan de helft van de stemmen in de raad van bestuur;
    - > Ofwel staat het beheer onder toezicht van de Vlaamse overheid, een lokale overheid of een andere instelling met een publieke taak.

Deelnemers aan het onderzoeksplatform, evenals het platform zelf, kunnen bijgevolg of verantwoording moeten afleggen aan de Vlaamse toezichtcommissie of de Gegevensbeschermingsautoriteit.

Verantwoording door middel van een protocolverplichting

Bij uitwisseling van gegevens door een Vlaamse bestuursinstantie aan een andere Vlaamse instantie, of externe overheid of federale instantie aan een andere overheid of privé-instantie, bestaat een verplichting tot het opstellen van een protocol. Voor federale bronnen legt de Kaderwet AVG die verplichting op. Voor Vlaamse bestuursinstanties bepaalt het AVG decreet de verplichting.[52]

Deze protocollen moeten na advies van de DPO worden gepubliceerd op de website van alle betrokken instanties en de inhoud is wettelijk vastgelegd in de overeenkomstige regelgeving. Voor federale instanties geldt bovendien dat indien het advies van de DPO negatief is en de verwerking toch doorgaat, de instantie zich hierover schriftelijk moet verantwoorden. Voor Vlaamse bestuursinstanties kan een protocol worden voorgelegd aan de Vlaamse Toezichtcommissie.

De protocolverplichting is niet van toepassing indien:

- De wet dit expliciet uitsluit (bv. bijzondere opsporingsdiensten)
- De uitwisseling van gezondheidsgegevens door een Vlaamse bestuursinstantie onderworpen is aan een principiële beraadslaging door het informatieveiligheidscomité (IVC).

Machtiging door het Informatieveiligheidscomité

Dat brengt ons bij de vraag: wanneer is een verwerking onderworpen aan een principiële beraadslaging door het IVC? De modaliteiten voor een beraadslaging door het IVC bij de uitwisseling van gezondheidsgegevens is beschreven in artikel 42 van de wet van 13 december 2006 houdende diverse bepalingen betreffende gezondheid. Afhankelijk van de gemaakte keuzes zal een dergelijke principiële machtiging vereist zijn.

Het Informatieveiligheidscomité (meer specifiek de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité) is bevoegd voor het verlenen van een principiële machtiging met betrekking tot elke mededeling van persoonsgegevens die de gezondheid betreffen, behalve in de volgende gevallen:

- Indien de mededeling gebeurt tussen beroepsbeoefenaars in de gezondheidszorg die door het beroepsgeheim gebonden zijn en persoonlijk betrokken zijn bij de uitvoering van diagnostische, preventieve of zorgverlenende handelingen ten opzichte van een patiënt.
- Indien de mededeling is toegestaan door of krachtens een wet, een decreet of een ordonnantie, na advies door de Commissie voor de bescherming van de persoonlijke levenssfeer.
- Indien als dusdanig bepaald in een KB.
- Indien gegevens worden meegedeeld tussen instanties van eenzelfde Gemeenschap of Gewest die geen gebruik maken van de basisdiensten van het eHealth-platform.

Hoofdstuk 7
Is het allemaal ook ethisch verantwoord?

Big data, het gebruik van data, het delen van gegevens en het hergebruik ervan: het roept allemaal belangrijke ethische vragen op. Hoe kan dat alles op een ethisch verantwoorde manier verlopen? Welke principes en normen staan hier op het spel? Op welke ethische argumenten kunnen we dit voorstel stoelen? En hoe kunnen we een ethisch verantwoorde koers blijven aanhouden? Dit hoofdstuk probeert die vragen te beantwoorden. Gebaseerd op internationale wetenschappelijke literatuur doen we vier clusters van ethische principes uit de doeken.

7.1. Uitgangspositie: vier overkoepelende ethische thema's

In de internationale literatuur bestaat er een overvloed aan ethische principes en normen rond big data. Vooralsnog bestaat er geen breed gedragen *governance framework*. Het is wel mogelijk om **convergentie** te zien binnen die enorme hoeveelheid en variatie van principes en normen op een hoger aggregatief niveau. We onderscheiden **vier overkoepelende thema's**[53]:

1. Maatschappelijke meerwaarde;
2. Rechtvaardige verdeling van risico's, baten en lasten;
3. Respect voor individuen en groepen;
4. Publiek vertrouwen en duurzaam engagement.

We staan achtereenvolgens stil bij de implicaties van die vier thema's.

7.1.1. Maatschappelijke meerwaarde

Vanuit een ethisch perspectief moet de **finaliteit** van gegevensdeling gestoeld zijn op de maatschappelijke meerwaarde ervan. De activiteiten moeten worden beheerd volgens principes die zo maximaal mogelijk ten goede komen van gezondheid en welzijn (van zowel individuen als het bredere publiek) en moeten ten dienste staan van het **maatschappelijke belang**.

Dus: zolang het platform ten dienste staat van het algemeen belang, met name wetenschappelijk onderzoek, ontwikkeling en overheidsbeleid inzake welzijns- en gezondheidszorg vooruithelpt, is het goed. Om die finaliteit te bekomen, zijn er een aantal noodzakelijke randvoorwaarden te vervullen[54]:

- **Datakwaliteit:** goede kwaliteit en volledigheid van data is noodzakelijk. Dat vereist continue inspanningen voor datakwaliteit en –reproduceerbaarheid.
- **Wetenschappelijke validiteit:** er moet een aantoonbare wetenschappelijke validiteit en maatschappelijke meerwaarde zijn.
- **Gegevensdelingsinfrastructuur:** we hebben een toegankelijke gegevensdelingsinfrastructuur nodig die efficiënt kan worden gebruikt, interoperabel is, en toekomstbestendig. Dat vraagt om harmonisering van toegangsvoorwaarden en procedures, en om duurzame strategieën, processen en/of systemen.
- **Sensibilisering:** er dient actief en duurzaam werk te worden gemaakt van sensibilisering van het publiek bewustzijn over de voordelen van gegevensdeling tussen de verschillende stakeholders. Breed toegankelijke informatie en communicatie zijn onontbeerlijk.
- **Samenwerkingsverbanden:** we dienen samenwerkingsverbanden en praktijken van gegevensdeling constructief en duurzaam te promoten. Dat houdt ook in dat we allerlei belemmerende factoren wegwerken.
- **Disseminatie:** de resultaten moeten effectief en transparant worden gedissemineerd naar de samenleving toe.
- **Governance:** we hebben we *stakeholder-informed principles* nodig en *governance*-structuren die ervoor zorgen dat de noden en behoeften van *alle* betrokken stakeholders worden geïntegreerd in de initiatieven van gegevensdeling.

7.1.2 Verdelende rechtvaardigheid[55]

Praktijken en initiatieven van gegevensdeling moeten in overeenstemming zijn met de principes van verdelende rechtvaardigheid. Dat wil zeggen: de **voordelen** voor individu en samenleving moeten worden gemaximaliseerd en de **nadelige effecten** geminimaliseerd. Alles moet dus proportioneel met elkaar in evenwicht zijn (**principe van proportionaliteit**).

Verdelende rechtvaardigheid houdt ook in dat **billijke toegang** moet worden gegarandeerd door regels voor transparantie, *fair access fees* en een evenwicht tussen de noden van de eigenaars, *secondary users* en de bredere gemeenschap die gezondheidsvoordeel moet kunnen verwachten.

Toegang moet worden gebaseerd op goede en evenwichtige overeenkomsten tussen **publieke en private** spelers waarin de vraag naar het *bona fide* karakter van de laatste centraal staat, namelijk dat de onderzoeksvraag ten dienste staat van het verwerven van nieuwe kennis voor het algemeen gezondheidsbelang en dat die kennis publiek toegankelijk wordt gemaakt zonder onnodige vertraging (commerciële belangen zijn dus *in se* geen afdoende reden om de toegang te beperken).

7.1.3. Respect voor individuen en groepen[56]

Een van de fundamentele pijlers van de hedendaagse biomedische ethiek is het principe van respect voor de autonomie van personen. Binnen het domein van gegevensdeling uit dit principe van respect zich via het **principe van geïnformeerde toestemming**.

De uitgangpositie is dat de doelen van gegevensdeling gebeuren in overeenstemming met de principes van *informed consent*, al dan niet inclusief de reikwijdte van het oorspronkelijk gegeven *informed consent*. Hierbij wordt er onderscheid gemaakt tussen *specific informed consent* en *broad informed consent* of *dynamic informed consent* om ethische onderbouw te geven aan toekomstig datagebruik.

Wanneer *specific informed consent* niet mogelijk/aangewezen is (zie ook hoofdstuk 5), dan kan *broad informed consent* of *presumed informed consent* gelegitimeerd zijn. Voorwaarde is dat er **additionele waarborgen** zijn, zoals een deugdelijke *governance* structuur, zekerheid over het doel van secundair gebruik (wetenschappelijk onderzoek in algemeen belang), en voldoende informatie aan alle stakeholders (dit wordt ook bevestigd door het juridisch kader in hoofdstuk 5).

Hier is dan een officieel en onafhankelijk **orgaan** voor nodig dat de waarborgen bewaakt en de *data access* zou kunnen toestaan (zoals bv. een *Research Ethics Committee*, of zoals in het voorliggend voorstel, een onafhankelijk onderzoeksplatform met TTP). Ook op dat vlak geldt het principe van proportionaliteit.

Normen over de principes van **privacy en geheimhouding** brengen ons tot bij het instellen en periodiek updaten van veiligheidsmaatregelen (m.b.t. data transfer & access, verificatie en authenticatie…), protocollen (bv. werkingsprincipes inzake confidentialiteit, procedures voor toegang…) en andere beschermingsmaatregelen (bv. *for research purposes only*) die proportioneel zijn in relatie tot het gebruik en de aard van de data (geanonimiseerd/gepseudonimiseerd). Essentieel onderdeel hiervan is opleiding en permanente vorming van onderzoekers voor *data security* en *privacy compliance* (als voorwaarde voor *authorised access*). (Zie ook hoofdstuk 6, luik informatieveiligheid).

