Domeinarchitectuur IZB

Programma Pandemisch Parate Informatievoorziening (PP-IV)

Versiebeheer

VERSIE	DATUM	STATUS	AUTEURS	OMSCHRIJVING
0.1	04-04-2023	Werkversie	Henk de Koning en Marco Braakman	Initiële versie. Doorlopend werkdocument.
0.2	14-02-2024	Concept	Henk de Koning, Charles Renshoff en Laurens Groenewegen	Eerste afslag voor semi-openbaar gebruik
0.3	26-03-2024	Concept	Atte Bootsma en Henk de Koning	Review commentaar verwerkt
0.4	27-03-2024	Concept	Laurens Groenewegen	Review vanuit architectuurboard
0.6	April/mei 2024	Concept	Diverse	Interne review
0.8	06-06-2024	Concept	Atte Bootsma	Ter commentaar naar PGIM-leden en ICT-commissie LOI
0.9	11-06-2024	Concept	Virginia Zorn	Eindredactie op document
1.0	18-06-2024	Publicatieversie	Henk de Koning	

1 Inhoudsopgave

Inhoud

2 Leeswijzer

Dit is de domeinarchitectuur voor (Pandemisch Parate) infectieziektebestrijding binnen de GGD GHOR Nederland. Dit is nadrukkelijk een levend document. De huidige versie (1e concept) is noch compleet, noch volledig; de focus voor deze versie lag meer op correctheid van wat beschreven staat, dan op volledigheid. De redeneerstijl in dit document is zuiver vanuit functionaliteit richting techniek en technische consequenties. In dit document staan dan ook de nodige eisen en principes, die beperkend of leidend werken voor de keuzes in de techniek. Om de leesbaarheid te vergroten zijn er stijlen doorgevoerd:

Een eis heeft deze stijl; dit is een consequentie waar de oplossingsrichting aan heeft te voldoen;

Een definitie heeft deze stijl; dit introduceert een betekenis van een concept die voor de rest van het document geldt.

Een principe heeft deze stijl; dit poneert een uitgangspunt waar de rest van de tekst op voortborduurt.

3 Inleiding

In de evoluerende wereld van infectieziektebestrijding neemt informatievoorziening een steeds prominentere plaats in. Waar Q-koorts duidelijk aantoonde dat interdisciplinaire data-uitwisseling en (bron)informatiedeling randvoorwaardelijk zijn voor begrip en (dus) bestrijding, maakte de COVID-19 pandemie pijnlijk duidelijk dat de extreme flexibiliteit die gevraagd werd, zowel in aantallen/grootte als in snelheid van veranderingen aan datastromen en toepassingen, de geautomatiseerde ondersteuning op het kritieke pad bracht van effectieve infectieziektebestrijding en daar feitelijk ook een bottleneck voor vormde. Daarom vraagt de doelarchitectuur van het programma Pandemisch Parate Informatievoorziening veel aandacht voor begrippen als betrouwbaarheid, schaalbaarheid en wendbaarheid: de IV van de infectieziektebestrijding moet (beter) voorbereid zijn op een toekomstige nieuwe pandemische situatie.
Een grote uitdaging hierbij is het onvoorspelbare karakter van een toekomstige nieuwe pandemie; bij een IV-traject zijn we gewend te opereren vanuit heldere business requirements en vervolgens door te redeneren naar de te realiseren voorzieningen. In het geval van pandemische paraatheid zit daar een element bij van onzekerheid. Een nadrukkelijk doel van deze domeinarchitectuur is om zo goed mogelijk voorbereid te zijn op een aantal onzekere factoren, zoals ook benoemd in de doelarchitectuur IZB. Hiertoe volgen we een tweesporenbeleid:

1. Enerzijds verkennen we de functionele behoefte, zoals aanwezig in de huidige reguliere IZB en zoals we uit het recente COVID verleden geleerd hebben. Dit zijn de functionele requirements.
2. Anderzijds abstraheren we uit diverse mogelijke maatregelen, de kernconcepten die ons tijdens de COVID-19 periode geholpen zouden hebben beter in te spelen op de veranderende behoefte in een pandemische situatie ten opzichte van de reguliere IZB. Deze concepten zijn:

    - **Schaalbaarheid: het vermogen van een systeem om snel te reageren op veranderende werklast.**
    - **Wendbaarheid: het vermogen van een systeem om snel gedrag aan te passen aan veranderende situaties.**

- **Betrouwbaarheid: betrouwbaarheid kent verschillende aspecten:**
  - **De waarschijnlijkheid dat een systeem zijn functie uitvoert binnen een gespecificeerde tijdsperiode onder gespecificeerde omstandigheden.**
  - **De mate waarin een burger kan vertrouwen op het zorgvuldig gebruik van informatie in het IZB-systeem.**

De kern van dit document bestaat uit de verdere uitwerking van deze concepten in relatie tot het werkveld van de 25 GGD'en.

3.1 Doelstelling

Dit document beschrijft de nieuwe informatievoorziening voor het IZB-werkveld en de plaats van de GGD hierin, die zowel inzetbaar is voor reguliere werkzaamheden als tijdens een pandemie.

Tevens bevat dit document richtinggevende kaders en keuzes voor de realisatie van de nieuwe IV.

3.2 Doelgroep

Dit document is met name gericht op:

- Medewerkers van GGD'en / GGD GHOR Nederland, die de nieuwe IV realiseren.
- Marktpartijen die de nieuwe IV van GGD GHOR Nederland leveren.

4 Grondslagen en kaders

Dit document staat niet op zichzelf, maar bouwt voort op diverse wettelijke grondslagen en kaders vanuit bestaande bedrijfsvoering van de GGD'en. Deze grondslagen staan in Bijlage 07 - Kaderdocument conceptueel model. Welke kaders specifiek zijn voor het karakter van de IZB, het aspectgebied van dit document, is uitgewerkt in hoofdstuk 7.

5 IZB in Nederland

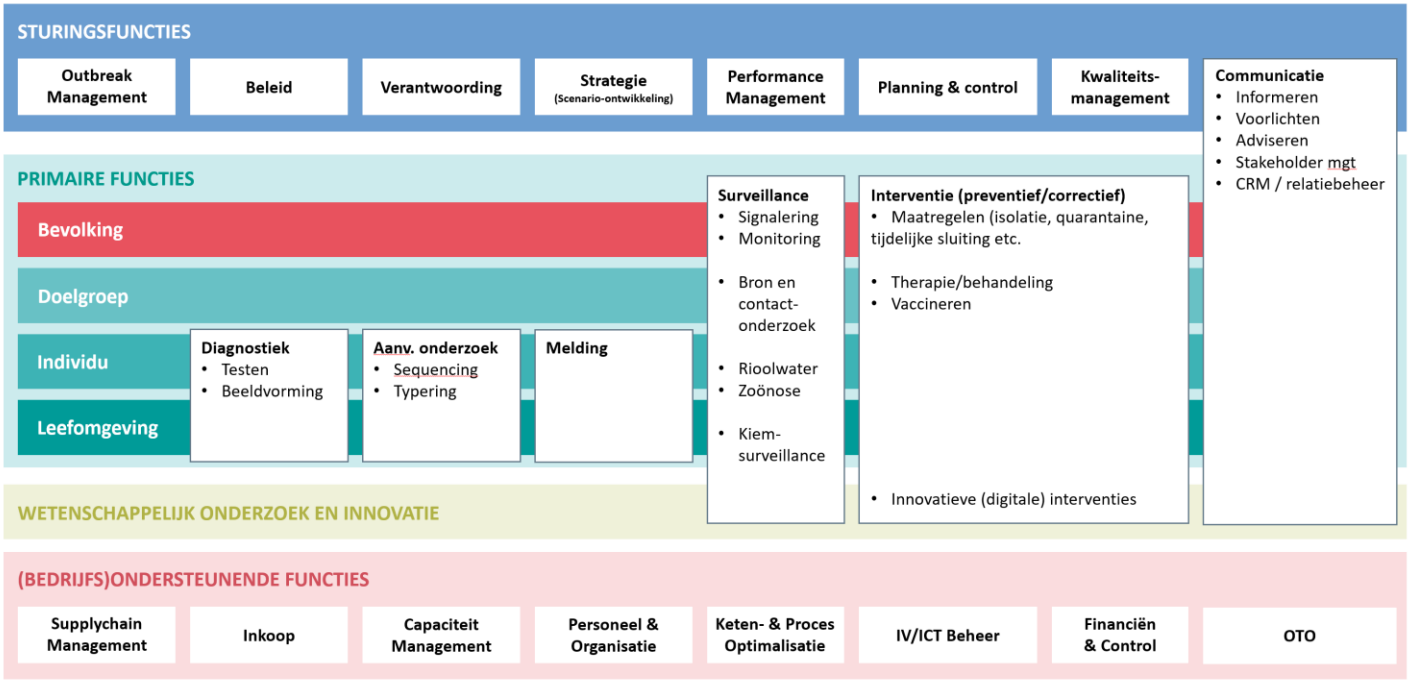
Infectieziektebestrijding in Nederland is een gedeelde verantwoordelijkheid van zorgverleners, instellingen, laboratoria, GGD (zowel regionaal als overkoepelend), RIVM en het ministerie (VWS).

- **Rijksoverheid**: de Rijksoverheid (het ministerie van VWS) heeft volgens de WPG de verantwoordelijkheid om het landelijke beleid voor infectieziektebestrijding te ontwikkelen. Daarnaast is de Rijksoverheid verantwoordelijk voor coördinatie in het geval van een landelijke uitbraak van infectieziekten (zie ook het RIVM hier onder).
- **RIVM**: de Rijksoverheid heeft een deel van de taken die zij heeft in het kader van de infectieziektebestrijding ondergebracht bij het RIVM. Daarbij gaat het bijvoorbeeld om:
  - Het opstellen van richtlijnen voor de uitvoering van de IZB
  - Landelijke surveillance
  - Coördinatie van bovenregionale uitbraken
  - Via de LFI (Landelijke Functionaliteit Infectieziektebestrijding) aansturen van de IZB-keten in het geval van een pandemie
- **Gemeenten**: gemeenten zijn verantwoordelijk voor de lokale uitvoering van het infectieziektebestrijdingsbeleid. Dit omvat het monitoren van infectieziekten, het reageren op lokale uitbraken, en het voorlichten van het publiek over preventiemaatregelen.

- **GGD'en** (Gemeenschappelijke Gezondheidsdiensten): GGD'en voeren in opdracht van gemeenten de infectieziektebestrijding uit. Ze zijn verantwoordelijk voor de surveillance van infectieziekten, het onderzoeken van uitbraken, het nemen van maatregelen om de verspreiding van ziekten te beperken, en het geven van voorlichting en advies aan het publiek en andere betrokken organisaties.
- **GGD GHOR Nederland**: GGD GHOR Nederland is de brancheverenigingen van de GGD'en. GGD GHOR Nederland fungeert namens de GGD'en als opdrachtgever voor de realisatie van het GGD-deel van het pandemisch parate IV-landschap.
- **Zorgaanbieders**: zorgaanbieders hebben de verantwoordelijkheid om infectieziekten te melden bij de GGD, en om deel te nemen aan maatregelen om de verspreiding van ziekten te beperken.
- **Instellingen**: instellingen waar voor infectieziekten kwetsbare populaties verblijven of samenkomen voor een of meer dagdelen per etmaal, hebben een meldingsplicht aan de regionale GGD.
- **Laboratoria**: een laboratorium dat een verwekker van een infectieziekte A, B1, B2 of C vaststelt, heeft een meldingsplicht aan de regionale GGD waar aanvragend arts praktijk houdt.

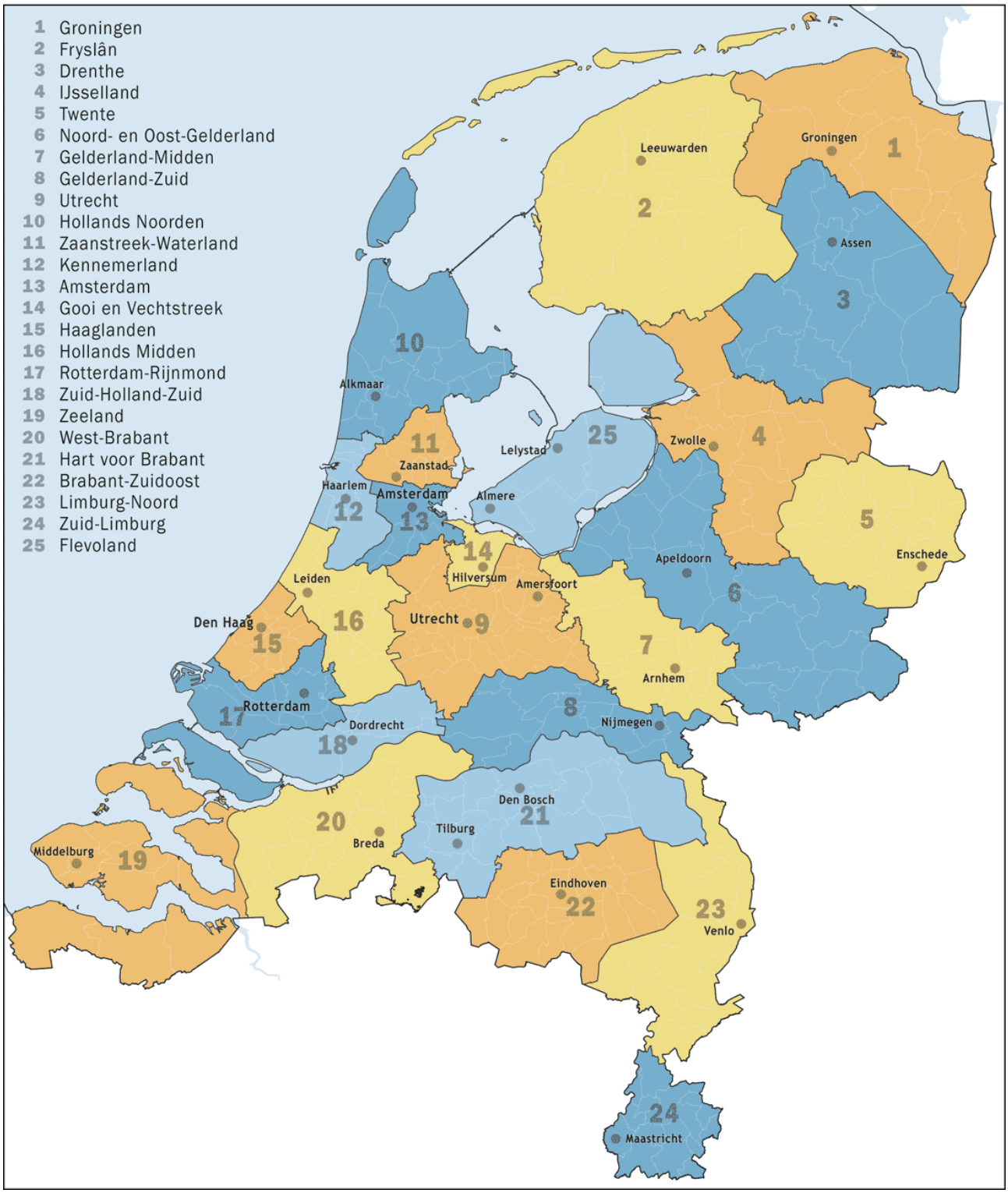
5.1 Bedrijfsfunctiemodel

Tijdens het opstellen van de doelarchitectuur IZB is samen met professionals uit de IZB een eerste versie gemaakt van het bedrijfsfunctiemodel van de IZB:

