

Obstakel-Verwijder-Traject

Actieplan Cluster 2 – Spelregels

(Actie)partners:

Health-RI (HRI)	Nederlandse Federatie van Universitair Medisch Centra (NFU)
Ministerie van VWS (VWS)	Samenwerkende Topklinische opleidingsZiekenhuizen (STZ)
Ministerie van OCW (OCW)	Zorgverzekeraars Nederland (ZN)
Ministerie van EZK (EZK)	Vereniging Innovatieve Geneesmiddelen (VIG)
Patiëntenfederatie (PF)	Federatie Medisch Specialisten (FMS)
TNO (TNO)	Maatschappelijk Adviesraad Health-RI (MAR)
Health-RI Knooppunten	Integraal Kankercentrum Nederland (IKNL)
Zorginstituut Nederland (ZiN)	Commissie Regelgeving Onderzoek (COREON)
KWF Kankerbestrijding (KWF)	Rijksinstituut voor Volksgezondheid en Milieu (RIVM)

Probleemanalyse (voor 3 clusters gezamenlijk)

Voor een lerend zorgsysteem is het essentieel dat gegevens over gezondheid en ziekte, incl. gegevens gegenereerd binnen de zorg, (kort gezegd: gezondheidsdata), effectief en efficiënt gebruikt, en op persoonsniveau gekoppeld, kunnen worden voor secundaire doelen. Die secundaire doelen kunnen verdeeld worden in 3 categorieën:

1. Doen we de goede dingen? (Zorgevaluatie & Goed gebruik)
2. Doen we de dingen goed? (Kwaliteitsmanagement & Beleid)
3. Zijn er nieuwe dingen (te ontdekken) die beter zijn dan het bestaande? (Onderzoek & Innovatie)?

De ministeries van VWS, OCW en EZK, en Health-RI, hebben 18 uiteenlopende obstakels beschreven die het efficiënt meervoudig gebruik van gezondheidsdata in de weg staan, en daardoor het ontstaan van een lerend zorgsysteem belemmeren.



Deze obstakels beperken goede zorgevaluatie, kwaliteitsmanagement en onderzoek & innovatie, doordat het potentieel van de data niet wordt benut. Daarnaast leiden de obstakels ertoe dat, in plaats van gebruik te maken van bestaande data, naar alternatieve manieren gezocht wordt om de benodigde data (*de novo*) te genereren. Dit kost onnodig tijd en geld, en doet af aan de kwaliteit. Ook is belangrijk dat het gebrek aan data-gedreven nieuwe kennis risico's met zich meebrengt (zoals bijv. tijdens een pandemie). Het uitblijven van een echt lerend zorgsysteem raakt alle inwoners van Nederland.

NB: Ook het secundair gebruik van materialen en beelden valt binnen de scope. Voor het gemak hanteren we de term 'data' of 'gegevens' en worden daarmee ook beelden en materialen bedoeld.

Beoogde impact (voor 3 clusters gezamenlijk)

Een effectief en efficiënt zelflerend zorgsysteem, waarbinnen gezondheidsdata optimaal gebruikt worden voor evaluatie, kwaliteit, beleid, onderzoek en innovatie ten gunste van burgers, organisaties en professionals (zoals bijv. onderzoekers, beleidsmakers, zorgprofessionals).

Scope Cluster 2

Dit Actieplan beschrijft de stappen die de genoemde Actiepartners zullen nemen om de obstakels t.a.v. de juridische, ethische en maatschappelijke 'spelregels' te verwijderen (Obstakel cluster 2). Op dit moment wordt het gebruik en de koppeling van data beperkt door meerdere obstakels, zoals beschreven in het [obstakel-verwijder-document](#).

Data van dezelfde persoon worden op verschillende locaties en op verschillende tijdstippen gegenereerd. Naast spelregels voor optimaal gebruik is het dus bovendien noodzakelijk dat gegevens over ziekte en gezondheid op persoonsniveau gekoppeld kunnen worden, met bescherming van de privacy.