7.1.4. Publiek vertrouwen en duurzaam engagement[57]

Publiek vertrouwen

Alles staat of valt met het publiek vertrouwen in de praktijk van gegevensdeling. Die is gestoeld op het ethisch verantwoorde karakter ervan. Om dit te kunnen garanderen en legitimeren dienen we de volgende voorwaarden te vervullen:

- **Participatiemodel**: we moeten actief en duurzaam inzetten op de effectieve betrokkenheid en/of participatie van relevante stakeholders in het maatschappelijke debat en de feitelijke praktijken van gegevensdeling. Dit dient zowel procesmatig als inhoudelijk te worden gegarandeerd.
- **Procesparticipatie**: procesmatig moet deze betrokkenheid aanwezig zijn in het design, de *governance* en review van initiatieven voor gegevensdeling waarvan de resultaten uiteindelijk in beleid zullen worden vertaald.
- **Inhoudsparticipatie**: inhoudelijk dienen we formats en mechanismen te ontwikkelen die een effectieve deliberatie met de relevante stakeholders over belangwekkende kwesties inzake gegevensdeling kunnen bewerkstelligen. Dat houdt onder meer in dat de patiënt- en burgerbetrokkenheid wordt verhoogd via events en workshops voor disseminatie van de onderzoeksresultaten; dat we panels, conferenties of workshops organiseren voor een breed publiek; dat er stuurgroepen of werkgroepen worden ingericht om zo de participanten en het bredere publiek een effectieve en betekenisvolle stem te geven in de *governance* van gegevensdeling.
- **Organen & tools:** Het is essentieel dat we over *trusted intermediaries* kunnen beschikken (TTPs), alsook over *easy-to-use* tools om gegevensdeling überhaupt mogelijk te maken op een ethisch en juridisch verantwoorde manier.

Het principe van transparantie

Dit loopt als een rode draad doorheen de literatuur als cruciale component van *responsible data sharing*. Het betreft transparantie in de gehele workflow van gegevensdeling en -transactie, alsook disseminatie van publieke informatie over bestaande initiatieven en praktijken van gegevensdeling. Daarbij komt ook dat er inspanningen moeten worden geleverd om binnen een transparante debatcultuur het maatschappelijke bewustzijn aan te scherpen over het doel, de noodzaak en meerwaarde van gegevensdeling in het kader van de democratisering van het gezondheidsonderzoek.

Governance structuur

De governance structuur moet beantwoorden aan de ethische principes van **integriteit, solidariteit en verantwoording** inzake de praktijk van gegevensdeling. Elk initiatief moet opereren in het kader van een expliciet publieke ethiek en ethisch verantwoorde *governance*. Dat houdt in dat:

- De verantwoordelijkheden/vertegenwoordigers van de respectievelijk betrokken individuen of partijen duidelijk omschreven en afgebakend zijn.
- Dat er heldere verantwoordingsmechanismen worden uitgetekend (bv. of het initiatief van gegevensdeling effectief voldoet aan alle gestelde voorwaarden).
- Men zich houdt aan de principes van *good stewardship* in het bewaren, consulteren, delen en monitoren van de data.
- Dat er meer specifiek een *governance committee* wordt ingesteld dat toeziet op het beleid inzake gegevensdeling.
- Dat men zich te allen tijde dient te houden aan de wettelijke randvoorwaarden, ethische principes en gestelde samenwerkingsovereenkomsten.
- Dat er voldoende wordt geïnvesteerd in professionalisering terzake (vorming en training van betrokkenen), alsook in goede informatie en communicatie met patiënten en het bredere publiek.

- Dat de *review* en *approval* procedures worden uitgevoerd door een onafhankelijk *Research Ethics Committee* of vergelijkbaar orgaan (zoals in voorliggend voorstel).
- Dat toegang en gebruik gebaseerd is op de legitimiteit van de onderzoeksvraag, op objectieve en helder geformuleerde criteria (gerapporteerd in beleidsdocumenten), en enkel mogelijk voor geautoriseerde onderzoekers (die voldoende aantoonbare *data security training* hebben gehad) en die onderhavig zijn aan supervisie en mogelijke sanctionering bij misbruik.
- Dat toegang en gebruik wordt gereguleerd in bindende overeenkomsten (*Data Access Agreements (DAAs)/Data Transfer Agreements (DTAs)*, die idealiter in een gestandaardiseerd format opgesteld zijn ten behoeve van uniform en consistent gebruik.

7.2. Set van ijkpunten voor ethische weging

Het ethisch raamwerk dat wordt geboden in dit hoofdstuk is gebaseerd op een zeer recent gepubliceerde (maart 2018) systematische review van internationale literatuur over ethische principes en normen aangaande *responsible data sharing in international health research*. Het zorgt ervoor dat dit kader kan worden beschouwd als een **up-to-date en volledig raamwerk van ethische toetsingspunten** voor gegevensdeling en (her)gebruik van data voor wetenschappelijk onderzoek in de gezondheidszorg.

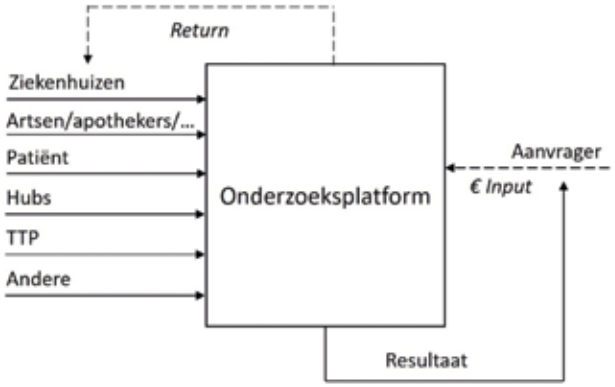
In dit conceptvoorstel maakten we meermaals melding van de noodzaak van een op te richten **orgaan** dat waakt over het verantwoord (her)gebruik van de data en dat kan bevestigen dat de aanvragen tot gebruik van data wel vallen onder de uitzonderingen voorzien voor onderzoek in publiek belang. In dezelfde lijn stelden we dat binnen het onderzoeksplatform een (ethische) **commissie** fungeert die de aanvragen juridisch en ethisch toetst. Die commissie kan eventueel ook de beleidslijnen voor de controle van het proces vastleggen en toezien op de uitvoering van die controle. Het ethisch raamwerk in dit hoofdstuk biedt aan deze (op te richten) commissie alvast de volledige set van ijkpunten voor inhoudelijke en procesmatige ethische weging.

Hoofdstuk 8
Businessmodel en financiering

In de vorige hoofdstukken stonden we grondig stil bij de technische, juridische, ethische en privacy gerelateerde randvoorwaarden voor gegevensdeling en (her)gebruik van gezondheidsgegevens voor onderzoek. Inhoudelijk en procesmatig creëerden we een kader voor verder maatschappelijk debat en concrete vormgeving. Maar hiermee stopt het niet. We moeten ook stilstaan bij de financiering van het onderzoeksplatform en de te vervullen randvoorwaarden. In dit afsluitende hoofdstuk bieden we hiervoor alvast een eerste aanzet.

8.1. Businessmodel

Onderstaande figuur geeft in grote lijnen weer wie welke inbreng levert.



De investeringen die het platform voeden en de partijen die deze investeringen inbrengen zijn zeer divers van aard:

- Ziekenhuizen: beheren/bekostigen de EPD-systemen die de gegevens aanleveren, genereren data via hun medewerkers, installeren de connector, ...
- Artsen/apothekers/thuisverpleging...: genereren data in het EMD, installeren de connector...
- Andere zorgactoren: woonzorgcentra, CGG, PVT, welzijnsactoren enz.: idem;
- Patiënt: stelt zijn gegevens ter beschikking en geeft vertrouwen;
- Hubs: technische aanpassingen aan de hub, ...
- Commissie-orgaan: toetst de aanvragen op juridisch en ethisch vlak;
- TTP: garandeert de privacy van de patiënten;
- Anderen: bv. het eHealth-platform levert basisdiensten, bv. gegevensbronnen van derden, ...

8.1.1. Input

De input bestaat in principe uit vier elementen: klinische gegevens, menselijke inzet, software en infrastructuur in de brede zin en financiële inbreng. De partijen die deze elementen aanreiken doen dat omwille van de maatschappelijke of financiële meerwaarde die kan worden gerealiseerd via de onderzoeksresultaten of via de extra mogelijkheden die het platform biedt.

Klinische gegevens

De motivatie voor het verstrekken van klinische gegevens kan niet financieel zijn. Zelfs al zou het wenselijk zijn een financiële vergoeding aan te rekenen hiervoor, dan zou het

simpelweg onmogelijk zijn een waarde toe te kennen aan de inbreng van eenieder. Gezien de aard van het beoogde onderzoek en de inzichten die het onderzoek zou opleveren, is de maatschappelijke meerwaarde die hiermee wordt gerealiseerd de belangrijkste drijfveer. Dat veronderstelt dat de partijen die klinische gegevens aanleveren (inclusief de patiënt) te allen tijde moeten overtuigd zijn en blijven van deze meerwaarde.

Zoals reeds eerder in het document vermeld wordt voor de klinische actoren een bijkomende meerwaarde voorzien, namelijk het verkrijgen van inzicht in het traject van de patiënt doorheen het zorgsysteem. Het traject van de patiënt is weliswaar ook samen te stellen uit de gegevens die toegankelijk zijn via de hubs, kluizen, ziekenhuisportalen, EMD's en dergelijke, maar dit samenstellen vergt tijd, tijd die niet voorhanden is.

Gezien het klinisch gebruik van de trajectgegevens zal het belangrijk zijn te beschikken over (quasi) **real-time gegevens**. Het heeft weinig zin het traject van de patiënt te raadplegen als men niet kan beschikken over de gegevens van (bijvoorbeeld) de laatste weken. Als men niet zeker kan zijn van de volledigheid van de gegevens zal men deze niet gebruiken. Het gaat echter over een grote hoeveelheid data die men beschikbaar dient te stellen. Het zou daarom technisch raadzaam zijn deze in een aantal batches per dag aan te leveren, waardoor men over quasi-real time gegevens kunnen spreken. Op die manier verhoogt de technische haalbaarheid zonder de waarde van de informatie te hypothekeren.

Bronnen van klinische gegevens: (algemene, psychiatrische, revalidatie-)ziekenhuizen, huisartsen, apothekers, woonzorgcentra, thuisverpleging, mutualiteiten, overheden, ...

Menselijke inzet

De menselijke inzet in deze is zeer divers en veronderstelt engagement van een groot aantal partijen. Menselijke inzet is onder meer nodig voor het creëren van draagvlak, voor de technische realisatie en voor het optimaal gebruik van het onderzoeksplatform.

Draagvlak

Zoals de voorgaande hoofdstukken overvloedig hebben aangetoond is het gebruik van patiëntengegevens voor het beoogde secondair gebruik geen evidentie. Blijvende inspanningen zullen moeten worden geleverd om het draagvlak uit te breiden. Dit is een gedeelde verantwoordelijkheid zowel van initiatiefnemers van het platform als van zij die van de onderzoeksresultaten genieten, inclusief patiënten(organisaties) en publieke actoren.