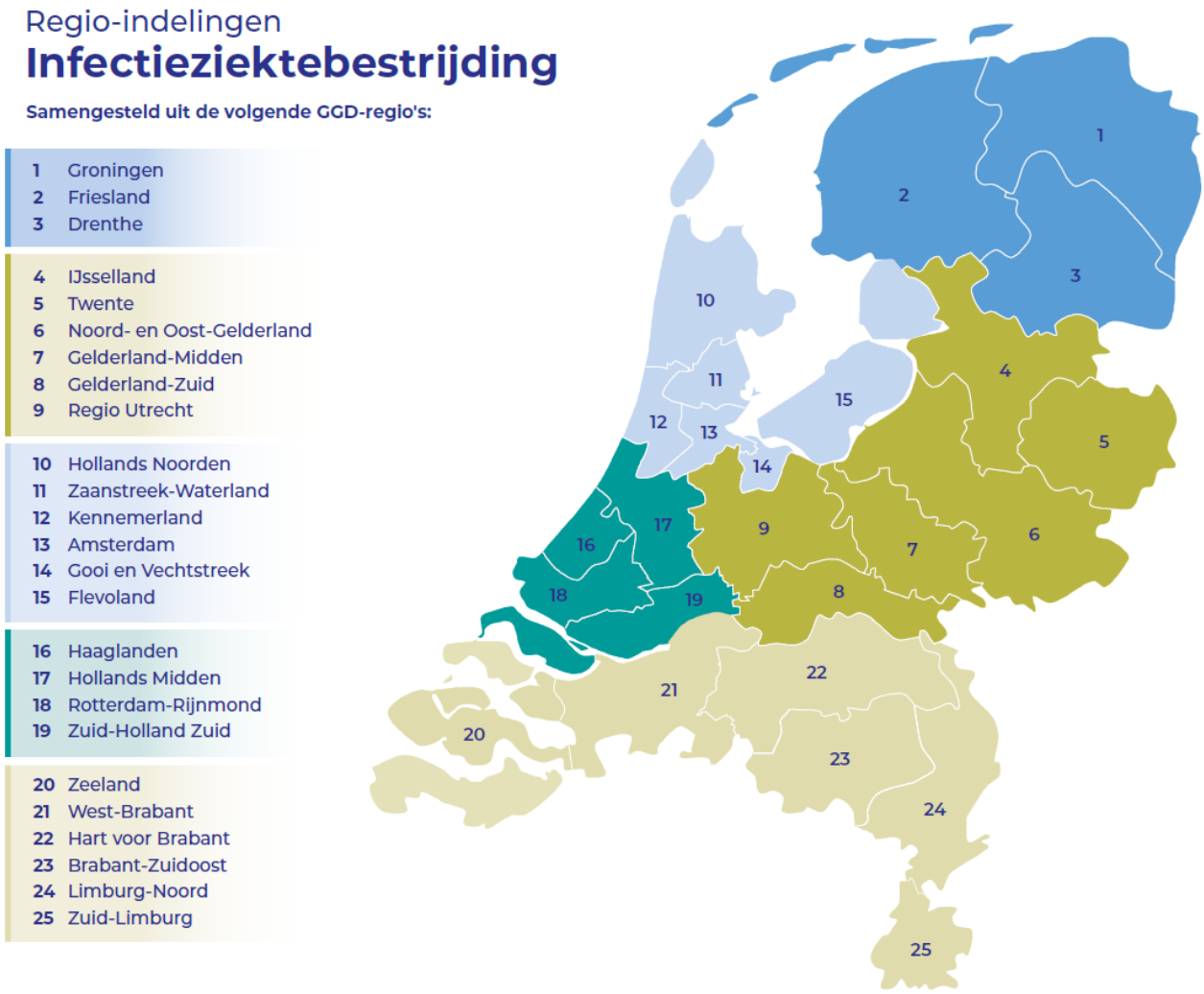


5.2 Indeling GGD-regio's

Nederland kent vijfentwintig onafhankelijke GGD'en:



Deze zijn verdeeld in vijf IZB-regio's. Er is in diverse vormen sprake van regionale en bovenregionale samenwerking. De regio-indeling is als volgt:



6 Taken van de GGD

Binnen de Wet Publieke Gezondheid (WPG) heeft de GGD (als containerbegrip voor één van de vijfentwintig) een belangrijke taak binnen de infectieziektebestrijding. Waar reguliere zorgaanbieders (huisartsen, ziekenhuizen, instellingen) verantwoordelijkheid dragen in de curatieve sfeer, heeft de GGD verantwoordelijkheid in de publieke sfeer:

- bestrijden van infectieziekten en voorkomen van verdere verspreiding;
- surveillance;
- beleidsadvisering;
- preventieactiviteiten;
- netwerk en regie;
- voorbereiding op grootschalige infectieziekte-uitbraken;
- kennis en onderzoek.

(bron: Adviesrapport de-kerntaken van de IZB)

6.1 Organisatie van de 25 GGD'en

Hoewel de GGD een centrale rol speelt in de infectieziektebestrijding is de wijze van organiseren decentraal. Er zijn 25 onafhankelijke GGD'en die deel uitmaken van een gemeentelijke organisatie of veiligheidskoepel.

6.1.1 Grensregio's

De GGD'en die een grens delen met België en/of Duitsland hebben doorgaans, naast de formele meldingsplicht via de Europese kanalen, een informele relatie met de buitenlandse buurregio's waarbij een casus telefonisch of via email informeel aangekondigd wordt. In sommige gevallen wordt daarbij de formele meldplicht aan de buurregio overgelaten, om een langdurige hiërarchische keten te omzeilen.

De grensregio's hebben, uit de aard der zaak, een bredere scope bij surveillance en bron- en contactonderzoek (BCO). Ook voor GGD-regio's met een (lucht)haven (zoals bijvoorbeeld GGD Kennemerland) is de scope breder. De International Health Regulations verplicht landen om maatregelen te treffen bij (lucht)havens. Voor GGD'en met een haven of luchthaven aangewezen als 'plaats van binnenkomst' betekent de implementatie van de IHR extra voorbereidingen voor:

- surveillance: afspraken maken voor meldingen van gezagvoerders van (lucht)vaartuigen) en
- respons: het afhandelen van incidenten in de (lucht)haven.

6.1.2 Generieke versus specifieke uitvoering

In de infectieziektebestrijding wordt al sinds begin jaren negentig met de oprichting van het LOI en LCI en het later opgerichte LOVI gewerkt aan de kwaliteit van de IZB. De richtlijnen van het LCI hebben daarin een centrale plaats. Deze generieke richtlijnen worden door de GGD'en uitgewerkt in werkinstructies. Het is verder zo dat er lokaal accenten zijn in de uitvoering die worden ingegeven door de context (luchthaven, zeehaven, asielopvang, landgrens).
Generiek: iedereen werkt op dezelfde manier conform LCI-richtlijnen op basis van consensus of noodzaak (bijvoorbeeld Covid-19).
Specifiek:

1. Door specifieke karakteristieken in de regio: luchthaven, zeehaven, asielopvang, landgrens.
2. Door verschillen die ontstaan door lokale interpretatie en uitvoering van LCI-richtlijnen of beschikbare tijd voor uitvoering van werkzaamheden.

6.1.3 Regulier versus pandemisch

De opschaling van de medisch-operationele processen bij de GGD'en heeft consequenties voor de uitvoering.
In de reguliere bestrijding wordt de IZB uitgevoerd door gespecialiseerde professionals (artsen, verpleegkundigen, epidemiologen, deskundigen infectiepreventie, etc.) volgens landelijk ontwikkelde richtlijnen. De professionals voeren deze taken autonoom uit en zullen de richtlijn binnen de context van de casus interpreteren. Wanneer er geen verheffing van een infectieziekte gaande is, kenmerkt de werkwijze zich door een hoge mate van vrijheid in het kiezen en opvolgen van een aantal standaardtaken. Hierbij is tijd en gelegenheid beschikbaar voor een meer op de casus gerichte interpretatie van richtlijnen, of extra aandacht voor voorlichting en kennisdeling.
Op het moment dat er sprake is van een opschaling, en zeker ten tijde van een pandemie, zal extra personeel worden ingezet dat met een korte opleiding taken zal verrichten. Deze taken worden strakker applicatief ondersteund qua workflow en beslisondersteuning. Dit stelt ook eisen aan de functionaliteit om werk te verdelen.

Regulier:

1. Kenniswerkers (highly skilled): veel vrijheid in workflow binnen de gebruikersinterface van het IZB systeem met brede autorisatie

2. Noodzakelijke, specifieke eisen op lokaal niveau mogelijk
    a. Wel op basis van een gedeeld domeinmodel
3. Kenmerken gebruikersinterface: veel vrijheid voor gebruiker, kiest zelf pad en volgorde

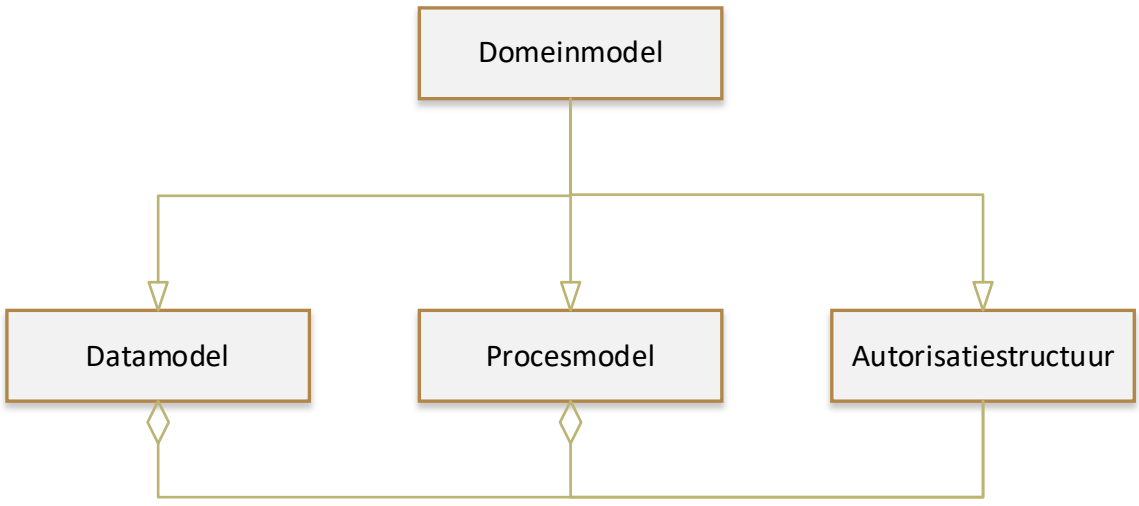
Pandemisch (opgeschaald):

1. Veel (low-skilled) medewerkers
2. Hoge standaardisatie van workflow met medewerkers in specifieke rollen met beperkte autorisatie.
3. Opdelen in kleine taken
4. Kenmerken gebruikersinterface: sterke sturing door de stappen en volgorde ervan. Er is sprake van een workflow component.

6.1.4 Elke GGD in regie op eigen data

Er zijn in Nederland vijfentwintig onafhankelijke GGD'en, zij zijn en blijven eigenaar zijn van hun eigen data. Een infectieziekte houdt zich echter niet aan de grenzen van één GGD en ook burgers bewegen zich van de ene GGD naar de andere. Dus is het voor processen als diagnose, interventie, surveillance en bron- en contactonderzoek van belang dat er (inzage)functies zijn die GGD en regio-overstijgend zijn. Om bij het doelarchitectuur principe van een datacentrisch landschap te blijven: de dataservice gedraagt zich als één logisch geheel, maar bestaat wellicht uit meerdere, onafhankelijke services die tezamen de complete data van de vijfentwintig GGD'en bevatten.

Los van privacy- en securityaspecten heeft dit consequenties voor de manier waarop we gegevens structureren; de verschillende GGD'en dienen elkaars gegevens te begrijpen op het niveau van overkoepelend belang, zowel syntactisch als semantisch. Dit betekent dat er eenheid van taal moet zijn en eenheid van begrip. Alle informatie rond kernentiteiten in het domein van de IZB zoals context, dossier, locatie, bron en contact, moet dermate rigide beschreven en geüniformeerd zijn, zodat alle GGD'en - ongeacht lokale verschillen - elkaars gegevens kunnen duiden en begrijpen. We doen dit in een domeinmodel, dat alle metadata[1] over gegevens, processen en autorisaties[2] bevat:



Dit houdt in dat de GGD'en binnen de IZB gaan werken op basis van één gemeenschappelijk overkoepelend model, dat aansluit op de keten waar RIVM ook in participeert. Gezien de aard van de IZB valt te verwachten dat dat model met grote regelmaat aangepast zal worden.

[1] Gegevens die andere gegevens beschrijven, inclusief zichzelf

[2] En beschrijvende karakteristieken als retentietermijn, grondslag, BIV classificatie en doelbinding

De vijfentwintig GGD'en zijn de eigenaren/verwerkingsverantwoordelijken van de data en hebben ieder een eigen (toegang tot een) subset van de GGD IZB data, dus vijfentwintig 'logische partities'. Tezamen vormen ze de IZB-data van de GGD in Nederland.

6.1.4.1 De rol van de GGD GHOR Nederland

Op dit moment zijn de GGD'en verwerkingsverantwoordelijk voor de data die zij genereren en fungeert GGD GHOR Nederland hooguit als verwerker. In het kader van de evaluatie van de COVID-19 pandemie worden wetsvoorstellen voorbereid waarin de rol van de GGD GHOR Nederland expliciet benoemd wordt.

6.1.5 IV-samenwerking tussen GGD'en: iStrategie

De GGD'en hebben gekozen voor een pad waar toekomstige IV meer in gezamenlijkheid wordt ontwikkeld (iStrategie, 2024).

"In de afgelopen jaren hebben we voor de verschillende domeinen in de publieke gezondheid een omgeving opgebouwd waarbij niet voor alle dossiersystemen of beschikbare technische (basis) voorzieningen sprake is van landelijke schaalgrootte.