Probleemanalyse cluster 2

Voor efficiënt en verantwoord gebruik en koppeling van data zijn heldere spelregels nodig, t.a.v. de juridische, ethische en maatschappelijke aspecten. In de huidige situatie ontbreekt dat kader, doordat:

- De spelregels er niet zijn (geen sectorale wet- of regelgeving, geen nationale afstemming/afspraken); of
- De spelregels niet duidelijk zijn; of
- De spelregels in de praktijk niet haalbaar of uitvoerbaar zijn; of
- De spelregels niet overeenkomen met andere (ethische, maatschappelijke) normen, waarden en belangen.

Dit heeft gevolgen:

- Het potentieel van de data wordt te beperkt benut (vanwege handelingsverlegenheid, hoge belasting voor professionals en patiënten/burgers, beperkte respons op zeggenschapsvraag);
- Budget gaat verloren aan wielen opnieuw uitvinden, langdurige procedures, gestapelde toetsing, bijeenbrengen van gefragmenteerde data (link met cluster 3), etc. (budget oorspronkelijk bestemd voor onderzoek & innovatie, zorgevaluatie en kwaliteitsmanagement);
- De kwaliteit van de uitkomsten van het gebruik van de data laat te wensen over, doordat de data niet compleet is, er onwillekeurige selectie (bias) optreedt of de koppeling van data beperkt of inaccuraat is (link met cluster 3).
- Voor zowel professionals als patiënten/burgers is niet transparant wat de spelregels zijn, welke rol ze daarbij spelen en wat er wel/niet met data gebeurt of is gebeurd (link met cluster 1).
- Kennisveiligheid (voorkomen van ongewenste overdracht van kennis en technologie) komt in gevaar.
- Het vertrouwen in het gebruik van data t.b.v. een lerend zorgsysteem staat op de tocht (link met cluster 1).
- Het vernieuwend potentieel van ons zorgsysteem wordt belemmerd, wat leidt tot grotere gezondheidsverschillen en afname van de kwaliteit van de zorg.

Specifieke obstakels

(Gepercipieerde) juridische / ethische / maatschappelijke barrières:

De onduidelijkheden in de huidige wet- en regelgeving zorgen voor terughoudendheid en interpretatieverschillen. Hierdoor ontstaan verschillen in juridische, ethische en/of maatschappelijke afwegingen, het beleid dat daarop gebaseerd is, en de gehanteerde procedures en voorwaarden. Soms worden barrières verondersteld die er niet zijn. Het gaat daarbij om onderwerpen zoals grondslag voor gebruik en uitzonderingen daarop, garanderen van privacy, zeggenschap en inspraak, doelbinding, transparantie, patiëntinformatie.

De terughoudendheid leidt ertoe dat data onterecht niet gebruikt worden. De interpretatieverschillen veroorzaken fragmentatie wat het gebruik van de data beperkt en de kwaliteit van de resultaten negatief beïnvloedt. Het geheel komt daarnaast niet ten goede aan de transparantie richting burgers en patiënten.

Gezondheidsdata kunnen niet veilig en exact gekoppeld worden:

In Nederland ontbreekt een eenduidige methodiek voor koppelen. Hierdoor worden in de praktijk verschillende manieren gehanteerd om data van dezelfde persoon aan elkaar te koppelen. Daarnaast worden ook (verschillende combinaties van) verschillende persoonsgegevens gebruikt om een match te maken. In de meeste gevallen gaat het om een combinatie van verschillende identificerende persoonsgegevens. Doordat de mogelijkheden en de methodiek per instelling verschilt, worden er herhaaldelijk puntoplossingen bedacht om een koppeling te maken. Dit vergt veel tijd en geld. Doordat gewerkt wordt met verschillende identificerende persoonskenmerken, is het extra waarborgen van privacy nodig, waardoor het potentieel van de data niet benut kan worden. Een ander probleem is dat de gebruikte identificerende persoonskenmerken niet altijd een unieke combinatie opleveren; dit vergroot de kans op mismatches, dat afdoet aan de kwaliteit van de data en daarmee aan de uitkomsten van het gebruik ervan. Naast het ontbreken van een eenduidige methodiek voor koppelen in Nederland, zijn er ook nog geen mogelijkheden voor het koppelen met een bredere/Europese dimensie.