Technische realisatie

Voor de technische realisatie zal moeten worden teruggevallen op gespecialiseerde technische expertise. Het bouwen van de connectoren veronderstelt een goede kennis van de verschillende software-applicaties waar de zorgverstrekkers gebruik van maken en (gezien de link met eHealth) van de werking en de basisdiensten van het eHealth-platform. Idealiter wordt zoveel mogelijk van de technische realisatie van het platform gecentraliseerd, maar het moge duidelijk zijn dat omwille van de specificiteit van elke applicatie de inbreng van de betrokken softwareleverancier zal moeten worden gevraagd. Veel van deze leveranciers zijn echter goed vertrouwd met eHealth en afgeleiden (bv de healthdata-registers) zodat de incrementele inbreng die zij moeten doen haalbaar zou moeten zijn. Veel zal ook afhangen van de mate waarin hun klanten zullen vragen de nodige ontwikkelingen op te nemen in de jaarlijkse roadmap die met de leverancier wordt beslist. Hoe meer dat de ontwikkeling compatibel is met deze roadmap, hoe makkelijker deze beslissing. Hoe beperkter de nodige ontwikkeling, hoe makkelijker deze beslissing. Een implementatie van de connector in lijn met internationale standaarden (bv FHIR) zal sneller te realiseren zijn als men reeds voor deze standaard heeft geopteerd.

Naast het gebruik van de eHealth systemen/basisdiensten en het opteren voor internationale standaarden is het zoeken naar synergieën met complementaire initiatieven eveneens een goede manier om de inspanningen te minimaliseren.

Gebruik & Optimalisering

Ook voor het formuleren van onderzoeksvragen, het verwerken van de gegevens en de interpretatie van onderzoeksresultaten is menselijke inbreng vereist. Er zal beroep moeten gedaan worden op specialisten in de materie, profielen die niet eenvoudig aan te trekken zijn. Wellicht zal er beroep moeten worden gedaan op onderzoekscentra waar deze kennis aanwezig is en mogelijks kan ook de aanvrager van het onderzoek de nodige competentie aanreiken als dit onder gecontroleerde omstandigheden kan gebeuren.

Andere inspanningen die kunnen worden geleverd in deze situeren zich op het vlak van een goede gegevensregistratie. Hopelijk kan het onderzoeksplatform bijdragen aan de mate waarin zorgverstrekkers inzicht verwerven in het belang van een kwaliteitsvolle registratie. Een goede codering helpt niet enkel het eigen dossier meer uniform samen te stellen, maar levert ook veel voordelen op ikv gegevensdeling en draagt ten slotte ook bij tot een verruiming van de analyse-mogelijkheden. Er moet worden onderzocht in welke mate Natural Language Processing het maturiteitsniveau heeft bereikt om in deze een toegevoegde waarde te betekenen. Als dit het geval zou zijn kan NLP mogelijks ook een aantal administratieve processen makkelijker laten verlopen, wat nog een bijkomende meerwaarde zou kunnen betekenen.

Software en infrastructuur

Algemeen gesproken bestaat het beoogde ICT systeem grosso modo uit de volgende componenten: de zorg- en administratieve applicaties van de zorgverstrekkers, de connectoren, het eHealth platform en aanverwanten, de Trusted Third Party (TTP) en het platform waarop het onderzoek kan worden uitgevoerd. Het laatste zal wellicht specifiek moeten worden ontwikkeld en ingericht om de toegangs- en gebruiksvereisten te accommoderen die de stakeholders onderling afspreken en zal bijgevolg wellicht door een derde partij op maat moeten worden ontwikkeld.

De TTP daarentegen is een relatief generisch onderdeel in het geheel. De keuze van een TTP is ingegeven door kost, compatibiliteit met andere big-data-initiatieven en de mate waarin de TTP ook in aanvullende mogelijkheden kan voorzien. Als bijvoorbeeld rechtstreeks via de TTP nog een aantal andere gegevensbronnen kunnen worden aangeboord, kan dit een aanzienlijke toegevoegde waarde zijn voor het platform. Op die manier kunnen gezondheidsgegevens worden gecombineerd met gegevens van andere aard, bijvoorbeeld milieugegevens. Als men er voor dit laatste in slaagt om dit op een voldoende geaggregeerd niveau te doen, kan de keuze voor een bepaalde TTP dus ook een inhoudelijke meerwaarde opleveren.

8.1.2. Financiering op korte termijn

Hoe dan ook gaat het initiatief een lange periode tegemoet van voorbereiding. Niet alleen moeten de connectoren worden gebouwd, ook de gegevensbeschermingsautoriteit dient te worden geconsulteerd, de *governance* structuur dient te worden opgebouwd (inclusief ethisch comité) enz. Het resultaat is een lange periode waarin inspanningen worden geleverd zonder dat daar directe inkomsten tegenover staan.

Een financiering op korte termijn vanwege de **overheid** zou daarom optimaal zijn. Dat biedt een aantal voordelen:

- Overheidsfinanciering is overkoepelend: het aantal betrokken zorgverstrekkers is aanzienlijk.

- De maatschappelijke relevantie kan verzekerd worden: een financiële ondersteuning door commerciële partijen kan het systeem sturen in de richting van de belangen van die partijen.
- Compatibiliteit: de overheid financiert een initiatief dat voortbouwt op de eigen systemen.

Daarenboven zal de overheid mogelijks bij de eerste gebruikers kunnen worden gerekend. Er wordt immers gestart met onderzoek op basis van logistieke informatie (zie 3.3.1. 'Workflow onderzoek'). Dat kan inzichten bieden in het zorgsysteem die vooral interessant zijn voor de overheid, maar minder nuttig voor commerciële ondernemingen.

Een eerste bijdrage die de overheid kan leveren is het financieren van het vervolg van de voorstudie. Het onderzoeksplatform zal verder worden geconcretiseerd op basis van een aantal eenvoudige pilootprojecten (zie verder). Het in de steigers zetten van de bovenvermelde *governance* structuur en het realiseren van de pilootprojecten zijn bijgevolg de volgende stappen.

8.1.3. Financiering op lange termijn

Van zodra de *whereabouts* kunnen worden aangevuld met klinische informatie wordt onderzoek mogelijk dat meer van nut kan zijn voor commerciële partijen. Op dat moment moeten zij een deel van de financiering overnemen, via het bestellen van onderzoek op basis waarvan zij een (commerciële en maatschappelijke) meerwaarde kunnen realiseren.

De omvang van de inbreng zal dan ook in verhouding zijn tot deze meerwaarde, hoewel het verband uiteraard moeilijk te kwantificeren is. Het moet echter duidelijk zijn dat de uitbouw van het onderzoeksplatform op lange termijn voornamelijk van de inbreng van industriële partijen zal afhangen, ook omdat de inzichten van het onderzoek een meer tastbaar resultaat opleveren.

De structuur die vandaag wordt gecreëerd moet de financiering op lange termijn in zich dragen. Bijgevolg moet vandaag al expliciet rekening worden gehouden met de behoeften van de commerciële partijen op de lange termijn. Het zal dus zaak zijn die partijen te blijven betrekken bij de verdere uitbouw van het onderzoeksplatform.

8.1.4. Output

De mogelijke meerwaarde van het platform is reeds meerdere malen belicht. Hieronder nog kort een overzicht.

Klinische output

De klinische output bestaat in de eerste plaats over het zicht dat zorgverstrekkers bekomen op het traject van de patiënt doorheen het zorgsysteem. Naarmate meer zorgverstrekkers als gegevensbron voor het onderzoeksplatform kunnen optreden wordt deze output groter.

Een tweede klinische output is eerder onrechtstreeks en bestaat uit de klinische inzichten die de onderzoeksresultaten opleveren en de uit de mogelijke behandelingen die daaruit kunnen voortvloeien.

Het zijn vooral patiënten en zorgverstrekkers die de begunstigden zijn van deze output door respectievelijk het ontvangen van betere zorg en het beter kunnen verstrekken van zorg.

Commerciële output

Commerciële bedrijven kunnen de onderzoeksresultaten gebruiken voor productvernieuwing of -evaluatie.

Naast het commercieel voordeel is er onder de juiste omstandigheden ook het voordeel voor de patiënt die uiteindelijk kan gebruik maken van een verbeterd commercieel aanbod.

Maatschappelijke output

Klinische en commerciële output kunnen ook leiden naar maatschappelijke output. Daarnaast kunnen de onderzoeksresultaten ook de onderbouw vormen voor beter beleid met een maatschappelijk voordeel als gevolg.

8.2. Pilootprojecten

8.2.1. Uitgangspunt: draagvlak

Gedurende het gehele traject dat werd gevolgd voor de redactie van dit document zijn de reacties op het initiatief grotendeels positief geweest. Van vele partijen kregen we de expliciete vraag om blijvend te worden betrokken bij het vervolgtraject. Dat sterkt ons in de overtuiging dat het draagvlak voldoende groot is om de volgende stappen te zetten en dat er een plaats is te midden van de initiatieven die in het verleden reeds werden genomen.

8.2.2. Projectselectie

Tijdens het stakeholderoverleg werd het voorstel geopperd een aantal pilootprojecten te realiseren. Die kunnen worden gedefinieerd en geselecteerd op basis van de technische en organisatorische haalbaarheid en van de meerwaarde die kan worden bekomen. Na de publicatie van dit document zullen we stakeholders bijeenbrengen die kunnen bijdragen aan die pilootprojecten (zie ook verder). De verschillende stadia die kunnen worden onderscheiden om tot de uitvoering van de pilootprojecten te komen zijn de volgende:

1) Selectie van zorgverstrekkers

Een aantal zorgverstrekkers hebben reeds te kennen gegeven in een vroeg stadium van de verdere uitwerking betrokken te willen worden. De belangrijkste doelstelling in dit stadium is over een voldoende aantal zorgverstrekkers te beschikken om een aantal pilootprojecten te definiëren (zie volgende).

Zorgnet-icuro zal een grote groep zorgverstrekkers aanschrijven om hun eventuele interesse formeel te bevestigen.

2) Samenbrengen van stakeholders – voorbereiden governance structuur

Vermits het uiteindelijke onderzoek zal gebeuren op gegevens van verschillende zorgverstrekkers zal het initiatief van Zorgnet-Icuro gaandeweg moeten plaatsmaken voor **gedeeld eigenaarschap**. Niet enkel de geselecteerde zorgverstrekkers kunnen hier een rol opnemen. Ook andere stakeholders zoals patiënten, artsen, gebruikers van het onderzoeksplatform, verschillende overheden, andere zorgverstrekkers, etc. moeten worden betrokken in de mate van het haalbare. Zorgnet-Icuro zal samen met de geselecteerde zorgverstrekkers een voorstel uitwerken voor de verdere aansturing van het project. Ook het inbouwen van de nodige juridische, ethische en informatieveiligheidscontroles zijn hiervan een onderdeel.