Het platform van de toekomst is de digitale snelweg; het technisch fundament dat onder het pandemisch parate IV- en datalandschap komt te liggen. In het platform van de toekomst creëren we op landelijk niveau de technische 'basisvoorzieningen' die we kunnen op- en afschalen. Bij het realiseren van de landelijke basisvoorzieningen hanteren we het motto 'centraal als het kan, decentraal als het moet'. Dit vloeit voort uit de volgende overwegingen:

- Het gezamenlijk verwezenlijken van IV-voorzieningen is effectief, efficiënt en noodzakelijk. Een regionale GGD is individueel te klein om voorzieningen zoals softwaresystemen te bouwen, te beheren, door te ontwikkelen of te exploiteren.
- Landelijk ontwikkelen en beheren is goedkoper dan op 25 plaatsen opnieuw het wiel uitvinden.
- Als we generieke basisvoorzieningen (zoals het inregelen van toegankelijkheid) beschikbaar maken vanuit één punt, hebben de regionale GGD'en er geen omkijken meer naar.
- Als we diensten (her)ontwerpen met samenwerkingspartners kunnen we die versterken en vernieuwen op basis van de landelijke, centraal beheerde en ontwikkelde systemen, want die vormen immers een stevige basis.
- Een goede centrale ondersteuning van dossiervoering, registratie en werkprocesondersteuning is van belang bij de uitvoering van onze reguliere taken in de publieke gezondheid, evenals de taken die we in de pandemische setting met andere instanties en partijen (moeten) oppakken.
- Door met ketenpartners samen te werken kunnen we werken aan een optimale datatoegankelijkheid waarbij we ook data-uitwisseling en dataverrijking realiseren.

De IV voor de IZB wordt ontwikkeld volgens deze iStrategie. De eigen data van iedere GGD wordt geplaatst op het gezamenlijke platform (centrale dataopslag).

6.1.6 Consequentie voor de nieuwe IV

De eis aan de nieuwe IV is:

1. **Iedere GGD blijft zelf eigenaar/verwerkingsverantwoordelijke voor de eigen data.**
2. **De eigen data van iedere GGD wordt geplaatst op het gezamenlijke (centrale) platform.**

3. **Iedere GGD bepaalt zelf welke medewerker welke autorisaties krijgt**
4. **Elke GGD handelt op basis van het gedeelde model, en kan aanvullingen doen voor (bijvoorbeeld) regio specifieke informatie. Deze aanvullingen worden centraal doorgevoerd.**

6.2 Communicatie met ketenpartners

Het bestrijden van een infectieziekte vraagt samenwerking tussen diverse partijen. Deze ketensamenwerking staat (grotendeels) benoemd in de Wet Publieke Gezondheid. De belangrijkste ketenpartijen zijn:

- **RIVM**: het RIVM is verantwoordelijk voor het vaststellen van richtlijnen voor de bestrijding van een infectieziekte en het bewaken van een nationaal beeld (van o.a. verspreidingsgraad, typering en vaccinatiegraad).
- **(Huis)artsen**: bij het constateren van een meldingsplichtige infectieziekte is een (huis)arts verplicht deze te melden bij de lokale GGD, dit kan telefonisch of via zorgmail.
- **Laboratoria**: een laboratorium meldt de vaststelling van een verwekker van een infectieziekte behorend tot groep A1, A2, B1, B2 of C aan de GGD van de gemeente waarin de arts die het onderzoek bij het laboratorium heeft aangevraagd, zijn praktijk heeft.
- **Zorginstellingen**: Op basis van artikel 26 van de Wet publieke gezondheid dient het hoofd van een instelling, waar voor infectieziekten kwetsbare groepen verblijven of samenkomen, de GGD op de hoogte te stellen van het optreden van een ongewoon aantal zieken. Een aantal GGD'en gebruiken het digitale platform MUIZ (Meldpunt Uitbraken Infectieziekten & BRMO) voor artikel 26 meldingen.

Tijdens een pandemie kunnen (bijvoorbeeld doordat extra gegevens nodig zijn) andere partijen bij de bestrijding betrokken worden. De omvang van de interactie vereist verregaande automatisering.
Dit betekent dat er naast standaardisatie in de communicatie met bekende ketenpartners ook sprake moet zijn van een grote mate van flexibiliteit om snel nieuwe, voorheen onbekende, ketenpartners aan te kunnen sluiten. In de doelarchitectuur wordt dit aangeduid met *paradoxale standaardisatie* en dit is een belangrijke drijfveer voor het opzetten van een sluitend domeinmodel.

6.3 Bedrijfsvoering

Het voert te ver om hier de complete bedrijfsvoering van de IZB binnen de GGD'en te beschrijven, hiervoor is een globale functionele beschrijving gemaakt (zie Bijlage 11 - Beschrijving hoofdprocessen IZB). Er is echter een aspect in de bedrijfsvoering dat grote architecturele consequenties heeft: de mate van opschaling van processen en, daarmee, de hoeveelheid mensen die betrokken zijn. Dit heeft zich tijdens de COVID-19 pandemie geuit in het massaal aanhaken van extra personeel, zowel geschoold als ongeschoold. De nieuwe IV moet hierop voorbereid zijn. Een belangrijke pijler hierbij is de wijze van authenticeren en autoriseren.

7 IV voor IZB voor, tijdens en na COVID

Om goede keuzes te kunnen maken, is begrip van het bestaande IV-landschap essentieel. Kenmerken van de IV die op dit moment door de GGD'en gebruikt wordt bij hun werkzaamheden in de IZB zijn:

- IV voor IZB kent een groot aantal applicaties en leveranciers.
- Medewerkers kunnen niet makkelijk bij data van andere GGD'en; de toegang is niet automatisch geregeld.
- Er is weinig sprake van hergebruik van applicaties.

Deze kenmerken zijn terug te leiden tot:

- Het decentrale karakter van de uitvoering van de reguliere infectieziektebestrijding en daarmee van de IV (uitvoering per GGD).
- Noodzakelijke toevoegingen en aanpassingen in de informatievoorziening, specifiek ten behoeve van de COVID-19 bestrijding vanuit een landelijke inzet.
- De veelheid van opdrachtgevers (gemeenten, VWS-directie Publieke Gezondheid, VWS (programma)directie COVID-19, VWS-directie Pandemische Paraatheid) en daarbij behorende (separate) verwachtingen en financiering.
- Gescheiden opdrachtgeverschap en uitvoering van de deelgebieden van de infectieziektebestrijding kennen hun eigen IV-middelen en leveranciers (naast de Algemene Infectieziektebestrijding en COVID-19 zijn GGD'en ook actief op het gebied van TBC-bestrijding, HPV-vaccinaties, MPX-vaccinaties, Seksuele Gezondheid, Reizigersvaccinatie en het uitvoeren van het Rijksvaccinatieprogramma).

7.1 Kernsystemen medio 2024

Corona-gerelateerde vaccinatie- en testgegevens liggen vast in CoronIT (SaaS-dienst), de reguliere infectieziektebestrijding vindt plaats in HPZone (op basis van centrale hosting) bij 23 GGD'en en GLIMS en Vaccinatieregister respectievelijk bij twee andere GGD'en. GLIMS wordt daarbij mogelijk dit jaar nog vervangen door HPZone. In dat geval blijven er twee systemen over.
Bij HPZone is het daarbij zo, dat er geen sprake is van een uniforme inrichting en werkwijze, maar dat GGD'en hun eigen inrichtingskeuzes hebben gemaakt.
Bij de implementatie van de nieuwe informatievoorziening zal migratie van data uit deze bronsystemen een belangrijk element vormen.

7.2 IV IZB COVID-19 landschap

Het COVID-19 IV-landschap is onder regie van het ministerie van VWS door de LCCB en GGD GHOR Nederland gerealiseerd als noodzakelijke -heel specifieke- voorziening voor de landelijke bestrijding van COVID-19. Dit maatwerk (puntoplossing) was nodig omdat een landelijke oplossing niet voorhanden was vanuit de decentraal ingerichte GGD'en.
De COVID-19 bestrijding zal naar verwachting de komende jaren, in lijn met het advies van de Gezondheidsraad, structureel onderdeel blijven van de werkzaamheden van de IZB-afdelingen van de GGD'en. Het COVID-19 IV-landschap is momenteel het enige operationele IV-landschap dat deze bestrijding de komende jaren kan ondersteunen, hoewel het is teruggebracht tot enkel functionaliteit ten behoeve van de reguliere Covid-19 vaccinatiecampagne. Dit landschap blijft daarom nog nodig, maar zal op termijn overgaan in het nieuwe pandemisch parate IV-landschap. De manier waarop dit laatste zal gebeuren is nog niet bepaald. Voor de hand ligt om het oude landschap waar mogelijk te hergebruiken en waar dat niet mogelijk is af te bouwen en de data over te brengen naar het nieuwe landschap.

7.3 Beoogde strategie

De beoogde kernstrategie is een convergentiemodel: binnen een periode van 3 jaar (2023-2026) gaan we middels convergentie van het huidige IZB IV-landschap, inclusief voorzieningen voor COVID-19 IV, naar het nieuwe pandemisch parate IV-landschap, dat dagelijks bij de reguliere IZB-werkzaamheden gebruikt wordt en bovendien structureel voldoet aan de eisen voor pandemische paraatheid.

- Een geleidelijke overgang is noodzakelijk voor het adequaat afbouwen van een onder druk opgebouwd (COVID-19) IV-landschap. Immers, er zijn veel data, kennis en systemen opgebouwd, waar nog verplichtingen aan vastzitten (denk aan wettelijke bewaartermijnen van data) en waar potentieel waardevol hergebruik mogelijk is.
- Het convergentiemodel geeft ruimte om op gecontroleerde wijze het één in het ander te laten overvloeien. Ook hier geldt: IV is niet alleen ICT, maar raakt ook data, wetgeving, eigenaarschap, proces, mens, contract, leverancier, geld, enzovoorts.
- Omdat het pandemische parate IV-landschap een structureel andere opzet kent dan het huidige landschap, zal een deel van de voorzieningen fundamenteel vernieuwd moeten worden.

- Tegelijkertijd is het zo, dat een deel van het IV-landschap zoals dat op dit moment bestaat, in de periode 2024-2026 (de 'tussenfase') een cruciale rol speelt bij het behalen van de volgende doelen:
  1. Beheer en continuïteit van de (medische) data (en bijbehorende applicaties), kunnen voldoen aan wettelijke eisen voortvloeiend uit WGBO, AVG en wetenschappelijk onderzoek.
  2. De uitvoering van COVID-19 vaccinatiewerkzaamheden. Dit betreft zowel najaarscampagnes als een continu aanbod voor specifieke risicogroepen.
  3. Voldoen aan de opdracht om 'zo goed mogelijk' pandemisch paraat te zijn, voor het geval zich een nieuwe pandemie voordoet, voordat het nieuwe IV-landschap gereed is. Vanuit de LFI wordt daarbij allereerst aandacht gevraagd voor de beschikbaarheid van voorzieningen voor Datalab, Geoefendheid, Serviceplein en Grootschalig Klantcontact.
  4. Potentieel hergebruiken/continueren van delen van het huidige COVID-19 IV-landschap voor het pandemisch parate IV-landschap dat vanaf 2027 (of zoveel eerder als mogelijk) gereed is.
  5. Ondersteuning van de 'Landelijke vaccinatievoorziening' waar op dit moment over gesproken wordt, indien deze wordt gerealiseerd door de GGD'en. Dit is van toepassing wanneer deze voorziening start voordat de daarvoor benodigde IV in het pandemisch parate IV-landschap gereed zijn.

8 Nieuwe IV voor IZB

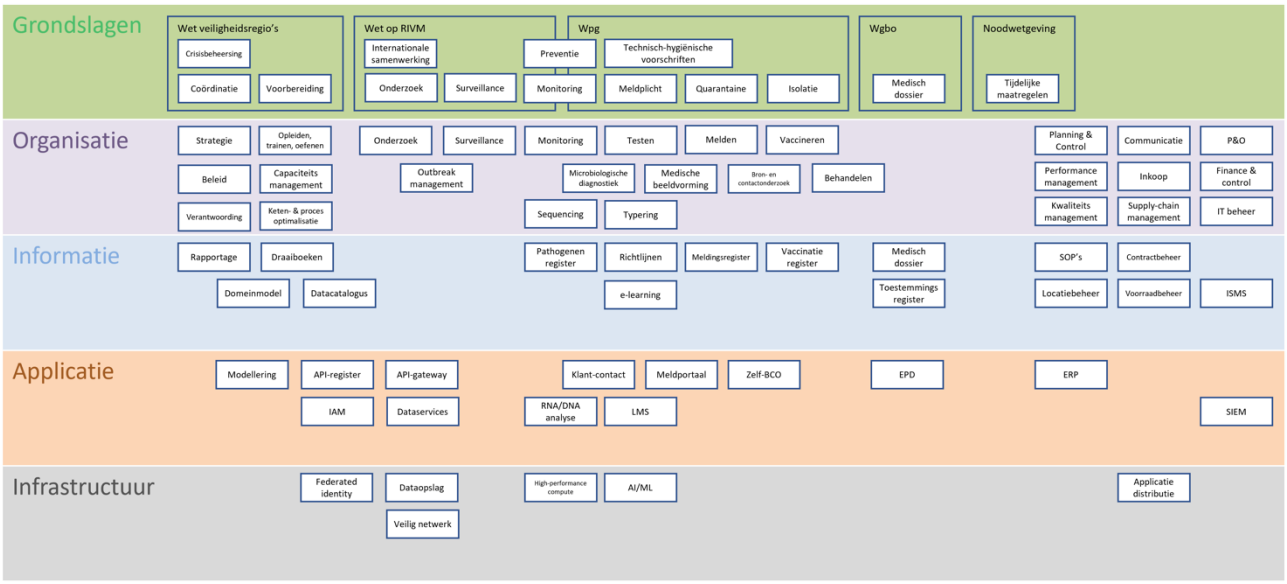
8.1 Visie op het nieuwe IZB-systeem

Het platform levert voor professionals van GGD'en, die effectief infectieziekten willen voorkomen en bestrijden, IZB-functionaliteit die - naast de dagelijkse infectieziektebestrijding waaronder surveillance, testen en (grootschalig) vaccineren - ook wetenschappelijk onderzoek en het opstellen van beleid ondersteunt. Doordat het systeem eenvoudige en eenmalige registratie mogelijk maakt en snel de juiste informatie en verbanden in beeld brengt, hebben professionals tijd over om zich te richten op hun zorgtaken en wordt het werk leuker. Dit systeem bevordert de betekenisvolle gegevensdeling tussen partners in de IZB, waardoor men beter bovenregionaal kan samenwerken. Kennis uit richtlijnen is geïntegreerd in de werking van het systeem, wat het werk makkelijker en beter maakt. Uitgangspunt is "gestandaardiseerd waar het kan, en specifiek waar het moet".
De kracht van het platform is, dat het een veilige, gebruikers- en privacyvriendelijke en weinig foutgevoelige omgeving is, die zowel in de reguliere als in de pandemische situatie het werk goed ondersteunt. Uiteindelijk

ondersteunt het platform al het werk in de algemene infectieziektebestrijding en in de toekomst mogelijk ook in andere afdelingen van de GGD'en.