Waarborgen privacy:

Privacy wordt (over het algemeen) goed geborgd. Dit gebeurt echter wel op heel veel verschillende manieren, wat versnippering van de data in de hand werkt. Daarnaast kost dit veel tijd en geld, omdat steeds opnieuw het wiel wordt uitgevonden, of er een stapeling aan waarborgen wordt gerealiseerd om het zekere voor het onzekere te nemen. Het is onduidelijk waar de balans ligt tussen gegevensbeschermingsmaatregelen en risico's t.a.v. de aard van de data en het gebruik. Technische oplossingen leveren schijnzekerheid op als het waarom en de organisatie eromheen niet goed zijn of niet goed begrepen worden. Er heerst de onterechte opvatting dat het vragen van toestemming privacy waarborgt, waardoor het resultaat juist averechts kan uitpakken: als iemand toestemming geeft, ligt de verdere verantwoordelijkheid bij die persoon zelf (wat niet zo is, en ook niet kan). Als laatste ligt de nadruk op de verantwoordelijkheid van degene die de data genereert en beheert, en is er (te) weinig aandacht voor het sanctioneren van degenen die de privacy bewust of onbewust schenden.

Waarborgen kennisveiligheid:

Kennisveiligheid wordt goed geborgd als het FAIR principes uitgangspunt - *as open as possible, as closed as necessary* - goed wordt gehanteerd. De nadruk ligt bij de uitzonderingsgronden herleidbare persoonsgegevens en potentiële nationale veiligheidsproblemen. Met de toename van het gebruik van persoonlijke (zorg)data neemt ook de noodzaak toe om hier bewust van te zijn en dit duurzaam te regelen. Het ministerie van OCW werkt met onder andere NFU aan een nationale leidraad

kennisveiligheid, maar binnen de zorg en aanpalende domeinen is er nog weinig aandacht voor dit onderwerp.

Gestapelde toetsing:

Toetsing en beheer van het gebruik van zorgdata (data governance) voor secundaire doeleinden hangt af van het kader aan juridische, ethische, maatschappelijke en privacy- en kennisveiligheid gerelateerde wet- en regelgeving en afspraken. Omdat dit kader onduidelijk is, vindt de toetsing plaats op meerdere locaties, op verschillende manieren, op verschillende momenten, met verschillende belangen en vanuit verschillende perspectieven. Dit levert langdurige procedures en soms tegengestelde uitkomsten op.

Gezondheidsdata kunnen niet internationaal gedeeld worden:

Veel internationale samenwerkingen stranden, omdat afstemming over de juridische kant van het gebruik van zorgdata te lang duurt en/of te veel belemmeringen oplevert.

Gewenste outcomes Cluster 2

Het juridisch-ethisch-maatschappelijk kader voor het (meervoudig) gebruik van gezondheidsdata en -materiaal is helder, eenduidig en op nationaal niveau afgestemd. Daarbinnen en/of daarnaast is helder op welke manieren data met passende privacy-maatregelen en secuur gekoppeld kunnen worden. Vervolgens is het kader uitgewerkt in eenvoudige, haalbare, praktische en eenduidige standaardprocedures die zoveel mogelijk zijn verwerkt in bestaande (digitale) praktijken, zodat naleving zo eenvoudig mogelijk is, zowel voor professionals als voor burgers (compliance-by-design). Deze standaardprocedures betreffen in ieder geval:

- Het waarborgen/bevorderen van privacy,
- Het waarborgen/bevorderen van kennisveiligheid,
- Eenmalige (dus uniforme) toetsing,
- Internationaal delen,
- Verantwoord databeheer (*data governance*),
- Data voor/door bedrijven,
- Data voor/door overheid,
- Zeggenschap
- En veilig en eenduidig koppelen.

Er is draagvlak voor het gebruik van de procedures en optimale ondersteuning daarbij. Daarnaast is er een gestandaardiseerde systematiek voor controle, monitoring, evaluatie, en vernieuwing.