3) Definitie van pilootprojecten

Bij de stakeholders zal worden gepeild naar mogelijke pilootprojecten die kunnen worden uitgevoerd. De beheersstructuur zoals die op dat moment is ingericht zal vervolgens op basis van criteria zoals de meerwaarde van het onderzoek, de juridische mogelijkheid, ethische overwegingen en technische haalbaarheid bepalen welke pilootprojecten kunnen worden uitgevoerd en wat hiervoor de randvoorwaarden zijn. Men zal daarbij ook expliciet rekening houden met de vraag of de uitvoering van het pilootproject maximaal gebruik maakt van de bestaande systemen en maximaal rekening houdt met bestaande initiatieven.

4) Financieringsaanvraag indienen

De pilootprojecten (één of meerdere) vormen dan de concrete basis waarop een financieringsaanvraag bij de overheid kan worden voorbereid. Alle beschikbare kanalen zullen worden bekeken. Deze situeren zich voornamelijk binnen het beleidsniveau zorg of economie en op Europees niveau. Van zodra de financieringsaanvraag (er kunnen er in principe ook meerdere zijn) is ingediend, is verdere opvolging nodig (bv. verdere toelichting). Er zal dan ook rekening moeten worden gehouden met mogelijke co-investeringen, hetzij van de betrokken zorgverstrekkers, hetzij van andere stakeholders, bijvoorbeeld de gebruikers van de resultaten van de pilootprojecten.

8.3 Permanente overlegstructuur

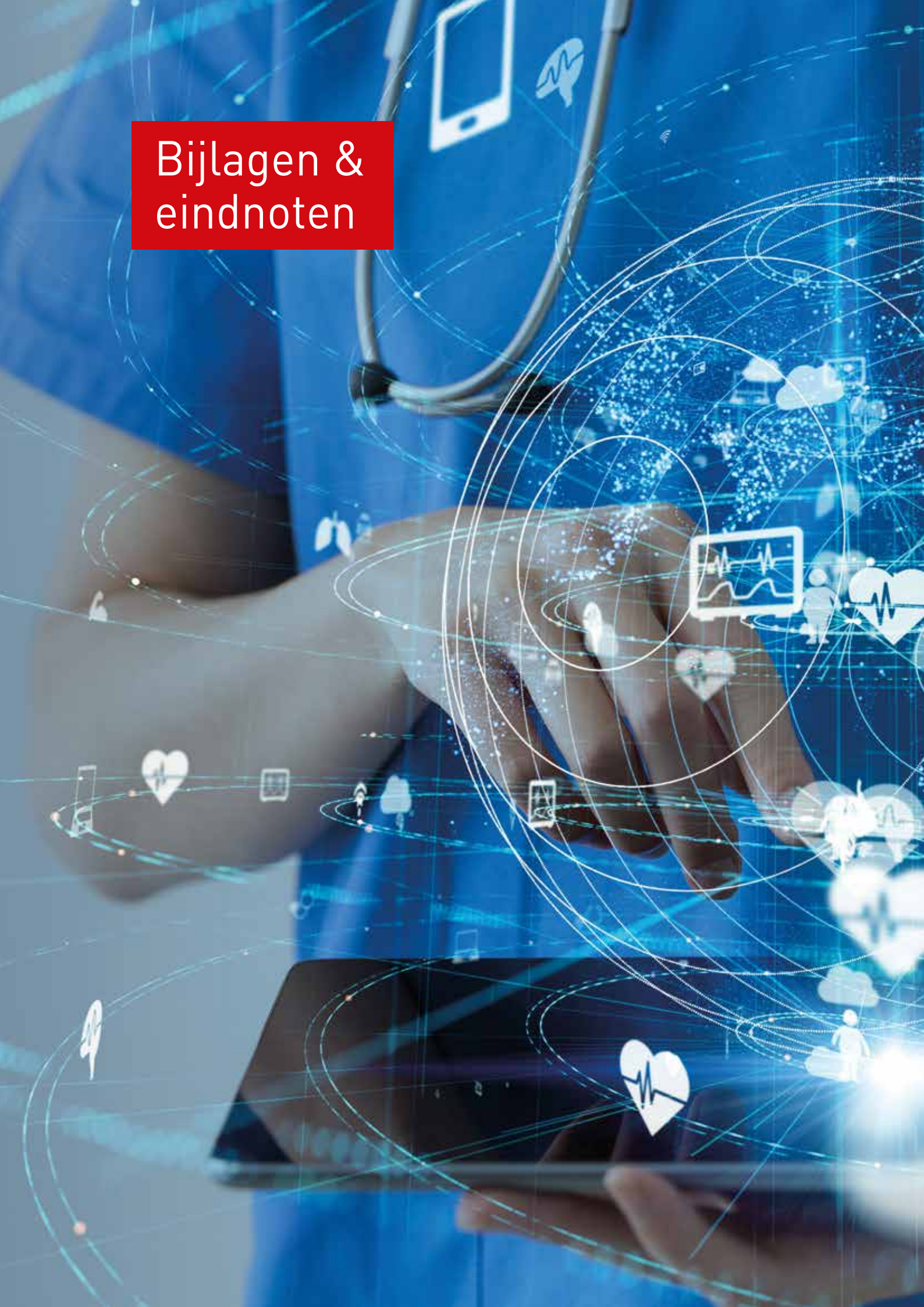
Op verschillende plaatsen in de tekst is het belang van een goede samenwerking met andere initiatieven (zie ook Bijlage 2) benadrukt. Ook een goede betrokkenheid van de overheden en de juiste technische ondersteuning zijn nodig. Vandaar stelt Zorgnet-Icuro voor om de stakeholders die betrokken zijn bij de reeds lopende of opstartende initiatieven op structurele basis samen te brengen. Enkel op deze manier kan de compatibiliteit tussen de verschillende initiatieven worden verzekerd en de juiste technische en andere keuzes gemaakt.

De Vlaamse overheid heeft tijdens de vorige legislatuur reeds een overlegstructuur ingericht rond gegevensdeling, namelijk het Vlaams Agentschap voor de Samenwerking rond Gegevensdeling tussen de Actoren in de Zorg (VASGAZ), waar voorliggend concept reeds is toegelicht en besproken. Gezien VASGAZ aanleiding kan geven tot beleidsmatige verankering van een aantal werkingsprincipes is het gepast het voorgestelde overleg binnen VASGAZ te organiseren, bijvoorbeeld onder de vorm van een overlegcomité. Op die manier is het niet enkel mogelijk om een aantal conclusies van het overleg te verankeren in regelgeving, maar ook de betrokkenheid van de Vlaamse en federale overheid te verzekeren.

Hoewel niet vertegenwoordigd in de raad van bestuur van VASGAZ maken de Strategische Onderzoekscentra of SOCs, imec en vito ook best deel uit van dit overleg. Zij zijn beide actief in de gezondheidszorg en kunnen in de uitwerking van de verschillende initiatieven evenals in de ondersteuning bij het overleg een actieve rol opnemen.

We merken hierbij ook op dat in het regeerakkoord 2020-2024 werd opgenomen dat de werking van VASGAZ zou worden geëvalueerd en waar nodig bijgestuurd. Bovenstaande is dus onder voorbehoud van dergelijke bijsturing. Het belangrijkste is echter het structurele karakter van het overleg en de betrokkenheid van de SOCs.

Bijlagen & eindnoten



Bijlage 1: Deelnemers stakeholderoverleg

Zoals toegelicht in hoofdstuk 1 (§1.7.) kwam het voorliggend conceptvoorstel tot stand via een maatschappijbreed consultatieproces. Een van de stappen was een uitgebreid en diepgaand stakeholderoverleg. Op 20 juni 2019 organiseerde Zorgnet-Icuro een bijeenkomst waarbij alle stakeholders de gelegenheid kregen om hun feedback te geven op het conceptvoorstel en de respectieve randvoorwaarden. Tijdens dat overleg werd er voldoende ruimte geboden voor iedere stem. De volgende personen namen deel aan het stakeholderoverleg:

Naam	**Organisatie**
Bart Demoor	KU Leuven
Johan Decruyenaere	UZ Gent
Tom Coolen	UZ Brussel
Ilse Weeghmans	Vlaams Patiëntenplatform
Bart Vannieuwenhuyse	Johnson & Johnson
Jo De Cock	RIZIV
Dirk Dewolf	Zorg en Gezondheid
An Vijverman	Dewallens & partners
Bart Vandenbosch	UZ Leuven
Johan Van Bussel	Healthdata
Michael Callens	CM
Marc Moens	BVAS
Vincent Dupont	PatiëntHealthViewer
Tom Fiers	UZ Gent/COZO
Erwin Bellon	Hub UZ Leuven
Christine De Bray	Abrumet
Marijn Geeroms	AZ Halle
Rudy Poedts	AZ Heusden-Zolder
Dominique Dejonckeere	Zorg en Gezondheid
Dirk Broeckx	éénlijn.be
Leo Geudens	Domus Medica
Georgres De Moor	UGent
Mahsa Shabani	KU Leuven
Stefaan Callens	KU Leuven
Carole Absil	Agoria
Pieter Vanherck	VOKA
Carine Boonen	Flanders' Care
Kathleen D'Hondt	Departement EWI
Tom Balthazar	Zorgnet-Icuro/UGent
Yvonne Denier	Zorgnet-Icuro/KU Leuven
Peter Raeymaekers	Zorgnet-Icuro
Margot Cloet	Zorgnet-Icuro

Bijlage 2: Gekende big-data-initiatieven

BELGIË
Onderstaande zijn de ons momenteel gekende big-data-initiatieven in België. Bij elke volgende stap in de verdere realisatie zal met hen contact moeten worden genomen om te kijken waar de praktische en andere raakvlakken zich situeren.

Data for better health

Het initiatief '#dataforbetterhealth' heeft tot doel de bestaande belemmeringen voor een FAIR-databeleid in de volksgezondheid in kaart te brengen en oplossingen voor deze belemmeringen te formuleren, te testen en uit te voeren om te komen tot een geïntegreerd datatoegangsbeleid. Deze oplossingen moeten technisch, semantisch, economisch en juridisch duurzaam zijn. Daarnaast moet een breed gedragen governance model worden uitgewerkt.

Verwacht mag worden dat een geïntegreerd beleid inzake gegevenstoegang zal leiden tot een betere ondersteuning van wetenschappelijk onderzoek, een effectievere ontwikkeling van geneesmiddelen en medische hulpmiddelen, een betere patiëntenzorg, een verbetering en ondersteuning van klinische proeven, ondersteuning van gepersonaliseerde zorg, ondersteuning van preventie, patiëntgeoriënteerde zorg, en lagere medische kosten...