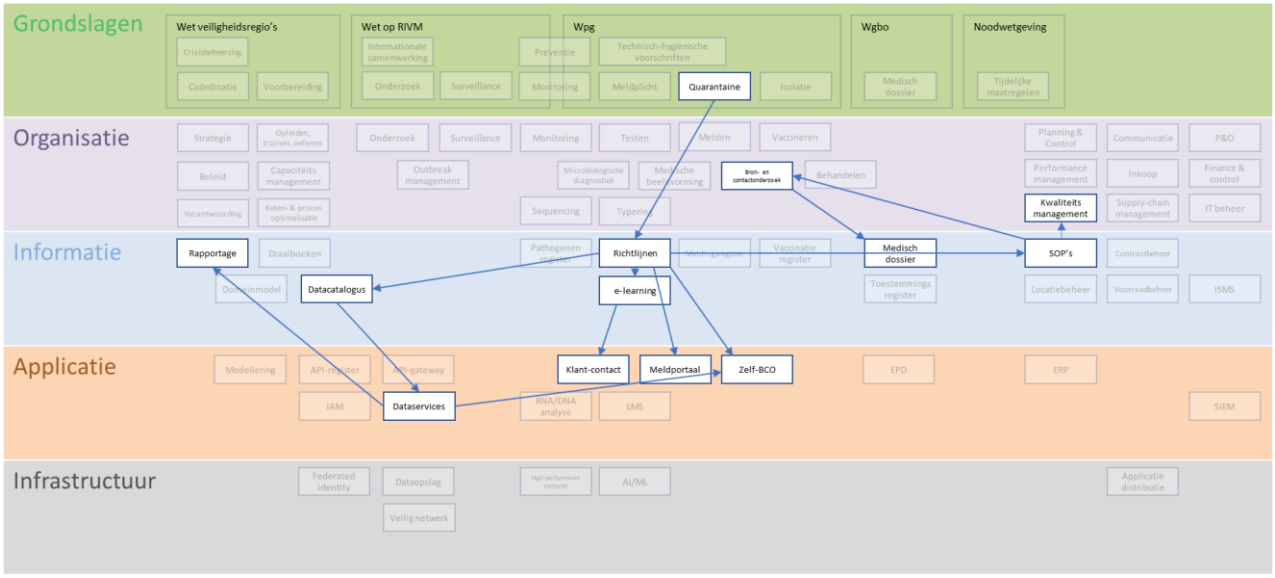
8.2 Capabilities in het nieuwe platform

Capabilities (gerelateerd aan NORA vijf-lagen model)



Zoals bovenstaande afbeelding[3] illustreert, vraagt de realisatie van het IV-landschap om capabilities in alle lagen van het NORA-model (de in de afbeelding weergegeven capabilities zijn indicatief, met andere woorden: de lijst is niet gegarandeerd volledig en kan nog wijzigen).
Wat de domeinarchitectuur voor de informatievoorziening voor de GGD bijzonder maakt, is het aspect pandemische paraatheid. Dit hoofdstuk behandelt met name de kenmerken van de nieuwe IV die afwijken van een doorsnee EPD of standaardsoftware- of maatwerkoplossing.
De karakteristieken wendbaarheid, schaalbaarheid en betrouwbaarheid, als kernwaarden voor de nieuwe IV, zijn niet uitsluitend voorbehouden aan de informatie- en applicatielagen. De context ervan is breder en een toename in het aantal besmettingen, wat leidt tot een endemie of pandemie, heeft net zo goed consequenties op grondslagen-, organisatie- en infrastructuurniveau, als op de informatie- en applicatielagen. Bijvoorbeeld een plotselinge verandering in quarantaineperiode vereist niet alleen wendbaarheid op het niveau van de IV, maar ook op grondslagen en organisatieniveau:

[3] Zie Bijlage 02 - Doelarchitectuur IV voor infectieziektebestrijding editie 2024Q1.pdf



De inhoud van de domeinarchitectuur IZB staat dus zeker niet op zichzelf en moet gekoppeld worden met gelijkluidende maatregelen op organisatorisch en wetgevend niveau.

Verantwoording van de werkwijze:

Om te komen tot een correcte en volledige set van inrichtingseisen / architectuurprincipes hanteren we twee invalshoeken:

Invalshoek 1: op basis van de acht NORA architectuurprincipes die genoemd worden in de doelarchitectuur, voorzien we de bij de architectuurprincipes behorende NORA implicaties van duiding en richting. In andere woorden: geredeneerd vanuit vigerende referentie documentatie beoordelen we de invloed daarvan op het nieuwe IV- landschap.

Invalshoek 2: op basis van de karakteristieke kenmerken van de IZB in Nederland formuleren we eigen architectuurprincipes en -implicaties die de eigenheid van het IZB-werkveld beschrijven en voorzien we deze van duiding en richting. In andere woorden: geredeneerd vanuit de bijzondere kenmerken van de infectieziektebestrijding in Nederland, beoordelen we de invloed ervan op de informatievoorziening.

Door de uitkomsten van beide invalshoeken te bekijken, ontdekken we waar er vanuit de referentiearchitecturen en ontwerpen nog onderwerpen missen. Dit zijn dan zaken die bij de aanbesteding van het IV-landschap extra aandacht nodig hebben.

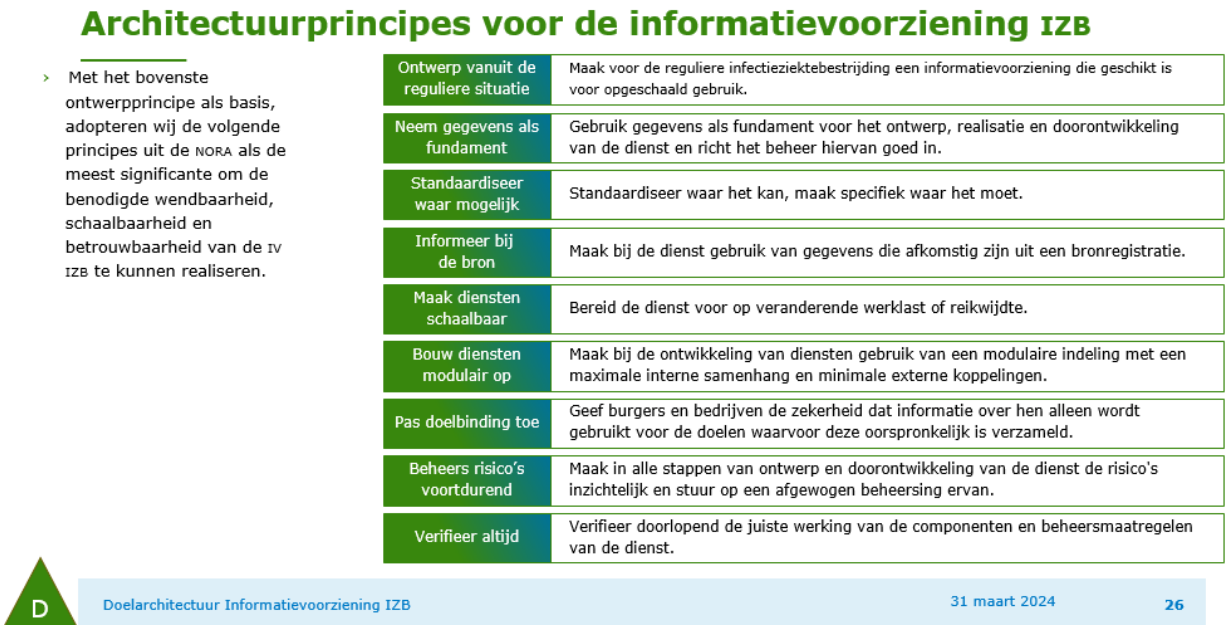
8.2.1 'Niet-functionele' functionaliteiten

Er zijn generieke functies te benoemen die niet direct uit een requirements analyse tevoorschijn zullen komen, omdat ze generiek van aard zijn. In het conceptueel ontwerp van de generieke infrastructuur, komen deze ook niet aan de orde omdat ze een functioneel karakter hebben. Er wordt daarom aandacht gevraagd voor het inventariseren van dit soort functies. Te denken valt aan:

- Printen
- Veilig mailen
- Randapparatuur (barcode scanners)
- PGO
- Toestemming register
- LSP-aansluiting

8.3 Uitwerking invalshoek 1 richtinggevende principes vanuit de doelarchitectuur

De doelarchitectuur typeert het pandemisch parate IZB IV-landschap dat moet voldoen aan de eisen van wendbaarheid, schaalbaarheid en betrouwbaarheid. Vanuit de doelarchitectuur zijn de volgende architectuurprincipes gegeven die de inrichting definiëren:



Hieronder worden de laatste 8 architectuurprincipes, die voortkomen uit de NORA verder uitgewerkt voor het IZB IV-landschap voor de GGD. De tabellen geven een overzicht van de implicaties van de bovengenoemde principes.

Per implicatie kijken we eerst of er nadere uitwerking nodig is voor het terrein van de infectieziektebestrijding, of dat de implicatie zelfevident is en geen verdere uitwerking nodig heeft om de gevolgen voor de domeinarchitectuur te begrijpen. De tabellen zijn doorklikbaar naar de NORA omschrijving.

8.3.1 Neem gegevens als fundament

ID	Implicatie	Beschreven in
IMP001	Beschrijf informatieobjecten in een model	8.3.1.1
IMP021	Bevorder hergebruik van gegevens	8.3.1.2
IMP049	Draag zorg voor juiste en actuele en volledige informatie	8.3.1.3
IMP044	Hanteer bewaartermijnen voor informatie	8.3.1.4
IMP051	Leg auditlogs vast bij de bronregistratie van het gegeven	x
IMP048	Leg de context van een informatieobject vast in metadata	x
IMP050	Maak gegevens herleidbaar tot de bron (herkomst)	8.3.1.5
IMP003	Maak zoveel mogelijk data beschikbaar als open data	x
IMP047	Pas de FAIR dataprincipes toe	8.3.1.6
IMP052	Sla informatie op in een duurzaam toegankelijk bestandsformaat	x
IMP073	Stel van ieder gegeven de kwaliteit vast	8.3.1.7
IMP058	Stel voor ieder gegeven de unieke bron vast	x
IMP046	Stel één verantwoordelijke vast voor ieder gegeven	x
IMP002	Voorkom verlies van informatie	x

8.3.1.1 IMP001 Beschrijf informatieobjecten in een model

Breng informatieobjecten onder in het IZB Domeinmodel. Zie ook 8.5.2. We publiceren het domeinmodel naar de buitenwereld.

8.3.1.2 IMP021Bevorder hergebruik van gegevens

De manier van hergebruik die in deze implicatie wordt beschreven vertaalt zich, conform de doelarchitectuur, in een federatief datacentrisch landschap. Het is goed denkbaar dat data deels bij het RIVM en deels bij de GGD'en opgeslagen staat, maar toch als één dataset wordt gepresenteerd.

8.3.1.3 IMP049 Draag zorg voor juiste en actuele en volledige informatie

Kernpunt bij het realiseren van deze implicatie is het federatieve karakter van de 25 GGD'en: we moeten de vraag beantwoorden bij wie de burger terecht kan voor correctie van geconstateerde fouten. Dit is een vraagstuk dat ook nadrukkelijk vraagt om organisatie. Uitgangspunt wordt, dat er een landelijke faciliteit ontstaat waar de burger (onder meer) geconstateerde fouten kan melden en inzage kan krijgen in de aard van de over hem opgeslagen gegevens.

8.3.1.4 IMP044 Hanteer bewaartermijnen voor informatie

De bewaartermijnen voor de verzamelde gegevens vallen deels onder het regime van de WPG en deels onder dat van de WGBO, met elk hun eigen bewaartermijnen. De koppeling tussen gegevens en de van toepassing zijnde wetgeving kan in de loop van de tijd variëren.

8.3.1.5 IMP050 Maak gegevens herleidbaar tot de bron (herkomst)

Het vastleggen van de bron van een gegeven moet een heldere vertaling krijgen naar een datacentrisch landschap. Waar voorheen RIVM een gegeven zou opslaan met als bron GGD, is in een datacentrisch landschap ditzelfde gegeven gedeeld. Dit betekent dat ofwel een ketenverantwoordelijkheid ontstaat om bij raadplegen de bron te verifiëren en zo nodig bij te werken, ofwel we de implementatie van deze implicatie

moeten oprekken door de systeemgrenzen om GGD'en en RIVM heen te trekken en deze beide als één en dezelfde bron te beschouwen. Deze laatste optie is wat automatisch zal gebeuren indien we hier geen speciale aandacht voor vragen, terwijl de vraag is of een dergelijke oplossing een privacy- en grondslagentoets kan doorstaan.

8.3.1.6 IMP047 Pas de FAIR dataprincipes toe

Vindbaarheid is een issue dat breed in de zorg speelt in het kader van datagedreven werken en data ophalen uit de bron. De nieuwe NEN7519 norm kan hierin een rol spelen. Het aandachtspunt is dat vindbaarheid niet alleen een rol speelt binnen de dataservice van het nieuwe IV-landschap, maar ook voor externe afnemers. De identificatie van gegevens en metadata moet hierop afgestemd zijn.

8.3.1.7 IMP073 Stel van ieder gegeven de kwaliteit vast

GGD: De 25 horizontale partities vormen tezamen de IZB-data van de GGD. Dit kan alleen als geheel gezien/gebruikt worden als de kwaliteit van ieder onderdeel op hetzelfde niveau is.
Dit vraagt dus om additionele maatregelen om de kwaliteit te kennen, verbeteren en borgen, bij voorkeur grotendeels geautomatiseerd in de applicatielaag.

8.3.2 Standaardiseer waar mogelijk

ID	Implicatie	Beschreven in
IMP034	Gebruik de standaard met het meest specifieke werkingsgebied	8.3.2.1
IMP035	Gebruik een actueel register met standaarden	8.3.2.2
IMP038	Gebruik gestandaardiseerde referentiedata	x
IMP075	Gebruik open standaarden voor modellering	x
IMP089	Gebruik standaard oplossingen (implicatie)	x
IMP025	Gebruik standaard oplossingen zonder maatwerk	x
IMP085	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	x
IMP076	Maak afspraken over nieuwe (en oude) versies van standaarden	x
IMP026	Pas je eigen proces en organisatie aan aan de standaard oplossing	8.3.2.3
IMP036	Pas open standaarden toe	x
IMP037	Pleeg onderhoud op de toegepaste standaarden	x

8.3.2.1 IMP034 Gebruik de standaard met het meest specifieke werkingsgebied

Wij leggen deze implicatie uit op laag 2-5 (Nora geeft 1 aan). Voorbeeld: benut internationale standaarden zoals Open EHR boven lokale of nationale standaarden voor de vastlegging van BCO, interventie, surveillance en vaccinatiedata.

8.3.2.2 IMP035 Gebruik een actueel register met standaarden

In een datacentrisch landschap zijn de meest relevante standaarden die op het gebied van data. Hierbij geldt, gegeven het concept van een koppelservice die conversies naar diverse uitwisselformaten verzorgt, dat het opslagformaat een centrale rol inneemt. Het informatiemodel dat onderdeel is van het domeinmodel zal naar verwachting in ieder geval voor de aan personen gekoppelde gegevens gebruik maken van OpenEHR.