Om de gewenste outcomes te realiseren zijn de volgende outputs gesteld:

- Output 1: Geïntegreerde wet- en regelgeving gericht op de sector met inachtneming van ethische en maatschappelijke normen en waarden (gebruik van gezondheidsdata, -beelden en -materiaal t.b.v. een lerend zorgsysteem).
- Output 2: Register voor vastleggen zeggenschap → Nationaal (web-based) register
- Output 3: Systematiek voor unieke **koppelsleutel** voor secundair gebruik → Versleuteld BSN

Te realiseren Outputs Cluster 2

Output 1: Geïntegreerde wet- en regelgeving gericht op de sector met inachtneming van ethische en maatschappelijke normen en waarden (gebruik van gezondheidsdata, -beelden en -materiaal t.b.v. een lerend zorgsysteem)

Binnen deze wet- en regelgeving moeten de volgende vragen helder en eenduidig beantwoord worden:

- Wat zijn de juridische grondslagen waaronder gezondheidsdata (her)gebruikt mogen worden t.b.v. een lerend zorgsysteem (omvat kwaliteit, beleid, evaluatie, onderzoek, gebruik van lichaamsmateriaal etc.)?
- Wat zijn de voorwaarden hierbij?
- Op welke manier moet aan deze voorwaarden voldaan worden?
- Welke rechten en plichten horen hierbij? Voor welke partijen (incl. bedrijven)?
- Hoe verhoudt dit zich tot de EHDS, en andere internationale kaders?
- Welke consequenties heeft dit kader voor het waarborgen/bevorderen van privacy, kennisveiligheid, verantwoord databeheer en de toetsing hiervan? En voor het internationaal delen van data?
- Op welke manier wordt de naleving zo eenvoudig mogelijk gemaakt (compliance-by-design)?

Met inachtneming van tenminste de volgende onderdelen:

- Prioriteit: Grondslag(en): toestemming, geen bezwaar, uitzonderingen, voorwaarden
- Definitie Algemeen belang
- Helderheid over privacy-aspecten, beschermingsmaatregelen in relatie tot risico, definitie anoniem/pseudoniem
- Commercieel gebruik: definitie, wanneer wel/niet, uitzonderingen, voorwaarden
- Internationaal delen: definitie, wanneer wel/niet, uitzonderingen, voorwaarden
- Gebruik door de overheid: definitie, wanneer wel/niet, uitzonderingen, voorwaarden
- Gebruik na overlijden
- Sancties bij schenden privacy
- Toetsing niet-WMO onderzoek, incl. biobankonderzoek
- Bewaartermijnen
- Omgang met individuele bevindingen
- Patiënt- / Publieksinformatie
- Vorm: nieuwe wetgeving, veldnorm, gedragscode, tijdelijke afspraken, 'gedoogconstructie', één/meerdere kaders etc.
- Verantwoordelijkheden: monitoring, evaluatie, toezicht op naleving

Intermediate Outputs

- 1.1 Uitwerken duidelijkheid over / en oprekken van huidig kader (uAVG, WGBO, voorstel WZL, Wet publieke gezondheid), met daarbinnen voldoende zeggenschap en transparantie – z.s.m.
- 1.2 Uitwerken functionele specificaties van ideale toekomstige situatie waarbij we opt-out/geen-bezwaar systeem als theoretisch uitgangspunt nemen. Definiëren wat daarbinnen en daarbuiten valt, en welke voorwaarden daarbij horen.
- 1.3 Uitwerken hoe deze ideale situatie te vertalen naar regels, beslismodellen en zoveel mogelijk compliance-by-design, zodat niet alles langs een jurist hoeft.

1.4 Goed verhaal/goede communicatie (ism Cluster 1).

1.5 Ophalen welke zorgen/argumenten er bestaan, om die zo goed mogelijk te kunnen adresseren (ism Cluster 1 en 3).

Output 2: Register voor vastleggen zeggenschap → Nationaal (web-based) register

Nationaal (web-based) register waar burgers m.b.v. Digi-D of BSN in kunnen loggen en aan kunnen geven of ze wel of niet bezwaar maken tegen / wel of geen toestemming geven voor het gebruik van hun gegevens voor secundaire doeleinden. Vergelijkbaar met het nationale donorregister. Bij aanvragen voor het gebruik van de data kan via dit register nagegaan worden of de betreffende personen geen bezwaar hebben gemaakt / toestemming hebben gegeven (via bijv. Versleuteld BSN).