Het initiatief '#dataforbetterhealth' wil alle dienstverleners en kennisinstellingen die actief zijn op het gebied van gezondheidszorg (waaronder geneesmiddelenontwikkeling, ontwikkeling van medische hulpmiddelen, ...), gezondheidseconomie, informatiemanagement, privacy en veiligheid, wetgeving (hogescholen, ...) stimuleren en betrekken. ..., zowel publieke als private organisaties, profit als non-profit (data science communities, open data communities, open knowledge communities, ...) organisaties.

#dataforbetterhealth is een INITIATIEF van de federale minister voor Volksgezondheid, de federale minister voor Digitale Agenda, en de federale Staatsecretaris voor Privacy, GESTEUND door Sciensano, NIDO – the innovation lab of the federal government en DigitYzer, en GEÏNSPIREERD door RIZIV-INAMI, FOD-SPF Public Health, FAGG-AFMPS, IMA-AIM, IMEC, AGORIA, PHARMA.BE, VPP, LUSS, HOSPITALS.be, KCE, BOSA, ...

Healthdata.be

Healthdata.be, ontwikkeld door Sciensano (voorheen het WIV) en gefinancierd door het RIZIV, biedt nieuwe perspectieven inzake e-Health door de vereenvoudiging van de registratie en de bewaring van de gezondheidsgegevens die verschillende zorgverleners toesturen. Healthdata.be zorgt op termijn voor betere kwaliteit van het gezondheidsonderzoek.

Door het verenigen van krachten in het kader van een nieuw inventarisatieproject zijn het KCE en Sciensano erin geslaagd om een lijst aan te leggen met meer dan 150 databanken met gezondheidsgegevens. De inventaris kan op de website Healthstat.be worden geraadpleegd en geeft een beschrijving van elke databank, haar voornaamste doelstellingen, de betrokken medische specialiteiten, het soort informatie die zij bevat (bijvoorbeeld facturatiegegevens of klinische gegevens) en de manier waarop alle informatie is verzameld.

Data Intermutualistisch Agentschap (IMA)

In België zijn 7 ziekenfondsen actief. Zij verzamelen heel wat gegevens om hun opdrachten uit te voeren:

- Demografische en socio-economische gegevens van de leden: geslacht, leeftijd, ...

- Facturatiegegevens van de leden: telkens als een lid recht heeft op een terugbetaling voor gezondheidszorgen verwerkt en verzamelt het ziekenfonds gegevens: zoals de datum, de plaats en de kost van de verstrekking…

Het InterMutualistisch Agentschap (IMA) verzamelt al deze data voor specifieke studies in verband met de gezondheidszorgen in België. De data waarover het InterMutualistisch Agentschap beschikt kunnen opgesplitst worden in 3 soorten gegevens:
- Populatie
- Gezondheidszorgen
- Farmanet

Het verzamelen van deze data en uitvoeren van studies heeft als doelstelling het ondersteunen van:
- Het beleid van de gezondheidszorgen in België;
- De onderhandelingen tussen de ziekenfondsen en de zorgverstrekkers;
- Gemeenschappelijke intermutualistische initiatieven.

De data van het InterMutualistisch Agentschap kunnen bovendien aangevuld worden met data van andere instanties, namelijk:
- Minimale Ziekenhuisgegevens
- Data van het kankerregister
- Enquêtegegevens
- Fiscale gegevens

Institute of Analytics for Health (INAH)

Het INAH moet het portaal worden voor de verwerking van klinische gegevens voor onderzoek in Wallonië. Het wordt uitgebouwd in de schoot van het Réseau Santé Wallon. De doelstelling is tweeledig: het ontwikkelen van nieuwe en innoverende therapeutische oplossingen enerzijds en het versterken van de medische preventie anderzijds. Men ontving hiervoor een steun van 1.2 mio euro van de Franse gemeenschap. Het initiatief kadert in de Digital Wallonië strategie.

Meer info: https://www.digitalwallonia.be/fr/publications/inah

Koninklijke Vlaamse Academie van België

We verwijzen hier naar het KVAB Standpunt 48, uitgegeven in 2017[1], dat de rol van de datawetenschappen in de gezondheidszorg omschrijft als drieledig (triple AIM): (1) een toename van de ervaring, kwaliteit en beleving van de patiënt, (2) een betere volksgezondheid en (3) een kostendaling.

Verder formuleren zij een aantal aanbevelingen voor alle stakeholders in het ecosysteem en doen zij een oproep aan het beleid om de ontwikkeling in datastandaarden, nieuwe big-data-technologieën en gezondheidszorgaanbevelingen (als resultaat van datawetenschappen) op te volgen en open te staan voor nieuwe ontwikkelingen.

VITO health data initiatief

VITO is in gesprek met de Zwitserse overheid over de uitbreiding van een Zwitsers initiatief naar andere Europese landen waaronder Nederland (Leiden), UK (Oxford) en Duitsland (Berlijn).

De basisgedachte is om burgers eigenaar te maken van hun digitale data en dit op één (nationaal) platform. De term digitale data wordt dan breed ingevuld (medisch dossier, eigendomstitels, energiekosten en -data, sociale informatie (wonen/werken), paswoorden,

bankrekeningen, voorkeuren, ...). Hij kiest zelf of hij deze wenst te delen of niet. Zo kan een medisch dossier en medische of sociale informatie gedeeld worden om toe te laten dat onderzoeken over duurzame gezondheidszorg en preventie gestoffeerd kunnen worden.

Het idee is dat thans vooral grote, Amerikaanse bedrijven (Google, Facebook, Amazon, ...) eigenaar zijn van deze data. Het gaat dan bv. om medische gegevens omdat ze weten welke medicatie iemand online bestelt of naar welke ziektebeelden iemand zoekt op google. Deze kennis wordt evenwel niet of onvoldoende gebruikt en zeker niet met instemming van de betrokkene.

Het voorgestelde platform zou gerichter en onder regie van de burgers zelf gegevensontsluiting kunnen sturen. Om vertrouwen te wekken bij de burger is het wenselijk dat het initiatief gedragen wordt door een neutrale speler (de overheid?). In Zwitserland is daarvoor een geëigend forum opgericht waar elke Zwitser 'aandeelhouder' van is. De mogelijkheden van een dergelijk dataplatform naar verdere kennisopbouw zowel geïndividualiseerd als collectief is zeer groot omdat het over authentieke data gaat – het echte medische dossier – en geen afgeleide informatie. (Het online koopgedrag van medicatie kan net zo goed kan slaan op medicatie voor de ouders of de buren).

Het initiatief dat VITO nu wenst te nemen kadert in hun onderzoeksprogramma 'duurzame gezondheid' waar ze milieu, levensstijl en fenotypische (omics-)data met elkaar willen verbinden om te zoeken naar verbanden en oorzaken van ziekte. Dit maakt onder meer een betere preventie mogelijk, ook gepersonaliseerd. Ze wensen deze data ook verder uit te bouwen met verschillende onderzoeks- en bedrijfspartners en hebben daartoe een betrouwbaar databeheer en data-analyse instrument nodig. Het datamanagement systeem dat ze willen voorstellen gaat daar heel ver in, en vormt uiteindelijk een coöperatieve structuur (waar VITO kan aan deelnemen, maar zonder winstbelang).

POM WestVlaanderen

Het EFRO project Health Impact (EFRO-P1320) werd ingediend in het raam van de GTI West Vlaanderen binnen het EFRO-Vlaanderen programma. Partners zijn de POM West Vlaanderen (coördinator), HoWest (kennispartner), Wit Gele Kruis West Vlaanderen (eerstelijnszorgpartner) en het Jan Ypermanziekenhuis (tweedelijnszorgpartner, mede namens alle ziekenhuizen in West Vlaanderen).

Door de ontwikkeling van een zorgdataplatform wil het projectconsortium een belangrijke stap zetten in het meten van de reële impact van producten of diensten in de zorgketen op de gezondheid van de personen met een zorgnood. Het onderbouwd aantonen van deze impact, niet enkel in een lab-omgeving maar ook in het dagelijks leven, zou dan marktintroductie kunnen versnellen en opschaling mogelijk maken, zowel Vlaams als internationaal.

Enerzijds zou dergelijk systeem de zorgsector dus toelaten om de meest efficiënte producten of diensten binnen te halen, met een lagere maatschappelijke kost tot gevolg. Anderzijds zou het toeleveranciers helpen hun producten en diensten beter af te stemmen op de noden van de zorgsector.

Om (medische en niet-medische) zorgdata op een verantwoorde en veilige manier te delen met de gebruikers is een passende technologische oplossing vereist. Concreet wordt binnen het consortium op basis van blockchaintechnologie een dataplatform ontwikkeld dat toelaat de impact van innovatieve producten en diensten te meten en te objectiveren.

BUITENLAND

In volgend overzicht zijn een aantal buitenlandse big data initiatieven opgelijst waarin zorgverstrekkers een trekkersrol spelen en waar het gaat om hergebruik van klinische gegevens. Het is zeker geen exhaustieve lijst, maar moet toch al een idee geven over hetgeen internationaal reeds lopende is.

Arsenal.it (Italië)

Italiaans consortium van zorgverstrekkers en lokale overheden. Men combineert een systeem voor gegevensuitwisseling met een big data platform.
https://www.promisalute.it/upload/mattone/documentiallegati/G.Pellizzon_Mobilizing-healthcareforyou...WithBigData_13660_3284.pdf

NIHR Health Informatics Collaborative (VK)

Collectief van NHS Trusts dat klinische, wetenschappelijke en ICT competentie combineert voor (voornamelijk biomedisch) onderzoek. Daarvoor maakt men afspraken rond data specificatie en beschikt men over een governance model voor het beheer van het systeem voor delen en hergebruik van gegevens.
https://hic.nihr.ac.uk/

SNIIRAM (Frankrijk)

Bevat alle terugbetalingsdata verzameld door de Franse nationale zorgverzekering en toegankelijk voor maatschappelijk relevant onderzoek.
https://www.ameli.fr/l-assurance-maladie/statistiques-et-publications/sniiram/finalites-du-sniiram.php

SCI-DC (Schotland)

Scottish Care Information – Diabetes Collaboration. Centraal patiëntendossier ivm diabetes real-time real-world data. Ook secundair gebruik van de data is mogelijk voor bepaling van behandelkost of voor de bepaling van de strategie ivm de klinische dienstverlening.
AEGLE

BigMedilytics (Europees)

Europees project gericht op het aanreiken van een blauwdruk voor big data systemen en het beheer ervan.
https://www.bigmedilytics.eu/big-data-project/

IMI-EMIF (Europees)

Publiek-privaat initiatief met 57 partners op Europees niveau. Liep 5.5 jaar tot juni 2018. Het doel van EMIF was het verbeteren van de toegang tot medische data voor (her)gebruik.
http://www.emif.eu/

C3 Cloud (Europees)

Is een Europees project dat gegevens samenbrengt van verschillende zorgverstrekkers voor zorgplanning en dit met focus op multi-morbiditeit en poly-pharmacie. Geen zuiver big data project maar illustreert hoe men gegevens van verschillende partijen op één platform kan samenbrengen.