8.3.2.3 *IMP026 Pas je eigen proces en organisatie aan aan de standaard oplossing*

Deze implicatie is in het licht van pandemische paraatheid triviaal: we eisen dat een eventueel standaardpakket wendbaar genoeg is voor een pandemische situatie, dit betekent tegelijkertijd dat zo'n pakket in staat is om zich te vormen naar de reguliere processen van de GGD'en. Als het nodig is om de processen en/of organisatie steeds aan te passen aan het standaardpakket, dan betekent dit automatisch dat zo'n pakket niet kan voldoen aan de wendbaarheidseisen.
Het kan natuurlijk wel zo zijn dat, ook in een pandemische situatie, bepaalde processtappen of stapvolgorden makkelijker, sneller of goedkoper te realiseren zijn dan functioneel vergelijkbare. In dit geval selecteren we de optie die het dichtst bij de door het pakket geboden standaardfunctionaliteit ligt. Standaardisatie en wendbaarheid hoeven elkaar in die zin niet uit te sluiten.

8.3.3 Informeer bij de bron

ID	Implicatie	Beschreven in
IMP060	Bepaal autorisaties met metadata	8.3.3.1
IMP021	Bevorder hergebruik van gegevens	x
IMP059	Geef de voorkeur aan halen i.p.v. brengen van gegevens	x
IMP055	Gegevens eenmalig uitgevraagd, uniek opgeslagen, meervoudig gebruikt	x
IMP033	Koppel bronsystemen op basis van een passende classificatie	x
IMP056	Registreer gegevens bij de bron	x
IMP077	Stel de juridische aansprakelijkheid per gegevensobject vast	x
IMP058	Stel voor ieder gegeven de unieke bron vast	x
IMP007	Verwijs naar de bron	8.3.3.2
IMP057	Weet welke (bron)gegevens in huis zijn	x

8.3.3.1 *IMP060 Bepaal autorisaties met metadata*

In een datacentrisch landschap betekent autorisatie allereerst het bepalen van toegang tot de data. Alle tussenliggende elementen (als userinterface en api's) kunnen rechten controleren, maar dan vooral in het kader van gebruiksvriendelijkheid, zodat een gebruiker alleen de voor hem relevante functionaliteit ziet en vroeg in een interactie terugkoppeling krijgt. De toegangscontrole op de data is essentieel omdat het pad tot de data niet bij voorbaat vaststaat.
De metadata waar hier over gesproken wordt is onlosmakelijk deel van het domeinmodel. Autorisatie wordt onder andere verleend op basis van de inhoud van gegevens. Dit heeft consequenties voor de manier waarop autorisaties worden vastgelegd (zie 8.5.5.2 Autorisatie), maar ook voor het mechanisme dat autorisatie controleert. Als voor het controleren van toegang tot een resource de inhoud van die resource bekend moet zijn, ontstaat een tweede authenticatie context (die van het controlerend mechanisme) die toegang moet hebben tot alle inhoud.

8.3.3.2 *IMP007 Verwijs naar de bron*

Er zijn twee manieren denkbaar waarop deze verwijzing vormgegeven kan worden:

- Tijdens toegang tot de dataservice lezen we, in de dataservice als onderdeel van de logica in de aangeroepen api, de gegevens bij waarnaar verwezen wordt;
- We retourneren als onderdeel van de dataset een verwijzing naar de brondata

8.3.4 Maak diensten schaalbaar

ID	Implicatie	Beschreven in
IMP085	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	x

8.3.5 Bouw diensten modulair op

ID	Implicatie	Beschreven in
NAP07.01	Diensten vullen elkaar aan (implicatie)	8.3.5.1
IMP033	Koppel bronsystemen op basis van een passende classificatie	x
IMP032	Ontwerp diensten met oog voor doelbinding en grondslag	x
IMP031	Ontwerp op modulaire wijze	8.3.5.2
IMP029	Scheid proces van data	x
IMP030	Scheiding van datasets	x
IMP087	Verwerk bericht-interactie persistent	x
IMP083	Wissel gegevens tussen (web)applicaties uit met API's	x
IMP039	Zorg voor open specificaties	x

8.3.5.1 NAP07.01 Diensten vullen elkaar aan (implicatie)

Voor burgers: Alle 25 GGD'en bieden dezelfde wettelijke diensten aan, verdeeld over Nederland. Deze situatie wordt ondersteund door één gemeenschappelijk IV-landschap.
De IV-oplossing maakt het voor afnemers volkomen duidelijk met welke onderliggende GGD men te maken heeft.
Note: een traject tussen GGD GHOR Nederland, RIVM en VWS (vervolg op ABCD-traject) zal hiervoor nadere richtlijnen geven.
Voor ketenpartners: Voor de communicatie met ketenpartners geldt dat zij 1 ingang hebben voor communicatie met "de GGD". Voorbeeld: ketenpartners hoeven dezelfde melding niet 2x aan te leveren, 1x bij de GGD en 1x bij het RIVM.
Note: Naar aanleiding van de geleerde lessen uit de recente COVID-19-pandemie lopen trajecten om enerzijds aanpassingen in de WPG door te voeren en anderzijds GGD GHOR Nederland een helder gedefinieerde rol binnen de IZB te geven. Deze trajecten zullen mogelijk veranderingen in de taken en processen opleveren.

8.3.5.2 IMP031 Ontwerp op modulaire wijze

De modulariteit in het IZB-systeem is onder meer gebaseerd op functionele blokken die in de domeinarchitectuur beschreven staan als procesbouwblok. Een procesbouwblok is een duidelijk afgekaderd deel van een bedrijfsproces, samen met de voor dat deel benodigde en/of geraakte gegevens. Deze procesbouwblokken zijn een essentieel mechanisme voor het realiseren van de kernwaarde wendbaarheid. In de reguliere fase bepalen de professionals van de GGD'en welke procesbouwblokken op welk moment uitgevoerd worden, bij een pandemische fase wordt de besturing van de pandemische processen in al zijn facetten bepaald vanuit het LFI, waarbij ook niet-geschoold personeel ingezet kan worden op afgebakende procesbouwblokken en meer gestuurd wordt op het zo effectief mogelijk afhandelen van grote aantallen. Deze variatie tussen vrijheid en procesgestuurd werken staat verder uitgewerkt in paragraaf 8.5.4.

8.3.6 Mapping naar de IV voor de GGD-en

De overlappende implicaties zijn:

IMP021	Bevorder hergebruik van gegevens
IMP033	Koppel bronsystemen op basis van een passende classificatie
IMP058	Stel voor ieder gegeven de unieke bron vast
IMP085	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS

Deze zijn hier weergegeven omdat ze vanuit meerdere principes naar voren komen en vanuit verder ontwerp dus extra aandacht behoeven. Implicaties IMP021, IMP033 en IMP058 behandelen een beschrijvend niveau over bronnen en gegevens en zijn uitstekend in te vullen met een metamodel, zoals dat bij het toepassen van domeinmodel ook voorzien is.
IMP085 leidt tot een gunningscriterium dat met name voor het technische IV-platform geldt.

8.3.7 Pas doelbinding toe

Karakter en aard van de data van de GGD'en is zodanig, dat data-aanvragen door externe partijen, als bijvoorbeeld het CBS, zorgvuldig beoordeeld moeten worden op rechtmatigheid. Dit betekent dat we van alle opgeslagen data (in de metadata) de grondslag moeten weten en dat dataleveringen door de GGD'en/GGD GHOR Nederland moeten worden geregistreerd, inclusief de afwegingen en wettelijke grondslagen op basis waarvan de levering werd toegestaan en de partij(en) aan wie geleverd werd.

ID	Implicatie	Beschreven in
IMP045	Leg de doelbinding vast in de metadata van het gegevensobject	
IMP054	Leg de grondslag en het doel van de gegevensverwerking vast	
IMP004	Minimaliseer het gebruik van gegevens	
IMP022	Neem oorspronkelijke grondslag mee bij hergebruik diensten	
IMP032	Ontwerp diensten met oog voor doelbinding en grondslag	
IMP053	Stel betrokkenen op de hoogte van het doel waarvoor gegevens verzameld worden	
IMP077	Stel de juridische aansprakelijkheid per gegevensobject vast	

(deze implicaties worden nader uitgewerkt in een volgende versie)

8.3.8 Beheers risico's voortdurend

De wettelijke taken van de GGD betekenen een grote, ook operationele, verantwoordelijkheid in de publieke gezondheid in Nederland. Elke vorm van falen heeft daarmee in potentie grote gevolgen op regionaal en zelfs landelijk niveau. Het is daarom van groot belang om risico's, ook op het gebied van IV, te onderkennen en mitigeren.

ID	Implicatie	Beschreven in
IMP063	Bepaal de continuïteitseisen	
IMP078	Bewaak de continuïteit en stel een calamiteitenplan op	
IMP081	Borg de vertrouwelijkheid van gegevens in maatregelen	
IMP080	Controleer de verwerking van gegevens	
IMP062	Evalueer de risicoanalyse bij veranderingen	

IMP079	Garandeer de beschikbaarheid van systemen	
IMP085	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	
IMP015	Maak beveiligingsmaatregelen zo gebruiksvriendelijk mogelijk	
IMP061	Reduceer rest-risico's	
IMP070	Segmenteer het netwerk	
IMP064	Stel onweerlegbaarheid vast	
IMP084	Versleutel gegevens in rust en transport	
IMP086	Zorg dat software up-to-date is	

(deze implicaties worden nader uitgewerkt in een volgende versie)

8.3.9 Verifieer altijd

Continuïteit is een belangrijke pijler onder de publieke gezondheid en daarmee ook onder de IV van de GGD'en.

ID	Implicatie	Beschreven in
IMP069	Hanteer het zero-trust model	
IMP019	Maak stelselafspraken over identificatie en authenticatie	
IMP068	Maak toegang tot applicaties en gegevens afhankelijk van authenticatieniveau	
IMP066	Richt een sterke logging en audit-trail in	
IMP070	Segmenteer het netwerk	
IMP064	Stel onweerlegbaarheid vast	
IMP065	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces	
IMP067	Verifieer de werking van algoritmes	
IMP088	Verleen alleen strikt noodzakelijke toegangsrechten	

(deze implicaties worden nader uitgewerkt in een volgende versie)

8.4 Tweede invalshoek: aanvullende architectuurprincipes

Het domein van de infectieziektebestrijding kent een aantal onderscheidende karakteristieken. Deze worden als IZB specifieke architectuurprincipes in dit hoofdstuk verder uitgewerkt.

8.4.1 KAR1 - Regulier vs. Pandemisch ondersteunen

Een belangrijk aspect van de nieuwe informatievoorziening voor de IZB binnen de GGD is dat deze zowel in de reguliere als in een pandemische situatie moet functioneren.

ID	Implicatie	Beschreven in
AIMP01	Het IV-landschap is aantoonbaar wendbaar	8.5.4
AIMP02	Het IV-landschap is aantoonbaar schaalbaar	8.5.3
AIMP03	Het IV-landschap is aantoonbaar betrouwbaar	

8.4.2 KAR2 – Generieke versus specifieke werkwijzen

Zoals al beschreven in 6.1.2 is de werkwijze van de GGD sterk geprotocolleerd; de LCI-richtlijnen beschrijven, per infectieziekte, welk protocol toegepast dient te worden. Ondanks de strakke protocollering zijn er toch nuance- c.q. interpretatieverschillen per GGD.

ID	Implicatie	Beschreven in
AIMP04	De nieuwe IV implementeert de LCI-richtlijnen	8.4.2.1
AIMP05	De nieuwe IV implementeert de meldingsplicht vastgelegd in de Wet publieke gezondheid.	8.4.2.2
AIMP01	Het IV-landschap is aantoonbaar wendbaar	8.5.4

8.4.2.1 De nieuwe IV implementeert de LCI-richtlijnen

De nieuwe informatievoorziening is in staat de LCI-richtlijnen te implementeren.

Dit houdt in dat er een proces is om de wijzigingen in de LCI-richtlijnen op te nemen in het GGD domeinmodel van de IZB én een proces waarin deze wijzigingen vervolgens (bij voorkeur geautomatiseerd) door medewerkers van GGD GHOR Nederland kunnen worden doorgevoerd in het informatiemodel en de opbouw van de procesbouwblokken.

8.4.2.2 De nieuwe IV implementeert de meldingsplicht vastgelegd in de Wet publieke gezondheid

De nieuwe informatievoorziening ontvangt en verstuurt meldingen zoals vastgelegd in de WPG.

Einddoel is om te komen tot één datacentrisch IV-landschap waarin data niet meer gekopieerd wordt. Het is de verwachting dat het voorlopig nog noodzakelijk blijft om meldingsdata geautomatiseerd door te sturen naar het RIVM (ic Osiris). Dit betekent ook dat tijdens verheffingen, endemische of pandemische situaties de meldingenstroom moet doorlopen. M.a.w. de schaalbaarheidseis geldt nadrukkelijk ook hiervoor. Anders uitgedrukt:

De nieuwe informatievoorziening is nooit de bottleneck in de meldingsketen.

8.4.3 KAR3 - Infectieziekten zijn grensoverschrijdend

De GGD'en die een grens delen met één van de buurlanden, of die gesitueerd zijn in een gebied met (lucht)havens of asielcentra, en als gevolg daarvan te maken hebben met instroom en uitstroom naar buitenlandse gebieden, richten hun processen (denk met name aan melden/signaal ontvangen, BCO en surveillance) in op een bredere scope dan alleen de eigen regio. Dit gaat verder dan bovenregionale samenwerking. Voor wat betreft de officiële procesgang rond melden en surveillance: deze zijn voorzien in (internationale) wetgeving. Wat hier van belang is, is de flexibiliteit om in de lokale processen/processtappen de mogelijkheid in te bouwen tot informeel contact met de buurregio's.

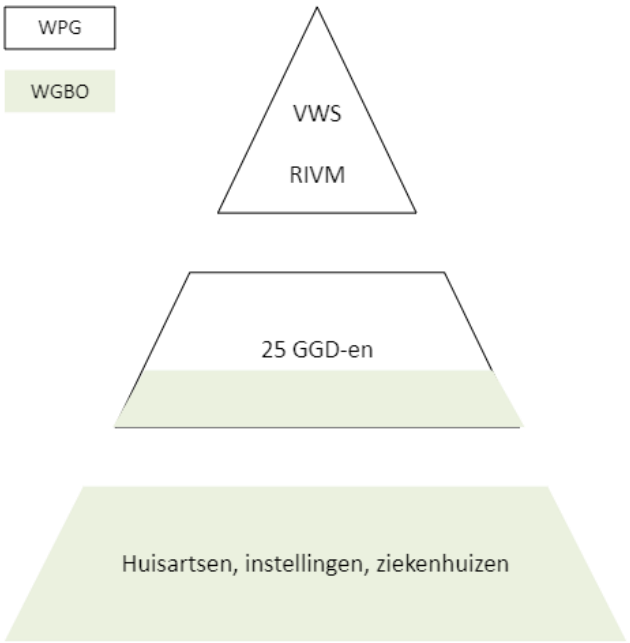
ID	Implicatie	Beschreven in
AIMP01	Het IV-landschap is aantoonbaar wendbaar	8.5.4

AIMP05	De nieuwe IV implementeert de meldingsplicht vastgelegd in de Wet publieke gezondheid.	8.4.2.2

8.4.4 KAR4 - De GGD dataset bevat medische gegevens

Infectieziektebestrijding binnen de GGD is in zekere zin een balanceeract tussen twee wettelijke grondslagen: de Wet publieke gezondheid en de Wet geneeskundige behandelovereenkomst. Hoewel dat bij het uitvoeren van een wettelijke taak wel vaker het geval is, zijn deze twee grondslagen dermate tegenstrijdig van karakter dat bij het vastleggen van gegevens en het delen ervan, zeer zorgvuldig moet worden geregistreerd onder welke grondslag de vastlegging (of deling) gebeurt. Data onder de WGBO valt onder medisch beroepsgeheim, en heeft een andere retentietermijn dan data onder de Wpg.