Deze output komt vnl. tegemoet aan de volgende genoemde obstakels:

- zeggenschap en bijkomende informatie is niet (uniform) geregeld
 - patiënten/burgers worden (te) herhaaldelijk geïnformeerd en gevraagd, en in andere gevallen helemaal niet
 - lokale zeggenschapsprocedure kan (te) veel administratie vergen voor een organisatie, waardoor ervan af gezien wordt
 - patiënten/burgers hebben geen zicht op welke zeggenschap ze hebben en/of hebben uitgeoefend
 - het nagaan van zeggenschap aanvragen voor gebruik van de data is tijdrovend en soms onmogelijk
- Met goede communicatie en transparantie komt deze output ook tegemoet aan de volgende obstakels:
- respons op zeggenschapsvraag is te laag
 - gekozen zeggenschapsprocedure veroorzaakt bias

Aandachtspunten:

- Uitkomst opt-in of opt-out (Output 1)
- Toestemming of bezwaar ligt niet meer (alleen) bij data verantwoordelijke (juridisch oké?)
- Mondelinge toelichting/persoonlijke begeleiding bij keuze moet anders georganiseerd worden
- Overtuiging richting burger nodig voor goede respons (publiekscampagne, inhoud en manier waarop, cluster 1)
- Transparantie, communicatie, terugkoppeling (ook cluster 1)
- Voor een aantal mensen lastig toegankelijk
- Link met databron en doel van datagebruik kan onduidelijker zijn voor burger
- Op welk(e) moment(en) in hun leven kunnen mensen hun zeggenschap uitoefenen?
- Versleuteld BSN nodig om zeggenschap na te gaan (=Output 3 binnen Cluster 2)
- Wie kan verantwoordelijk zijn voor een dergelijk register?

Intermediate Outputs

2.1 Concept/voorstel voor inrichten Mitz zodat het ook voor secundair gebruik geschikt is

2.2 Concept/voorstel voor: governance, juridisch kader, manier van toelichten/persoonlijke begeleiding (naast evt. Publiekscampagne), terugkoppeling

Output 3: Systematiek voor unieke koppelsleutel voor secundair gebruik → Versleuteld BSN

Voordelen

- Versleuteld BSN wordt al gebruikt om te koppelen binnen de zorg
- Er is een NEN norm voor pseudonimiseren
- BSN is geen bijzonder persoonsgegeven (AVG)
- Doordat BSN uniek is, kan exact gekoppeld worden
- Doordat BSN uniek is, kan de versleuteling volledig los staan van de overige gegevens
- BSN zit al in systemen van veel (zorg)organisaties
- Er is al ervaring met koppelen op basis van versleuteld BSN voor secundaire doeleinden, bijv. door CBS
- Er kan voortgebouwd worden op voorwerk gedaan voor secundair gebruik met trusted third parties (bijvoorbeeld GENONCO)
- Als BSN gebruikt mag worden, ook DigiD
- Technische aanvullingen (zie aandachtspunten) ontwikkeld voor secundair gebruik, kunnen ook primair van nut zijn

Aandachtspunten

- Wet- en/of regelgeving is nodig: Versleuteld BSN mag, mits....
- Goed verhaal nodig waarom dit beste optie is
- BSN zit (nog) niet in ieder systeem → fasering + mogelijkheden mee om te gaan zonder BSN
- Ook bij gebruik versleuteld BSN, is nog steeds een aanvullende uniforme systematiek nodig om de koppeling tot stand te brengen, om technische puntoplossingen te voorkomen. Verschillende technische tools in ontwikkeling om koppelen makkelijker en veiliger te maken, maar noodzaak koppelsleutel blijft.
- Er zijn mensen zonder BSN, en mensen die zorg in het buitenland afnemen (vooral langs de grenzen). Dan biedt BSN geen oplossing.

Randvoorwaarden

- Grondslag om te *mogen* koppelen blijft een voorwaarde (relatie met Cluster 2-Output 1)
- Politiek en maatschappelijk draagvlak

Sub-outputs

- Concept/voorstel voor aanpassen/nieuwe wetgeving
- Ophalen zorgen bij stakeholders
- Communicatie en transparantie richting burgers, politiek en professionals (relatie met Cluster 1)
- BSN in systemen (relatie met Cluster 3)