ARNO Observatorium (Italië)

Combineert de administratieve gegevens van een grote variëteit aan stakeholders voor onder meer collectief onderzoek. De resultaten worden gebruikt voor het monitoren van systeemperformantie, kosten etc.
https://www.cineca.it/en/projects/osservatorio-arno

Dit laatste initiatief is ook terug te vinden in onderstaand rapport besteld door de Europese Commissie:
"Study on Big Data in Public Health, Telemedicine and Healthcare" (dec 2016)
https://ec.europa.eu/health/sites/health/files/ehealth/docs/bigdata_report_en.pdf
In dit rapport zijn nog andere initiatieven terug te vinden, doch deze zijn veelal op klinisch onderzoek gericht of zijn gebaseerd op een uniform patiëntendossier.

Ook de OESO publiceerde een rapport over big data:
"Big data: A new dawn for public health?"
https://www.oecd-ilibrary.org/sites/e3b23f8e-en/1/2/5/index.html?itemId=/content/publication/e3b23f8e-en&mimeType=text/html&_csp_=c23ceb96c5ce2feb951a759a657e4b9f&itemIGO=oecd&itemContentType=book

Initiatieven waar zorgverstrekkers niet rechtstreeks bij betrokken zijn, maar toch het vermelden waard:

'All of us'

https://allofus.nih.gov/

Big data Value Association

http://www.bdva.eu/about

Bijlage 3: Bundeling reviewcommentaren stakeholders

Voorliggende ontwerptekst werd in de periode september-oktober 2019 voorgelegd aan alle stakeholders voor review en feedback. Hierop werd actief en constructief gereageerd door meer dan 200 personen en organisaties. De tekst werd onderworpen aan een uitgebreid scala aan perspectieven. Daar waar mogelijk werd de tekst aangepast op basis van de bedenkingen en suggesties. Aangezien de feedback op verschillende punten diametraal stond, was het niet altijd mogelijk om het in de tekst te integreren. Wel hebben we alle reacties verzameld en samenvattend gebundeld. U kan ze hier terugvinden. Op die manier kunnen ze het voortgaande debat mee blijven stofferen.

Toelichting

Een initiële versie van voorliggend document werd naar een groot aantal partijen verzonden met de vraag hun opmerkingen erop te formuleren. Zo werden onder meer de deelnemers aan het stakeholderoverleg van 21/6 voor een tweede maal geconsulteerd. Daarnaast werd de nota ook bezorgd aan de algemene directies van de ziekenhuizen, aan de leden van de werkgroep ICT van de ziekenhuizen, aan koepelorganisaties van ondernemingen, enzoverder.

Het inhoudelijke resultaat van deze bevraging is terug te vinden in onderstaand overzicht dat werd opgedeeld volgens de verschillende luiken van de basistekst. Algemeen gesproken kan men stellen dat de reacties op het initiatief en de gekozen benadering positief zijn en uitnodigen tot het verder exploreren van mogelijkheden voor samenwerking binnen de groep van stakeholders. De basistekst is echter geen gezamenlijk werk van de stakeholders en kan dus ook niet beschouwd worden als de grootste gemene deler van de visies die er ter zake bestaan. Voorliggend conceptvoorstel kan derhalve ook niet worden beschouwd als een consensustekst.

Om te vermijden dat individuele toestemming zou moeten worden verleend door alle stakeholders om hun commentaren te publiceren, werden deze niet integraal overgenomen, maar gereduceerd en beknopt weergegeven. Verdere toelichting is steeds te bekomen bij de auteurs waarna gerichte contactname met de betrokken stakeholders mogelijk is. Verder werden een aantal punctuele opmerkingen in dit overzicht niet opgenomen omdat zij werden aangepast in de tekst of omwille van de leesbaarheid van dit overzicht.

Zoals de basistekst een interpretatie is van Zorgnet-Icuro en niet kan worden beschouwd als de visie van alle stakeholders, zo kunnen ook de opmerkingen op de basistekst niet worden beschouwd als opmerkingen of standpunten van Zorgnet-Icuro.

Verdere uitwerking

Het gaat in deze om een conceptvoorstel, wat natuurlijk nog veel ruimte laat voor verdere concretisering. Daarom hebben vele stakeholders nog vragen over het verdere praktische verloop en wenst men bij een aantal onderdelen nog verdere verduidelijking. Een dergelijke verduidelijking kan er echter pas komen van zodra er een meer concrete definitie bestaat van het vervolgtraject.

Algemene opmerkingen op de ontwerptekst

- Als men het onderzoeksplatform openstelt voor commerciële partijen met commerciële belangen, moet men over de maatschappelijke verantwoording waken.
- Meerwaarde is afhankelijk van de datakwaliteit. Dit is nog eens een aanleiding om te pleiten voor de evolutie naar een uniform patiëntendossier voor alle zorgverstrekkers.

- Een controle door de overheid op basis van de gegevens moet kunnen volgens de mutualiteiten.
- Het bestaande systeem voor gegevensdeling (vitalink, hubs, …) wordt als volledig functionerend voorgesteld, maar er zijn nog heel veel aandachtspunten en hier loopt alles zeker niet perfect.
- Er mag ook aandacht zijn voor de welzijnsactoren.
- Administratieve gegevens en kost-gegevens kunnen ook relevant zijn en mogelijks ook met de whereabouts worden gecombineerd.
- Potentieel zeer groot project, de technische en economische haalbaarheid moet zorgvuldig worden bekeken.
- Verschillende overheden betrekken en verder kijken dan Vlaanderen.
- Waar onderscheidt dit initiatief zich tot de bestaande big-data-initiatieven? Antwoord: het traject van de patiënt wordt in rekening gebracht en het klinisch traject geeft extra klinische informatie.
- Het initiatief moet zelfrecruterend zijn.
- De datakwaliteit moet in de eerste plaats een klinisch voordeel hebben, dan kan je pas nadenken over secundair gebruik.
- Business model: wie zal de initiële investeringen dragen? Volgens sommigen moet dit de overheid zijn.
- Het is een ambitieus voorstel waarvoor we top-experten zullen moeten vinden.
- De zware projectaanpak kan een nadeel zijn.
- Je kan het initiatief best kleinschalig starten.
- De industrie moet van bij het begin betrokken zijn en ambitieniveau moet ab initio voldoende hoog zijn.
- Dat wil ook zeggen dat zij in de initiële governance structuur moeten worden opgenomen.
- Zoveel mogelijk toekomstgericht denken, dat wil zeggen rekening houden met internationale standaarden en dergelijke.
- Hoe wordt de rol van de universiteiten en kennisinstellingen/SOCs gezien in de verdere uitwerking van het voorstel?
- Belang van betrokkenheid psychiatrische ziekenhuizen.
- Doelstelling is momenteel nog te breed geformuleerd.
- Grote parallellen met iCaredata.
- Wat is de rol van VASGAZ in deze?
- De patiënt of burger als informatiebron niet vergeten.
- Preventie zou meer aan bod moeten komen.
- De kwaliteit van de data uit de eerstelijn moet niet overschat worden.
- Belang van longitudinale opvolging is groot voor de eerstelijn.
- Niet enkel de farmacie vermelden als mogelijke industriële gebruikers, maar ook de medische hulpmiddelen.
- De data zou controle door de mutualiteiten verder moeten ondersteunen.
- Belang van real-time data voor tijdige medische en niet-medische interventie is groot.
- Betrokkenheid van de farma-industrie is risicovol en mogelijks zelfs problematisch.
- Opstart van het initiatief moet met publieke middelen gebeuren.
- Replicatie-onderzoek zou moeten mogelijk zijn door het beschikbaar houden van de data.
- Idealiter is Healthdata TTP voor dit initiatief.
- Samenwerking met andere initiatieven is zeer belangrijk.

Technische opmerkingen

- Als men voor volledige anonimisering zou gaan, is het onderzoekspotentieel van de data dan nog voldoende hoog?
- De inspanningen van de leveranciers zijn niet noodzakelijk klein, zeker niet als de ambities worden opgeschroefd.

- Wat codering betreft staan we nog niet ver, voorbeelden die worden aangehaald zoals SAM en SNOMED zijn voorbeelden waarbij er nog een lange weg moet worden afgelegd.
- Er kunnen geen extra zaken verwacht worden van de hubs gezien zij momenteel niet gefinancierd worden voor hun basiswerking.
- De benamingen van de plaatsen in de ziekenhuizen is niet uniform, wat dus een hinderpaal vormt in de uitrol. Een suggestie is de whereabouts voor de facturatie te nemen, maar dan verlies je veel klinisch relevante verplaatsingen.
- Het idee om van de whereabouts te vertrekken is goed, maar men mag het ook niet onderschatten.
- De huisarstenpakketten en apotheekpakketten zullen ook whereabouts moeten doorgeven, wat extra programmatie zal vergen.
- De hubs zijn geen systeem van de overheid maar worden door de zorgverstrekkers uitgebaat.
- Het real-time doorgeven van de whereabouts gaat tot een groot transactievolume leiden, dus eerder denken om deze in batch door te geven.
- Er is zeker ook een inspanning nodig aan de kant van de zorgverstrekker, gezien de gewenste info zal moeten worden gemapt.
- Het verbinden van klinische gegevens aan de connector zal inspanningen vergen aan de kant van de zorgverstrekkers en is mogelijks moeilijk te realiseren.
- XDW zal een te grote transactie load met zich meebrengen.
- Hoe sluit dit aan bij het TriNetX initiatief?
- Kan Blockchain technologie hier een meerwaarde betekenen?
- Kans voor invoering van clinical building blocks.
- Hub platform ook migreren naar dit concept.
- Reeds XDW geïmplementeerd met 8 clinical building blocks in het zuiden van Nederland.
- Voor veel inzichten volstaat het om te werken met geaggregeerde data.
- MA Atlas biedt reeds een belangrijke bron van data aan.

Opmerkingen mbt privacy

- Risico voor heridentificatie: het woord anonimisering is soms onterecht gebruikt.
- Privacy is maximaal te waarborgen bij gebrek aan geïnformeerde toestemming.
- Bij verdere concretisering vraagt men best het oordeel van de gegevens-beschermingsautoriteit of het informatieveiligheidscomité.
- We moeten ten zeerste op onze hoede zijn voor het combineren met andere data om big brother toestanden te vermijden.
- Best het Center for Cyber Security betrekken.