De scheidslijn tussen WPG en WGBO heeft te maken met het al dan niet bestaan van een behandelrelatie tussen professional en patiënt. Een behandelrelatie valt onder de WGBO. De werkzaamheden van een GGD-arts kunnen soms het karakter hebben van een behandelrelatie en daarmee dus onder de WGBO vallen. Dit is in die zin problematisch, dat de WGBO zich focust op de geheimhoudingsplicht van de arts en dat de Wpg met name gericht is op informatiedeling in de keten. Daardoor moet er binnen de scope van de IV dus een duidelijk en afgedwongen onderscheid mogelijk zijn tussen data die tot stand komt in het kader van een behandelrelatie, en data die vallen onder de algemene infectieziektebestrijding.
De overgang van WGBO naar WPG is in de keten uniek voor de GGD'en[4], dit is weergegeven in onderstaande informatiepiramide, waarin de hoogte de reikwijdte van overzicht weergeeft en de breedte het detailniveau van persoonsgegevens.



Dit alles leidt tot een aantal IZB specifieke implicaties:

ID	Implicatie	Beschreven in
AIMP06	Een professional maakt aan de IV duidelijk of er een behandelrelatie gaande is	8.4.4.1
AIMP07	De retentietermijn van gegevens volgt de wettelijke grondslag	8.4.4.2

[4] Het RIVM slaat wel WGBO gebonden gegevens op, maar als afgebakende uitzondering

AIMP08	De grondslag van gegevens kan wijzigen	8.4.4.3

8.4.4.1 Een professional maakt aan de IV duidelijk of er een behandelrelatie is

Een professional moet de mogelijkheid krijgen om onweerlegbaar vast te leggen dat het systeem gebruikt wordt in het kader van een behandelrelatie.

In de meeste gevallen volgt dit uit de bouwblokken, maar er zijn situaties waar handmatige markering noodzakelijk is. Vanaf dat moment markeert het systeem alle nieuw ingevoerde of gewijzigde gegevens onder de grondslag WGBO en behandelt ze als medisch beroepsgeheim.

8.4.4.2 De retentietermijn van gegevens volgt de wettelijke grondslag

Voor persoonsgebonden gegevens is de retentietermijn geen statisch geconfigureerd metagegeven, maar volgt de wettelijke grondslag.

Daarbij geldt, dat een deel van de gegevens (met name de NAW-gegevens) pas verwijderd kan worden als er geen andere gekoppelde gegevens meer zijn.

8.4.4.3 De grondslag van gegevens kan wijzigen

Tijdens ontwerp van de gegevensmodellen, moet terdege rekening gehouden worden met het feit dat het ontstaan van een behandelrelatie de wettelijke grondslag van een gegeven kan wijzigen. Daarnaast kan de grondslag voor specifieke informatieobjecten in de loop van de tijd wijzigen, bijvoorbeeld door een wetswijziging. Dit kan extra maatregelen vergen met betrekking tot het waarborgen van integriteit en consistentie, omdat een concept als dossier heel goed voor een deel onder WGBO en de rest onder WPG kan vallen.

De grondslag van een gegeven kan veranderen

En

één concept kan onder verschillende grondslagen vallen.

8.4.5 KAR5 – De IZB in Nederland is federatief

Zoals beschreven in 6.1.4 wordt de wettelijke taak van de GGD uitgevoerd door 25 onafhankelijke organisaties. Dit betekent dan ook dat de nieuwe informatievoorziening federatief van karakter moet zijn, zowel in gegevens, procedures, als autorisaties: iedere GGD is verantwoordelijk voor het eigen deel, maar de wettelijke taak moet in gezamenlijkheid uitgevoerd worden. Tot die wettelijke taak behoort ook een ketensamenwerking met het RIVM. Dit heeft een aantal consequenties voor de informatievoorziening:

ID	Implicatie	Beschreven in
AIMP01	Het IV-landschap is aantoonbaar wendbaar	8.5.4
AIMP04	De nieuwe IV implementeert de LCI-richtlijnen	8.4.2.1

AIMP05	De nieuwe IV implementeert de meldingsplicht vastgelegd in de Wet publieke gezondheid.	8.4.2.2
AIMP09	De nieuwe IV bevat 25 datasets, die zich gedragen als één.	6.1.4
AIMP10	Authenticatie en autorisatie zijn federatief	8.4.5.1

8.4.5.1 Authenticatie en autorisatie zijn federatief

Het is nadrukkelijk de bedoeling dat de 25 GGD'en zelfstandig zijn en blijven. Dit betekent ook dat de verantwoordelijkheid voor identity provisioning en aanlog-, step-up en uitlog-processen van gebruikers die voor of namens die GGD werken nadrukkelijk bij de lokale GGD ligt.

Toegang tot bronnen bij andere GGD'en of ketenpartners vindt plaats via een federatief stelsel

8.5 Ontwerpprincipes

8.5.1 Datacentrisch

Een belangrijke les uit de coronaperiode was dat het te veel moeite kostte om, vanuit de verschillende registraties van de GGD'en, één gemeenschappelijk beeld te vormen. Dit had twee oorzaken: ten eerste waren de registraties gescheiden, waardoor er kopieer- en interpretatieslagen nodig waren om ze bij elkaar te brengen. Ten tweede lag de betekenis van de gegevens die gekopieerd werden niet vast, waardoor inconsistenties ontstonden bij het combineren van de datasets. Tot slot waren de datastructuren met name opgezet om functionaliteit te ondersteunen en waren ze in hun aard minder geschikt voor structurele data-uitwisseling.
Deze problemen kunnen, en zullen, in de nieuwe informatievoorziening voor de IZB voorkomen worden, door data in het landschap als first class citizen te behandelen en niet langer als silo die zich achter een applicatie ophoudt. We noemen dit een datacentrisch landschap. Data staat centraal; alle andere componenten van het landschap zijn slechts een manier om data te ontsluiten naar gebruiker en/of externe partner.
Dit betekent ook dat de Data Services, verantwoordelijk voor de opslag en toegang tot de gegevens van de GGD'en, autonoom zijn in functionaliteit rond auditing, semantische beschrijving, datakwaliteit en integriteit, toegangsverlening en privacyaspecten als doelbinding en BIV-classificatie.
Datacentrisch betekent dat alle data in het landschap zich als één logische gegevensverzameling gedragen. Deze gegevensverzameling is uit de aard der zaak federatief, daar de GGD'en zelfstandige entiteiten zijn en elk van de 25 GGD'en eigenaar is en blijft van haar data.
Datacentrisch werken leidt daarmee tot een aantal architectuurprincipes.

Data wordt opgehaald bij de bron

Als we vermijden om data te kopiëren, heeft dat als consequentie dat we de data altijd ophalen daar waar de authentieke registratie plaatsvindt. Dit principe hanteren we voor alle gegevens, dus ook voor externe bronnen.

De dataservice binnen de nieuwe IV-voorziening is federatief

Alle GGD'en moeten volledige autonomie blijven houden over hun eigen gegevens. Bovendien willen we kopiëren zoveel mogelijk voorkomen. Dit leidt tot één logische gegevensverzameling met divers eigenaarschap. Dit laat onverlet dat technische oplossingen als caching wellicht nodig zullen zijn om aan performance requirements te voldoen. Ongeacht daarvan mag er nooit een discrepantie ontstaan tussen de informatie uit de bron en de informatie die de dataservice aan de gebruiker levert.

Data is zelfbeschrijvend

We stellen hoge eisen aan het vastleggen van metagegevens als doelbinding, autorisatieregels en betekenis. Dit is essentieel om te voldoen aan de eis van autonomie van de dataservice; deze kan alleen op de juiste wijze toegang verlenen indien ook per informatieobject vastligt wie, onder welke voorwaarden en voor welke procesbouwblok dat informatieobject mag benaderen. De dataservice kan alleen een integere logisch gecentraliseerde gegevensverzameling opbouwen, indien hij ook de beschikking heeft over afdoende beschrijvende metagegevens die voorkomen dat ongelijksoortige informatieobjecten met elkaar worden gecombineerd tot één set.

Alle mutaties worden vastgelegd

Alle mutaties worden vastgelegd en bewaard (audit trail), zodat op elk moment kan worden geanalyseerd wie welke wijzigingen (of andersoortige toegang) heeft aangebracht. Dit is niet alleen van belang voor CISO-doeleinden, maar ook voor secundair gebruik.

8.5.2 Domeinmodel

Om eenheid van taal en begrip te kunnen (blijven) garanderen is in de doelarchitectuur het domeinmodel geïntroduceerd. Het domeinmodel is een samenhangende set modellen (van onder andere processen, autorisatie, informatie) waarin samen met professionals het domein van de IZB is beschreven. Een nadere uitwerking hiervan is te vinden in Bijlage 12 – Domeinmodelleren.

8.5.2.1 Metadata

Een algemeen geaccepteerde definitie van metadata is: *Metadata is data die andere data beschrijft*. In die zin bevat het domeinmodel dus metadata op verschillende niveaus. Een gangbaar onderscheid in de soorten metadata is de volgende:

- Beschrijvende metadata: Dit type metadata biedt gedetailleerde informatie over de inhoud van een digitaal item, zoals de titel, de maker, de datum van creatie en het onderwerp. Deze informatie helpt gebruikers om de context en het belang van het item te begrijpen en het gemakkelijk te vinden en terug te vinden.
- Technische metadata: Dit type metadata beschrijft de technische specificaties van een digitaal asset, zoals het bestandsformaat, de grootte, de resolutie en de kleurdiepte. Deze informatie is belangrijk om ervoor te zorgen dat het bedrijfsmiddel effectief kan worden geopend en gebruikt door verschillende systemen en apparaten.
- Structurele metadata: Dit type metadata definieert de structuur en organisatie van een digitaal item, zoals de hiërarchische relaties tussen verschillende delen van het item of de verbanden tussen verschillende items. Deze informatie helpt gebruikers om op een zinvolle manier door het item te navigeren en ermee om te gaan.
- Administratieve metadata: Dit type metadata biedt informatie over het beheer en de retentie van een digitaal item, zoals de auteursrechtelijke status, toegangsbeperkingen en retentieplannen. Deze informatie is belangrijk om ervoor te zorgen dat het item in de loop van de tijd goed wordt beschermd en onderhouden.
- Metagegevens van rechten: Dit type metagegevens definieert de rechten en machtigingen die zijn gekoppeld aan een digitaal item, zoals wie het recht heeft om het asset te gebruiken, hoe ze het kunnen gebruiken en wanneer ze het kunnen gebruiken. Deze informatie is belangrijk om ervoor te zorgen dat het op een legale en ethische manier wordt gebruikt.
- Statistische metadata: Dit type metadata geeft informatie over andere gegevens. Het kan details bevatten zoals de bron van de gegevens, de datum waarop deze zijn verzameld, de methode van verzameling en alle relevante opmerkingen of opmerkingen over de gegevens. Deze informatie helpt om de gegevens op een zinvollere manier te begrijpen en te interpreteren, en kan ook helpen om de betrouwbaarheid en nauwkeurigheid van de gegevens te waarborgen. Statistische metadata wordt

vaak gebruikt in onderzoek en data-analyse en kan nuttig zijn voor het volgen en managen van een item gedurende een tijdsspanne.

In het kader van pandemische paraatheid, waar begrip van data uit voorheen onbekende bronnen, zowel op syntactisch als op semantisch gebied, van cruciaal belang is, is echter een sterkere definitie van metadata nodig:

Metadata is data die andere data beschrijft én zichzelf

In andere woorden: het domeinmodel (daar waar de metadata wordt vastgelegd) is ontologisch compleet; alle concepten en attributen aanwezig in het domeinmodel worden in datzelfde domeinmodel gerelateerd en beschreven. Het doel van deze manier van beschrijven kan het best geformuleerd worden als de volgende eis:

Nieuwe ketenpartners hebben voor gegevensuitwisseling met de GGD'en genoeg aan het domeinmodel

De metadata, die de GGD-data beschrijft, is beschrijvend genoeg om de structuur en inhoud van de GGD data te begrijpen zonder tussenkomst van een GGD-medewerker. Daarmee wordt een belangrijk pandemisch struikelblok weggenomen: begrip van data ontstaat niet langer ter plekke in overlegvorm, maar ligt formeel vastgelegd in het domeinmodel. Het domeinmodel heeft daarmee het karakter van een knowledge graph.

Het GGD-domeinmodel van de IZB is een knowledge graph waarvan de betekenis vastligt in een ontologie.

8.5.3 Schaalbaarheid

Schaalbaarheid is het vermogen van een systeem om snel te reageren op veranderende werklast.

Eén van de succesfactoren voor infectieziektebestrijding is de snelheid waarmee de informatievoorziening een verheffing kan volgen. Tijdens de coronaperiode werd duidelijk dat het huidige landschap daar niet toe in staat was. Het LFI heeft daarom richtlijnen gesteld aan onder andere de schaalbaarheid van de IV van ketenpartners in de publieke gezondheid. We nemen deze (uiteraard) over, maar zullen in de loop van het ontwerptraject een nadere analyse moeten maken hoe deze eisen uiteenvallen in requirements voor de diverse componenten van het IV-landschap van de GGD'en. Dit is een proces dat op dit moment loopt (tussen LFI en de diverse partners in de PG keten).

Het IV-landschap moet in staat zijn te schalen

8.5.3.1 Schaalbaarheid versus betrouwbaarheid

Infectieziektebestrijding (IZB) in een pandemische situatie vereist een zorgvuldige afweging van verschillende concepten en principes. Eén van de uitdagingen in dit domein is het vinden van de juiste balans tussen betrouwbaarheid en schaalbaarheid. Betrouwbaarheid in de context van IZB verwijst onder andere naar de kwaliteit, integriteit en actualiteit van gegevens, terwijl schaalbaarheid betrekking heeft op het vermogen om de systemen en processen aan te passen aan de snel veranderende en groeiende vraag tijdens een pandemie. Deze twee concepten kunnen echter met elkaar in conflict komen, met name wanneer gangbare applicatiearchitecturen worden toegepast, zoals event sourcing en CQRS, die streven naar eventuele consistentie.

Infectieziektebestrijding vereist nauwkeurige en actuele gegevens om effectieve besluitvorming te ondersteunen. Betrouwbaarheid in dit verband betekent dat de gegevens consistent en accuraat moeten zijn. Het gaat niet alleen om de integriteit van gegevens, maar ook om de garantie dat de informatie die wordt gebruikt voor epidemiologische analyse en besluitvorming up-to-date en betrouwbaar is.