Juridische opmerkingen

- Aansluiting met de regelgeving moet nog beter.
- Juridische drempels op te lijsten.
- Artsen en ziekenhuizen zijn doorgaans geen gezamenlijke verwerkingsverantwoordelijken.

Opmerkingen mbt ethiek

- Ethisch comité is noodzakelijk.
- Betrokkenheid van de burger is hierin cruciaal.
- Ook transparantie ivm het platform is zeer belangrijk.
- Oorspronkelijk doel van het platform gaat terug naar de behandeling, zeker met inzet van AI.
- Waarom voorziet men geen opt-out?
- Parallel met en gebruik maken van bestaande Data Access Committees (DACs).
- Controlemogelijkheden van de patiënt toevoegen, bv myhealthmydata.eu.
- Er is een verschil tussen onderzoeksgegevens overdragen en toegang krijgen tot onderzoeksgegevens.

- Een vast comité van experten voor beoordeling van de dossiers is te vermijden, wel iets voor te zeggen op ethisch vlak.
- Noodzaak om belangenconflicten te vermijden en het misbruik door een dominante positie vermijden.
- Waken over de maatschappelijke meerwaarde bij het gebruik van de gegevens.
- Maximale consent van de patiënt is nodig.
- Mutualiteiten beschermen ook de patiënt en komen op voor de privacy van de patiënt.
- Transparante governance is noodzakelijk.
- De TTP mag geen enkele band hebben met commerciële partijen.
- Best aantal onderzoeksdomeinen uitsluiten die al te gevoelig kunnen liggen zoals fertiliteit, psychische aandoeningen, etc.

Eindnoten

1 Zie: https://www.nictiz.nl/wp-content/uploads/2018/03/Handreiking_interoperabiliteit_tussen_XDS_Affinity_Domains_2015.pdf

2 Zie: https://www.ehealth.fgov.be/standards/kmehr/en/transactions/summarised-electronic-healthcare-record-v20.

3 De AVG is voluit: de Verordening 2016/679 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van de gegevens en tot intrekking van richtlijn 95/46/EG.

4 De Kaderwet is voluit: de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

5 De eHealth-wet is voluit: de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen.

6 Decreet van 25 april 2014 betreffende de organisatie van het netwerk voor de gegevensdeling tussen de actoren in de zorg.

7 Kwaliteitswet is voluit: de wet van 22 april 2019 inzake de kwaliteitsvolle praktijkvoering in de gezondheidszorg.

8 Wet van 22 augustus 2002 betreffende de rechten van de patiënt.

9 *Parl.* St. 54, 3685/002.

10 Overweging 33: 'Het is vaak niet mogelijk op het ogenblik waarop de persoonsgegevens worden verzameld, het doel van de gegevensverwerking voor wetenschappelijke onderzoeksdoeleinden volledig te omschrijven. Daarom moet de betrokkenen worden toegestaan hun toestemming te geven voor bepaalde terreinen van het wetenschappelijk onderzoek waarbij erkende ethische normen voor wetenschappelijk onderzoek in acht worden genomen. Betrokkenen moeten de gelegenheid krijgen om hun toestemming alleen te geven voor bepaalde onderzoeksterreinen of onderdelen van onderzoeksprojecten, voor zover het voorgenomen doel zulks toelaat'.

11 Overweging 50: 'De verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel worden toegestaan indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld. In dat geval is er geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de verzameling van persoonsgegevens werd toegestaan. Indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, kan in het Unierecht of het lidstatelijke recht worden vastgesteld en gespecificeerd voor welke taken en doeleinden de verdere verwerking als rechtmatig en verenigbaar met de aanvankelijke doeleinden moet worden beschouwd. De verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, moet als een met de aanvankelijke doeleinden verenigbare rechtmatige verwerking worden beschouwd. De Unierechtelijke of lidstaatrechtelijke bepaling die als rechtsgrond voor de verwerking van persoonsgegevens dient, kan ook als rechtsgrond voor verdere verwerking dienen. Om na te gaan of een doel van verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, moet de verwerkingsverantwoordelijke, nadat hij aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking heeft voldaan, onder meer rekening houden met: een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking; het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan; de aard van de persoonsgegevens; de gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; en passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen'.

12 Overweging 156: 'De verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, dient onderworpen te zijn aan passende waarborgen voor de rechten en vrijheden van de betrokkenen overeenkomstig deze verordening. Die waarborgen dienen ervoor te zorgen dat technische en organisatorische maatregelen worden getroffen om met name de inachtneming van het beginsel gegevensminimalisering te verzekeren. De verdere verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek, of statistische doeleinden dient te worden uitgevoerd wanneer de verwerkingsverantwoordelijke heeft beoordeeld of deze doeleinden te verwezenlijken zijn door persoonsgegevens te verwerken op basis waarvan de betrokkenen niet of niet meer geïdentificeerd kunnen worden, op voorwaarde dat passende waarborgen bestaan, zoals de pseudonimisering van de persoonsgegevens. De lidstaten dienen passende waarborgen te bieden voor de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. De lidstaten dienen te worden gemachtigd om, onder specifieke voorwaarden en met passende waarborgen voor de betrokkenen, nader te bepalen welke specificaties en afwijkingen gelden voor de informatievoorschriften, en te voorzien in het recht op rectificatie, het recht op wissing, het recht op vergetelheid, het recht op beperking van de verwerking en het recht van gegevensoverdraagbaarheid en het recht van bezwaar tegen verwerking van persoonsgegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Indien dit tegen de achtergrond van de met de specifieke verwerking beoogde doeleinden passend

is, kunnen in de genoemde voorwaarden en waarborgen specifieke procedures voor de uitoefening van deze rechten door betrokkenen worden opgenomen, in combinatie met technische en organisatorische maatregelen om, in het licht van de evenredigheids- en noodzaakbeginselen, het verwerken van persoonsgegevens tot een minimum te beperken. De verwerking van persoonsgegevens voor wetenschappelijke doeleinden dient ook te voldoen aan andere toepasselijke wetgeving, zoals die over klinische proeven'.

13 Overweging 157: 'Door gegevens uit verschillende registers te koppelen, kunnen onderzoekers nieuwe en zeer waardevolle kennis verwerven over veel voorkomende medische aandoeningen zoals hart- en vaatziekten, kanker en depressie. Omdat zij op een groter deel van de bevolking zijn gebaseerd, kunnen onderzoeksresultaten met behulp van registers worden verbeterd. In de sociale wetenschappen kunnen wetenschappers dankzij registeronderzoek essentiële kennis verwerven over de wisselwerking op lange termijn van een aantal sociale factoren, zoals werkloosheid en onderwijs met andere levensomstandigheden. Onderzoeksresultaten die door middel van registers worden verkregen, leveren solide kennis van hoge kwaliteit op, die kan worden gebruikt om een op kennis gebaseerd beleid te ontwikkelen en te implementeren, de levenskwaliteit van een deel van de bevolking te verbeteren, en sociale diensten efficiënter te maken. Daarom moet, teneinde wetenschappelijk onderzoek te faciliteren, worden bepaald dat persoonsgegevens, met inachtneming van de passende voorwaarden en waarborgen die in het Unierecht of het lidstatelijke recht zijn vastgesteld, met het oog op wetenschappelijk onderzoek mogen worden verwerkt'.

14 Deze mogelijke grondslag is wel onderworpen aan belangrijke beperkende voorwaarden. Art. 1.f AVG luidt voluit: 'de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is'.

15 Zie vraag 42 ('Identificatie van de rechtsmatigheidsgronden') in T. BALTHAZAR en P. RAEYMAEKERS, Gegevensbescherming in de zorg, Brugge, Die Keure, 2018, p. 81.

16 Art. 6 Wet van 7 mei 2004 inzake experimenten op de menselijke persoon.

17 Verordening 536/2014 over klinische proeven voor geneesmiddelen voor menselijk gebruik ('CTR-regulation').

18 Zie V. CHICO, "The impact of the General Data Protection Regulation on health research", *British Medical Bulletin*, 2018, 128: 109-118; J. RUMBOLD en B. PIERSCIONEK, "The effect of the General Data Protection Regulation on Medical Research", *J. Med. Internet Res.* 2017, 19; G. CHASSANG, "The impact of the EU general data protection regulation on scientific research", 2017, 11: 709.

19 A. VIJVERMAN, "Gezondheidsgegevens verwerken voor wetenschappelijk onderzoek: toestemming vereist of niet?", Tijdschrift voor gezondheidsrecht 2019-20, p. 98-101.

20 Art. 21.6 GDPR.

21 Zie de tekst van overweging 33 in voetnoot 10.

22 World Medical Association Declaration on Ethical Considerations regarding Health Databases and Biobanks (2016), http://www.wma.net.

23 International Ethical Guidelines for Health-related Research Involving Humans van de Council for International Organisations of Medical Sciences (CIOMS), http://www.cioms.ch.

24 Zie de toelichting hierover bij M. MOSTERT, "Big data, medisch-wetenschappelijk onderzoek en gegevensbescherming", in Vereniging voor gezondheidsrecht (ed.), *Big data in de zorg*, Den Haag, Sdu Uitgevers, 2017, 177.

25 Commissie voor de bescherming van de persoonlijke levenssfeer, Big Data getoetst aan de Algemene Verordening Gegevensbescherming: enkele aanbevelingen voor goed gebruik, Brussel, Politeia, 2017, p. 101.

26 Pseudonimisering is in art. 4.5. AVG als volgt gedefinieerd: 'Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld'. Zie ook de bijna identieke definitie van het proces van pseudonimisering in art. 26, 5° Kaderwet Bescherming Persoonsgegevens.

27 Binnen de stroom van literatuur signaleren wij een helder, volledig en recent rapport over anonimisering, pseudonimisering en andere 'privacy enhancing techniques' dat de door Ierse Data Protection Commission werd uitgebracht in juni 2019: https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation.

28 Zie AVG-overweging 26.

29 Zie het onderdeel "Het einde van anonimiteit?" bij M. MOSTERT, "Big data, medisch-wetenschappelijk onderzoek en gegevensbescherming", in Vereniging voor gezondheidsrecht (ed.), *Big data in de zorg*, Den Haag, Sdu Uitgevers, 2017, 171.

30 N. SAVAGE, "The myth of anonimity", *Nature* 2016, 537: 70.

31 Zie uitdrukkelijk overweging 26 bij de AVG.

32 Art. 188, 1° en 203 wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. In art. 1881, 1° is de derde vertrouwenspersoon gedefinieerd als

"de natuurlijke persoon of de rechtspersoon, de feitelijke vereniging of de overheidsadministratie, niet zijnde de verantwoordelijke voor de verwerking met het oog op archivering of onderzoek of statistische doeleinden, die de gegevens pseudonimiseert'.