De betrouwbaarheid in IZB komt tot uiting in verschillende aspecten:

Datakwaliteit: De gegevens die worden verzameld, moeten van hoge kwaliteit zijn en vrij zijn van fouten. Foutieve gegevens kunnen leiden tot misleidende analyses en besluitvorming.
Data-integriteit: Het is van cruciaal belang dat gegevens niet worden gemanipuleerd of gecorrumpeerd. Data-integriteit garandeert dat de gegevens die worden gebruikt voor epidemiologische rapporten en modellering betrouwbaar zijn.
Actualiteit: In IZB is tijd van essentieel belang. Verouderde gegevens kunnen leiden tot vertragingen in de reactie op een pandemie. Betrouwbare gegevens moeten actueel zijn om effectieve besluitvorming te ondersteunen.

Aan de andere kant van het spectrum staat schaalbaarheid. Tijdens een pandemie kan de vraag naar informatie en diensten exponentieel toenemen. Schaalbaarheid is het vermogen om deze groeiende vraag aan te kunnen zonder dat de prestaties van het systeem in gevaar komen. Dit vereist vaak geavanceerde architecturale benaderingen, zoals bijvoorbeeld event sourcing en CQRS, die het mogelijk maken om de staat van het systeem op elk moment te reconstrueren door de gebeurtenissen opnieuw af te spelen, maar die ook kunnen leiden tot inconsistentie van delen van het systeem.
Een kernprincipe van deze benadering is immers eventual consistency, wat betekent dat het systeem uiteindelijk naar een consistente staat evolueert nadat een gebeurtenis is verwerkt. Dit betekent dat er een periode van tijd kan zijn waarin verschillende delen van het systeem verschillende gegevens tonen. In de context van IZB kan dit een risico met zich meebrengen.
Om de uitdaging van betrouwbaarheid versus schaalbaarheid aan te pakken, kunnen hybride architecturen worden overwogen. Deze benadering combineert elementen van event sourcing en CQRS met traditionelere dataconsistentiemethoden om betrouwbaarheid te waarborgen.
In een hybride architectuur kunnen cruciale gegevenspunten worden geïdentificeerd waarbij absolute consistentie vereist is. Deze gegevenspunten kunnen worden beheerd met behulp van traditionele databasesystemen die sterke consistentie bieden, terwijl minder kritieke gegevens eventueel consistent kunnen worden gehouden via event sourcing.

8.5.4 Wendbaarheid

Eén van de kernbegrippen die de nieuwe IV voor infectieziektebestrijding beschrijven is *wendbaarheid*. Het is een eis dat de nieuwe IV niet alleen de veranderde schaalgrootte tijdens een nieuwe pandemie kan doorstaan, maar ons ook in staat stelt om meer actoren toe te voegen aan bedrijfsprocessen, de stapvolgorde van processen te wijzigen en/of nieuwe processtappen of zelf processen toe te voegen, andere data en/of datastromen te introduceren en het autorisatielandschap te laten meebewegen met data, actoren en processtappen.

8.5.4.1 Procesbouwblokken

Een belangrijk onderdeel in het domeinmodel is het zogenaamde procesbouwblok. Een procesbouwblok koppelt de actie die een gebruiker wil uitvoeren aan de inkomende en uitgaande informatie. Een procesbouwblok is synoniem voor een transactie binnen de DEMO methodologie. De formele definitie van een procesbouwblok is te vinden in het woordenboek domeinmodelleren. Een belangrijke karakteristiek van wendbaarheid in de nieuwe IV is dat de (in de regel hoog opgeleide) professional in een reguliere situatie in grote mate vrij is om op eigen initiatief procesbouwblokken te starten en/of te vervolgen, maar dat naar mate

een uitbraak zich verheft, werk verdeeld wordt en ook wordt uitgevoerd door minder opgeleid personeel, waardoor meer en meer processturing plaatsvindt, waarbij het systeem feitelijk bepaalt welk procesbouwblok de professional wanneer dient uit te voeren.

8.5.4.2 Kenmerken van wendbaarheid

Net als schaalbaarheid, kenmerkt wendbaarheid zich doordat er ten opzichte van de reguliere situatie in het geval van verheffing, endemie of pandemie iets extra's gevraagd wordt van de IV-voorziening. Waar dat bij schaalbaarheid vooral gaat over grootte (transactievolumes, concurrent users, aantallen datastromen, etc.) wordt er in het kader van wendbaarheid daadwerkelijk een verandering in gedrag gevraagd van de IV-voorziening.

8.5.4.2.1 Dimensies

Vooralsnog voorzien we drie dimensies waarin wendbaarheid zich manifesteert:

1. Verandering op procesniveau;
2. Verandering aan datastromen en/of datastructuur;
3. Verandering in autorisatiestructuur.

Dit hoofdstuk geeft duiding aan hoe deze verandering eruitziet en welke eisen dit met zich meebrengt voor de IV-voorziening (en daarmee het PvE).

8.5.4.3 Procesniveau

Om de invloed op procesniveau te duiden, classificeren we wendbaarheid in vier gradaties:

- Meer gebruikers: dat wil zeggen dezelfde professionals, maar meer
- Meer of andere actoren
- Gewijzigde stapvolgorde
- Nieuwe processen en/of processtappen

8.5.4.3.1 Meer gebruikers

De eerste dimensie waarin we de IV-voorziening zullen zien veranderen van gedrag is het toelaten van veel meer gebruikers. Feitelijk is dit gewoon schaalbaarheid (zie 8.5.3). Een aandachtspunt is testbaarheid[5]: bij elke nieuwe versie moet aangetoond kunnen worden dat de schaalbaarheid die nodig is voor pandemische paraatheid ook daadwerkelijk kan worden gerealiseerd.

8.5.4.3.2 Meer of andere actoren

Het gaat hier niet om meer gebruikers van ongewijzigde functionaliteit, maar om processen die voorheen door één actor werden uitgevoerd en nu door meerdere actoren. Dat kan zowel zijn vanuit een gewijzigde rolverdeling binnen de bestaande organisatie met als doel een (tijdelijk) efficiëntere werkverdeling, of het 'invliegen' van tijdelijke krachten die, met beperkte rechten, één of enkele processtap(pen) uitvoeren.
In dit geval vragen we van de IV-voorziening een mogelijkheid om werk, dat voorheen door één persoon werd uitgevoerd, nu te verdelen over meerdere medewerkers. Hier doorheen gloort dan meteen een workflow-achtige capability, namelijk werkverdeling en het dynamisch kunnen decomponeren van procesflows.

8.5.4.3.2.1 Eisen aan de IV

Er is een Workflow-achtige capability

[5] bijvoorbeeld in relatie tot de beperkte beschikbaarheid van test-DigiD accounts.

(lees: werkverdeling en decomponeren van flows)

Autorisatie volgt de benodigde autorisatieregels per processtap

wanneer taken gesplitst worden over verschillende actoren, ontstaat daarmee ook een dynamiek in autorisatie. Een gebruiker mag niet meer rechten toebedeeld krijgen, dan noodzakelijk. En wanneer er specialisatie plaatsvindt, waarbij de ene actor de ene processtap uitvoert en de andere actor een andere (waar beiden voorheen de hele flow uitvoerden), dienen hun rechten beperkt te worden tot de uit te voeren stappen. Dit heeft consequenties voor de onderliggende IAM dienst.

8.5.4.3.2.2 Aandachtspunten

- Testbaarheid
- Workflow dynamiek
- Autorisatie
- IAM-processen (dynamiek van)

8.5.4.3.3 Gewijzigde stapvolgorde

Een verdere dimensie aan wendbaarheid kan zijn om, hetzij vanuit protocolvoorschrift, hetzij vanuit doorlooptijdreductie, stappenvolgorde te wijzigen, bijvoorbeeld door de ene stap niet langer te laten wachten op uitkomsten uit de andere, door verschillende stappen parallel te nemen of door activiteiten in een geheel andere volgorde uit te voeren.
Het (bijvoorbeeld in een pandemische situatie) uitbesteden van (een deel van) bron- en/of contactonderzoek aan een andere partij, of door middel van gedigitaliseerde vragenlijsten, is hier een voorbeeld van.

8.5.4.3.3.1 Eisen aan de IV

- Workflow management-achtige capability (lees: dynamisch herschikken van processen en processtappen)

8.5.4.3.3.2 Aandachtspunten

- Testbaarheid
- Workflow dynamiek
- Autorisatie
- IAM-processen (dynamiek van)

8.5.4.3.4 Nieuwe processen en/of processtappen

Omdat de wereld van infectieziektebestrijding altijd voorbereid moet zijn op de uitbraak van een tot nu toe onbekende infectieziekte, is er geen uitputtende opsomming te maken van maatregelen en protocollen. Dit betekent dat er ook geen garantie kan zijn dat de processen die we nu analyseren toereikend zijn voor de infectieziektebestrijding van de toekomst. Met andere woorden, een nieuwe informatievoorziening voor de infectieziektebestrijding zal voorbereid moeten zijn op het introduceren van volledig andere processtappen, of zelfs processen.

8.5.4.3.5 Eisen aan de IV

Workflow management-achtige capability waarbij workflows eenvoudig en snel aan te passen zijn.

(lees: snel aanbrengen van nieuwe processtappen en processen)

De autorisatiestructuur moet fluïde genoeg zijn

om nieuwe processen en daarbij behorende autorisatieregels aan te leggen en activeren.

8.5.4.3.6 Aandachtspunten

- Testbaarheid
- Workflow dynamiek
- Autorisatie
- IAM-processen (dynamiek van)

8.5.4.4 Leerbaarheid

Een algemeen aandachtspunt voor wendbaarheid op procesniveau is dat, wanneer er nieuwe actoren, nieuwe processtappen en/of volgordes geïntroduceerd worden, inleertijd een cruciale rol speelt. Zeker in een opgeschaalde situatie moet de user experience zodanig ingericht zijn dat de gebruiker snel up and running is. Zeker wanneer sprake is van de inzet van niet-medisch geschoold personeel, is het van wezenlijk belang dat de user interface zodanig duidelijk en dwingend is dat de betrouwbaarheid van invoer geborgd wordt.

8.5.4.4.1 Eisen aan de IV

De inleertijd voor nieuwe functionaliteit zal verifieerbaar kort zijn

8.5.4.5 Dataniveau

In de moderne wereld wordt de strijd tegen infectieziekten steeds meer beïnvloed door geavanceerde data-analyse en informatietechnologie. Het vermogen om snel te reageren op veranderende gegevensbehoeften en -vereisten wordt cruciaal voor effectieve infectieziektebestrijding. Binnen een datacentrisch landschap voor de Infectieziektebestrijding (IZB) worden drie niveaus van datawendbaarheid geïdentificeerd:

- meer gegevens en/of datastromen
- nieuwe attributen en/of entiteiten
- en nieuwe soorten metadata.

In deze tekst zullen we deze drie niveaus van datawendbaarheid in detail bespreken, waarbij we benadrukken dat het laatste niveau, nieuwe soorten metadata, momenteel niet wordt verwacht binnen het huidige IZB-kader.

8.5.4.5.1 Niveau 1: Meer soorten gegevens en/of datastromen

Het eerste niveau van datawendbaarheid binnen het IZB-systeem omvat het vermogen om meer soorten gegevens en/of datastromen te integreren. Dit houdt in dat GGD'en in staat moeten zijn om de omvang en diversiteit van de verzamelde gegevens uit te breiden. Hierdoor kunnen ze beter inzicht krijgen in de verspreiding van infectieziekten, trends analyseren en tijdig reageren op uitbraken.
De integratie van nieuwe gegevensbronnen kan van vitaal belang zijn voor infectieziektebestrijding. Denk bijvoorbeeld aan het opnemen van gegevens van gezondheidssensoren, rioolwatermetingen, reizigersinformatie of genetische sequentiegegevens van ziekteverwekkers. Het vermogen om snel nieuwe gegevensbronnen te incorporeren en te analyseren, kan de reactietijd van de IZB-organisatie op opkomende bedreigingen aanzienlijk verkorten.
Een vorm van wendbaarheid is ook dat op technisch (bijv. ontbreken vpn), syntactisch (bijv. onbekend uitwisselingsformaat) of semantisch (bijv. itonose) vlak nieuwe koppelingen gerealiseerd dienen te worden.

8.5.4.5.2 Niveau 2: Nieuwe Attributen en/of Entiteiten

Het tweede niveau van datawendbaarheid draait om de mogelijkheid om nieuwe attributen en/of entiteiten binnen het datamodel te definiëren en te integreren. Dit houdt in dat de IZB-organisatie flexibel moet zijn in het aanpassen van de gegevensstructuur om nieuwe informatiecategorieën te omvatten, bijvoorbeeld demografische gegevens of nieuwe infectieziekte-specifieke entiteiten.

8.5.4.5.3 Niveau 3: Nieuwe Soorten Metadata

Het systeem moet ook in staat zijn om nieuwe soorten metadata op te slaan (bijvoorbeeld om het mogelijk te maken om terug te gaan in de tijd). Deze vragen in de regel forse ingrepen in het systeem.
Het huidige inzicht is, dat deze vorm van wendbaarheid niet van groot belang is voor de IZB: er zijn momenteel geen dringende aanwijzingen dat bijvoorbeeld in een volgende pandemie nieuwe soorten metadata nodig zijn om effectieve IZB te ondersteunen.

8.5.5 Security

8.5.5.1 Authenticatie

Voor we ook maar één besluit kunnen nemen omtrent wel of geen toegang tot processen of gegevens, dienen we vast te stellen met wie we te maken hebben. Het (digitaal) vaststellen van de identiteit van de gebruiker heet *authenticatie*.
In de context van het pandemisch parate landschap zijn er een aantal kenmerken aan het authenticatie proces die als eis moeten worden meegenomen:

- Vanuit de wet digitale overheid komt als grondslag dat authenticatie plaats dient te vinden door middel van een elektronisch identificatiemiddel met betrouwbaarheid substantieel of hoog.
- Eén (natuurlijk) persoon kan meerdere identiteiten aannemen in het systeem. Denk bijvoorbeeld aan een IZB-professional die als GGD-medewerker kan inloggen, maar ook als ingezetene (om bijvoorbeeld een testafspraak te maken).
- Vanwege het uitgangspunt van datacentrisch werkend dient toegang (in ieder geval) gecontroleerd te worden aan de voordeur van de dataservice. Dit heeft als consequentie dat een trusted-subsystem model (dat in de markt zeer gebruikelijk is) voor authenticatie niet voldoet. Ook de dataservice moet de identiteit van de eindgebruiker kennen. Er is sprake van een zogenaamd delegation model, waarbij de authenticatie context die werd vastgesteld ten tijde van inloggen, door alle systeemdelen heen doorgegeven dient te worden om uiteindelijk bij de dataservice uit te komen.