33 Zie art. 4.5. AVG en art. 26, 5° Kaderwet Bescherming Persoonsgegevens.

34 Art. 17.3.2 AVG.

35 Koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

36 Art. 204 Kaderwet Gegevensbescherming.

37 Art. 200 Kaderwet Gegevensbescherming.

38 Zie het tweede deel van overweging 159 bij de AVG: *Om als verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek te worden aangemerkt, moet de verwerking aan specifieke voorwaarden voldoen, met name wat betreft het publiceren of anderszins openbaar maken van persoonsgegevens voor wetenschappelijke onderzoeksdoeleinden. Indien de resultaten van wetenschappelijk onderzoek, met name op het gebied van gezondheid, aanleiding geven tot verdere maatregelen in het belang van de betrokkene, zijn met het oog op deze maatregelen de algemene regels van deze verordening van toepassing.*

39 'Guidelines on consent' WP259 (https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinions-and-documents)

40 M. SHABANI, B. KNOPPERS en P. BORRY, "From the principles of genomic data sharing to the practices of data access committees", *Embo Molecular Medicine* 2015, 1-3.

41 L. SKOVGAARD, S. WADMANN en K. HOEYER, "A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good", *Health Policy*, 2019, 564-571.

42 Ook personeelsleden van een 'verwerker' kunnen als 'bewerker' (onder het gezag van die verwerker) worden beschouwd; Zie een nadere toelichting hierover in de GDPR-gedragscode voor zorgvoorzieningen, nr. 6 (T. BALTHAZAR en P. RAEYMAEKERS, *Gegevensbescherming in de zorg*, Brugge, Die Keure, 2018, p. 39).

43 Art. 137, 12° Ziekenhuiswet.

44 Zie hierboven onder nr. 3.2.

45 Zie www.myhealthmydata.eu.

46 Volgens het Capability Maturity Model. Het model is ontwikkeld aan de Carnegie Mellon University. Zie https://resources.sei.cmu.edu/asset_files/TechnicalReport/1993_005_001_16211.pdf

47 21 AUGUSTUS 2008. — Wet houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen.

48 07 APRIL 2019. — Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

49 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32014R0910&from=NL

50 https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

51 Zie http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm voor een definitie

52 Decreet van 8 juni 2018 houdende de aanpassing van de decreten aan de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming)

53 Kalkman S, Moster M, Gerlinger C, van Delden JJM & van Thiel GJMW (2019). 'Responsible Data Sharing in International Health Research: a Systematic Review of Principles and Norms.' *BMC Medical Ethics* 20:21.

54 Dyke SO & Hubbard TJ (2011). 'Developing and implementing an institute-wide data sharing policy.' *Genome Med BioMed Central* 3:60; The Nuffield Council on Bioethics (2015). *The collection, linking and use of data in biomedical research and health care: ethical issues*; Council for International Organizations of Medical Sciences (CIOMS) (2016). *International Ethical Guidelines for Health-related Research Involving Humans*; OECD (2007). *Principles and Guidelines for Access to Research Data from Public Funding*; OECD (2009). *Recommendation of the Council on Human Biobanks and Genetic Research Databases*; OECD (2017). *Recommendation of the Council on Health Data Governance*; Rodriguez H et al. (2009). 'Recommendations from the 2008 international summit on proteomics data release and sharing policy: the Amsterdam principles.' *J Proteome Res*. 8:3689–92; Funders of public health research (2011). *Joint statement of purpose—vision, principles, and goals*; Auffray et al. (1916). 'Making sense of big data in health research: Towards an EU action plan.' *Genome Med BioMed Central* 8:71; 14; Lea et al. (2016). 'Data Safe Havens and Trust: Toward a Common Understanding of Trusted Research Platforms for Governing Secure and Ethical Health Research.' *JMIR Medical Informatics* 4:e22; Deverka et al. (2017). 'Creating a Data Resource: What Will it Take to Build a Medical Information Commons?' *Genome Med Biomed Central* 9:84.

55 Dove ES, Knoppers BM & Zawati MH (2013). 'An Ethics Safe Harbor for International Genomics Research?' *Genome Med BioMed Central* 5:99; Bredenoord et al. (2015). Data Sharing in Stem Cell Translational Science: Policy Statement by the International Stem Cell Forum Ethics Working Party.' *Regen Med* 10:857–61; Regulatory

and Ethics Working Group, Global Alliance for Genomics & Health R and EW, Sugano S (2014). 'International Code of Conduct for Genomic and Health-Related Data Sharing.' *Hugo J Springer* 8:1; OECD (2009). *Recommendation of the Council on Human Biobanks and Genetic Research Databases*; OECD (2017). *Recommendation of the Council on Health Data Governance; Knoppers* et al. (2011). 'Towards a Data Sharing Code of Conduct for International Genomic Research.' *Genome Med* 3:46; OECD (2007). *Principles and Guidelines for Access to Research Data from Public Funding*; Floridi et al. (2018). 'Key Ethical Challenges in the European Medical Information Framework.' *Minds Mach* 2018:1–17.

56 Baker DB, Kaye J & Terry SF (2016). 'Privacy, Fairness, and Respect for Individuals. eGEMs *(Generating Evid Methods to Improv patient outcomes*).' 4:7; EFPIA, PhRMA (2013). *Principles for Responsible Clinical Trial Data Sharing: Our Commitment to Patients and Researchers*; Global Alliance for Genomics and Health (GA4GH) (2014). *Framework for Responsible Sharing of Genomic and Health-Related Data*. Baker DB, Kaye J & Terry SF. (2016). 'Privacy, Fairness, and Respect for Individuals.' *eGEMs (Generating Evid Methods to Improv patient outcomes)* 4:7; The Nuffield Council on Bioethics (2015). *The collection, linking and use of data in biomedical research and health care: ethical issues*; Council for International Organizations of Medical Sciences (CIOMS) (2016). *International Ethical Guidelines for Health-related Research Involving Humans*. OECD (2007). *Principles and Guidelines for Access to Research Data from Public Funding*. OECD (2009). *Recommendation of the Council on Human Biobanks and Genetic Research Databases.* Chan T et al. (2016). 'UK National Data Guardian for Health and Care's Review of Data Security: Trust, better security and opt-outs.' *J Innov Heal Informatics*. 23:627; OECD (2017). *Recommendation of the Council on Health Data Governance*; Antman et al. (2015). 'Acquisition, analysis, and sharing of data in 2015 and beyond: a survey of the landscape.' *J Am Heart Assoc*. 4:e002810; World Medical Association (WMA) (2016). *Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks*; Mascalzoni et al. (2015). 'International charter of principles for sharing bio-specimens and data.' *Eur J Hum Genet* 23:721–8; World Medical Association (WMA) (2013). *Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects*; Dyke SO, Dove ES & Knoppers BM. (2016). 'Sharing health-related data: a privacy test?' *Genomic Med* 1:16024; Banzi et al. (2014). 'Fostering EMA's transparency policy.' *Eur J Intern Med* 25:681–4; Tucker et al. (2016). 'Protecting patient privacy when sharing patient-level data from clinical trials.' *BMC Med Res Methodol* 16:77; Kostkova et al. (2016). 'Who Owns the Data? Open Data for Healthcare.' *Front public Heal Frontiers* 4:7.

57 Kuehn BM. (2014). 'IOM Outlines Framework for Clinical Data Sharing, Solicits Input.' *JAMA American Medical Association* 311:665; Global Alliance for Genomics and Health (GA4GH) (2014). *Framework for Responsible Sharing of Genomic and Health-Related Data*; Auffray et al (2016). 'Sense of big data in health research: Towards an EU action plan.' *Genome Med BioMed Central* 8:71; Lea et al. (2016). 'Data Safe Havens and Trust: Toward a Common Understanding of Trusted Research Platforms for Governing Secure and Ethical Health Research.' *JMIR Med Informatics* 4:e22. 15; Baker DB, Kaye J & Terry SF (2016). 'Privacy, Fairness, and Respect for Individuals.' *eGEMs (Generating Evid Methods to Improv patient outcomes)* 4:7. The Nuffield Council on Bioethics (2015). *The collection, linking and use of data in biomedical research and health care: ethical issues*; Council for International Organizations of Medical Sciences (CIOMS) (2016). *International Ethical Guidelines for Health-related Research Involving Humans*. OECD (2007). *Principles and Guidelines for Access to Research Data from Public Funding*; OECD (2009). *Recommendation of the Council on Human Biobanks and Genetic Research Databases*; Chan et al. (2016). 'UK National Data Guardian for Health and Care's Review of Data Security: Trust, better security and opt-outs.' *J Innov Heal Informatics* 23:627; OECD (2017). *Recommendation of the Council on Health Data Governance*;. Knoppers BM (2014). 'Framework for responsible sharing of genomic and healthrelated data.' *Hugo J Springer* 8:3; Dove ES, Knoppers BM & Zawati MH (2013). 'An ethics safe harbor for international genomics research?' *Genome Med BioMed Central* 5:99; Antman et al. (2015). 'Acquisition, analysis, and sharing of data in 2015 and beyond: a survey of the landscape.' *J Am Heart Assoc*. 4:e002810; Knoppers et al. (2011). 'Towards a data sharing Code of Conduct for international genomic research.' *Genome Med* 3:46; Deverka et al. (2017). 'Creating a data resource: what will it take to build a medical information commons?' *Genome Med BioMed Central* 9:84; Allen et al. (2014). 'Data governance and data sharing agreements for community-wide health information exchange: lessons from the beacon communities.' *EGEMS (Washington, DC)* 2:1057; Bredenoord et al. (2015). 'Data sharing in stem cell translational science: policy statement by the international stem cell forum ethics working party.' *Regen Med.* 10:857–61; Regulatory and Ethics Working Group, Global Alliance for Genomics & Health R and EW, Sugano S (2014). 'International code of conduct for genomic and health-related data sharing.' *Hugo J Springer* 8:1; World Medical Association (WMA) (2016). *Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks;* Laurie G & Sethi N. (2013). 'Towards Principles-Based Approaches to Governance of Health-related Research using Personal Data.' *Eur J Risk Regul* 4:43–57; Floridi et al. (2018). 'Key ethical challenges in the European medical information framework.' *Minds Mach* 1–17; Tucker et al. (2016). 'Protecting patient privacy when sharing patient-level data from clinical trials.' *BMC Med Res Methodol* 16:77; Kostkova P (2016). 'Who Owns the Data? Open Data for Healthcare.' *Front public Heal Frontiers* 4:7; Prainsack B & Buyx A (2013). 'A solidarity-based approach to the governance of research biobanks.' *Med Law Rev* 21:71–91.

Zorgnet-Icuro
Guimardstraat 1, 1040 Brussel

www.zorgneticuro.be
post@zorgneticuro.be