8.5.5.1.1 Betrouwbaarheidsniveau

Het authenticatielandschap van de Nederlandse overheid is in beweging. Elektronische authenticatiemiddelen als DigiD, eID en straks e-Wallets zijn gemeengoed geworden. Dit laat echter onverlet dat een epidemie zich niets aantrekt van betrouwbaarheidsniveaus van authenticatie en dat ook personen die niet in staat zijn zich met een gewenst betrouwbaarheidsniveau te authentiseren, in tijden van verheffing, wellicht toch geautomatiseerde diensten van een GGD moeten kunnen afnemen. Het op te leveren systeem zal daarom niet alleen in staat moeten zijn om de in de WDO genoemde authenticatiemiddelen te accepteren, het zal ook in haar authenticatiemechanismen een dermate flexibiliteit moeten kunnen bieden dat in voorkomende gevallen afwijkende authenticatiemethoden (bijvoorbeeld OTP of social logon) kunnen worden toegevoegd.

8.5.5.1.2 Eén persoon, meerdere identiteiten

Omdat een GGD-medewerker doorgaans ook ingezetene (in Nederland) is, is duidelijk dat één natuurlijk persoon meerdere identiteiten in het systeem/de systemen zal hebben. Omdat een GGD-medewerker typisch met een andere authenticatiemethode inlogt dan een burger, is dit verschil vroeg in het authenticatie proces te achterhalen en is het eenvoudig om deze ene persoon in de hoedanigheid van GGD-medewerker geheel andere rechten toe te wijzen dan dezelfde persoon in de hoedanigheid van burger.

Er speelt echter nog een subtiele variant van hetzelfde issue: GGD-medewerkers kunnen voor meerdere GGD'en actief zijn. Hier logt dezelfde GGD-medewerker in, maar dienen de rechten aangepast te worden naar de GGD waar die persoon op dat moment inlogt. Dit issue zal worden opgelost in de Identity Manager van GGD GHOR Nederland.

Een derde variant die ten tijde van de crisis ook voortkwam is de medewerkers frequent van rol en taken wisselen: Een medewerker kan bijvoorbeeld de ene dag worden ingezet als tester en de volgende dag als BCO-medewerker. Ook hier verloopt autorisatie via de Identity Manager.

Een vierde, denkbaar, scenario waarin een GGD-medewerker meerdere identiteiten kan aannemen is helpdesk functionaliteit. Het kan een nuttige feature zijn dat een helpdeskmedewerker tijdelijk en met toestemming de identiteit van de probleemhebber kan aannemen. Dit is een wens die in het verdere analysetraject bekeken moet worden.

8.5.5.1.3 Dataservice kent identiteit van de eindgebruiker

Het is een eis dat de dataservice waarin de GGD haar gegevens opslaat, zelf verantwoordelijk is voor de autorisatie beslissingen. Dit betekent dat de dataservice, die normaal gesproken niet direct, maar via GGD systemen benaderd wordt, de beschikking moet hebben over identiteit en rechten van de eindgebruiker. Dit is niet in lijn met de gangbare manier van softwareontwikkeling op dit moment, waar een service vooraf consent vraagt aan een gebruiker om vervolgens onder eigen (service) identiteit verder het systeem in te trekken, maar noodzakelijk om te voldoen aan de eis van datacentrisch werken.

Een consequentie hiervan is dat de autorisatie informatie die door het systeem vloeit, geschikt moet zijn voor consumptie door de dataservice.

8.5.5.2 Autorisatie

Tijdens het analyse proces voor de functionaliteit van IZB in het pandemisch parate landschap komen we tot zogenaamde autorisatieregels. Een autorisatieregel is als volgt gedefinieerd:

Een *autorisatieregel* beschouwt

- **Een *subject*, diegene die informatie uit de dataservice benadert;**
  Bijvoorbeeld: wat is de identiteit waarmee je inlogde, wat is je functie volgens het HR-systeem van je lokale GGD
- **De *inhoud* van het informatie-item dat benaderd wordt;**
  Bijvoorbeeld: is er sprake van een behandelrelatie met de persoon in het dossier
- **De *context* die ontstond tijdens aanloggen van subject;**
  Bijvoorbeeld: met welk loginsysteem ben je ingelogd (GGD, DigiD, ..), vanaf welke locatie of vanaf welk apparaat log je in
- **Het *procesbouwblok* via welke toegang gevraagd wordt tot de gegevens;**
  Bijvoorbeeld: verifieer signaal
- **De *attributen* die de huidige toestand van het systeem beschrijven;**
  Bijvoorbeeld: is er sprake van een pandemische situatie

… en verleent op basis hiervan al dan niet de in de autorisatieregel beschreven toegang tot het gevraagde informatie item.
Inhoud is hier een samengesteld begrip, het duidt hier zowel op de metadata over de inhoud (denk aan bijvoorbeeld doelbinding), als op de inhoud van het informatie-item zelf (bijvoorbeeld, u mag alleen een uitslag zien als u ook de aanvrager bent).

Een concept dat nadere toelichting nodig heeft, is doelbinding. Doelbinding is een vastlegging van het gebruik van (een set van) gegevens door een persoon in een bepaalde rol in het kader van een wettelijke grondslag. Omdat we niet in het hoofd van een gebruiker kunnen kijken om erachter te komen met welk doel bepaalde gegevens opgevraagd worden, koppelen we dit begrip (doelbinding) aan de systeemfunctionaliteit waarmee de gegevens benaderd worden. In de autorisatieregel kan dan opgenomen worden welke procesbouwblokken toegang hebben tot een gegeven of een set van gegevens.

Voorbeelden van de autorisatieregels voor de IZB van de GGD:

Het meest elementaire voorbeeld van een autorisatieregel voor het IZB-systeem is:

U heeft een account dat bekend is bij een GGD

Een autorisatieregel die in feite nu al actief is, is:

U heeft een Teleperformance account, u heeft de rol callcentermedewerker en er loopt een campagne waarbij het callcenter wordt ingezet

8.5.5.2.1 Autorisatiecontrole

De kern achter de wijze waarop wij autorisatie binnen het nieuwe landschap willen vormgeven is een tweeledige, additieve, strategie:

1. Alle informatie-items in de dataservice zijn in hun metadata voorzien van autorisatieregels die exact de rechten en policies beschrijven waar minimaal aan voldaan moet worden om dat informatie-item respectievelijk te creëren, lezen, wijzigen, verwijderen of de metadata aan te passen.
2. Tijdens de analysefase zullen we alle bedrijfsprocessen decomponeren tot aan processtapniveau. Alle processtappen worden vervolgens gekoppeld aan autorisatieregels die beschrijven wie, en in welke hoedanigheid, de processtap mag uitvoeren.

In de vastlegging van autorisaties is er dus sprake van twee autoritatieve bronnen: de autorisatieregels van de dataservice en de autorisatieregels die gekoppeld zijn aan processtappen. Voor het nemen van een autorisatiebeslissing zijn deze bronnen additief, dat wil zeggen: om een processtap uit te voeren moet een gebruiker rechten hebben die voldoen aan zowel de autorisatieregels van de processtap, als aan de autorisatieregels van alle informatie-items die door de processtap geraakt (gaan) worden.
Er zijn twee denkbare scenario's voor het controleren van de toegangsrechten van een gebruiker:

1. Individuele verantwoordelijkheid:
    - De processtap controleert bij starten of de gebruiker de juiste rechten heeft om aan zijn autorisatieregels te voldoen.
    - De dataservice controleert daarnaast bij elke toegang of de gebruiker de juiste rechten heeft om aan de autorisatieregels van de geraakte informatie-items te voldoen.
2. Optimale gebruikersbeleving:
    - De processtap leest de autorisatieregels voor alle te raken informatie-items uit de dataservice en combineert deze met de autorisatieregels van de processtap zelf.
    - De processtap controleert bij starten of de gebruiker de juiste rechten heeft om aan al deze autorisatieregels te voldoen.
    - De dataservice controleert daarnaast bij elke toegang of de gebruiker de juiste rechten heeft om aan de autorisatieregels van de betrokken informatie-items te voldoen.

8.5.5.2.2 Interpretatie van autorisatieregels

Een belangrijk principe achter het concept van autorisatieregels is dat we in de functionele omschrijving doelbewust wegblijven bij technische oplossingsrichtingen als RBAC en ABAC. Een autorisatieregel is een vehikel dat ons in staat stelt om beschrijvingen te geven die variëren van simpel groepslidmaatschap tot en met complexe beleidsregels. Als illustratief (maar niet realistisch) voorbeeld:

Een autorisatieregel kan eisen dat:

u werkt voor een GGD,

maar ook, u krijgt pas toegang:

wanneer u beschikt over een artsenrol en er sprake is van een relatie tussen deze burger en de GGD waar u werkt.

8.6 Privacy by design

Een belangrijk karakteristiek van de IZB is dat in veel gevallen vanuit medische gegevens over personen een geaggregeerd beeld gevormd wordt op basis waarvan een uitbraak bestreden kan worden. Los daarvan kan het voorkomen dat er (bijvoorbeeld tijdens een pandemie) op grote schaal testen worden uitgevoerd of vaccinaties worden gezet.

Daarmee is de IZB niet alleen een data-, maar ook een bijzondere persoonsgegevens- intensieve sector. Het waarborgen van privacy is daarom een belangrijke functie van het nieuwe IV-landschap.
In het domeinmodel dat door GGD GHOR Nederland en het RIVM voor de IZB wordt ontwikkeld worden daarom de principes van 'Privacy by Design' en 'Privacy bij Default' toegepast. Privacy by Default kan gezien worden als een onderdeel van Privacy by Design. Privacy by Default vereist dat de standaardinstellingen altijd zo privacyvriendelijk mogelijk zijn. Zo mogen de standaard-antwoordsuggesties bij een vraag om toestemming voor het delen van gegevens nooit 'Ja' zijn.

Belangrijke aspecten van Privacy bij Design waar ook rekening mee moet worden gehouden zijn:

8.6.1 Toegangscontrole op het niveau van data-elementen

In de dataservice wordt voor ieder data element dat een gebruiker benaderd, gecontroleerd of er recht op toegang is. Dat recht wordt bepaald door de autorisatieregels, die niet alleen persoonsgebonden, maar ook situatiegebonden zijn.

8.6.2 Maximale invulling van wettelijke verplichtingen

Het landschap dient te faciliteren dat betrokkenen zo eenvoudig mogelijk (waar mogelijk door self-service, ook door burgers) een beroep kunnen doen op hun wettelijke rechten

zoals:

- De rechten vastgelegd in de AVG:
  - Recht op informatie
  - Recht op inzage
  - Recht op rectificatie en aanvulling
  - Recht op vergetelheid

- Recht om de verwerking te beperken
- Recht op overdraagbaarheid van gegevens en
- Recht van bezwaar

- Het recht om te zien welke behandelaar (naam én rugnummer) in jouw dossier heeft gekeken (minimaal tot 60 maanden terug in de tijd gerekend vanaf het moment van verzoek).
- Een 'geen-bezwaar'-regeling voor het wel of niet delen van gegevens die onder het WGBO-regime vallen.

8.6.3 Bijzondere dossiers

Gegevens over beroemde, beruchte, politiek gevoelige personen, maar ook van personen die worden beschermd (Blijf van mijn lijf huis) zijn extra kwetsbaar en moeten extra kunnen worden afgeschermd, zodat ze alleen voor speciaal daartoe geautoriseerde medewerkers inzichtelijk zijn.

Daarnaast wordt nagedacht over het creëren van een mogelijkheid om kwetsbare personen toch (verplicht) te registreren, zonder alle kenmerkende elementen van een persoon voor iedereen te openbaren. (zie: Prominente publieke functies in de definitie van politiek prominente personen (belastingdienst.nl).

8.7 Wpg versus WGBO

Gegevens binnen de IZB vallen deels onder het regime van Wpg en deels onder dat van de WGBO.

Wanneer een betrokkene onder behandeling is, dan spreken we van een behandelovereenkomst en is de behandelaar verplicht hier een (WGBO-)dossier van aan te leggen.

> *Elke arts is verplicht om te zwijgen over alles wat hij tijdens zijn beroepsuitoefening over een patiënt te weten komt. Dit moet ruim worden uitgelegd. Ook het gegeven dat een patiënt onder behandeling is bij een arts, valt bijvoorbeeld onder de zwijgplicht. De arts moet ervoor zorgen dat er geen inlichtingen over de patiënt worden verstrekt aan anderen. Ook moet hij ervoor zorgen dat anderen geen inzage krijgen in – of een afschrift krijgen van – (een deel van) het medisch dossier van de patiënt. (KNMG-richtlijn: omgang met medische gegevens)*

Wanneer (individueel) behandelen/genezen niet het doel is maar infectieziektebestrijding (IZB), lees: het verkrijgen van inzicht en voorkomen van (verdere) verspreiding van infectieziekte voor de massa (volksgezondheid) is de Wpg van toepassing.

De meeste registraties en vastleggingen omtrent IZB worden in beginsel vastgelegd vanuit de Wpg. De data die erbij horen kunnen dus als Wpg-data worden aangemerkt. Dat geldt bijvoorbeeld voor de gegevens uit bron- en contactonderzoeken.

Vaccineren is een vorm van behandelen en het voorschrijven van profylaxe ook. Hier is de WGBO van toepassing. Op dit snijvlak kan een GGD-vaccinatiemedewerker enerzijds een behandelaar zijn op grond van de WGBO en anderzijds de Wpg dienen. Omdat WGBO en Wpg een andere bewaartermijn kennen is het daarbij van belang dat bij ieder data element de van toepassing zijnde regels worden vastgelegd.

8.8 Voor iedereen…

De Publieke Gezondheid in Nederland is er voor iedereen. GGD'en richten zich in hun werk met nadruk op de kwetsbare groepen in de samenleving. Daarbij maakt het niet uit of mensen, bijvoorbeeld, beschikken over een verblijfsstatus en/of een BSN. Naast bijvoorbeeld illegalen en dak- en thuislozen vormen asielzoekers ook een grote doelgroep.

Consequentie is, dat niet iedere persoon waarmee contact is beschikt over dezelfde identificerende gegevens. Dat vraagt extra maatregelen om zoveel als mogelijk te voorkomen dat er dubbele dossiers ontstaan, zoals:

- Uniciteitscontrole aan de hand van meerdere unieke nummers, zoals BSN, V-nummer (dossiernummer van asielzoekers en immigranten bij de IND) en COA-zorgnummer.
- Uniciteitscontrole aan de hand van een combinatie van een combinatie van persoonsgegevens (bijvoorbeeld: Achternaam, geboortedatum, geslacht, postcode).

Het vraagt ook om het ondersteunen van vaste 'onbekend'-waarden voor een aantal velden die in verband met de data-kwaliteit en wettelijke verplichtingen wel verplicht moeten worden ingevuld, bijvoorbeeld BSN 9x9 en postcode 9999XX en om opties om aan te geven dat een persoon niet beschikt over bijvoorbeeld een e-mailadres of een (in Nederland geregistreerd) telefoonnummer.

9 BIJLAGEN

9.1 Overzicht van alle eisen

9.2 GGD-regio's

9.2.1 Dienst Gezondheid & Jeugd Zuid-Holland Zuid

Gemeenten:

- Alblasserdam
- Dordrecht
- Gorinchem
- Hardinxveld-Giessendam
- Hendrik-Ido-Ambacht
- Hoeksche Waard
- Molenlanden
- Papendrecht
- Sliedrecht
- Zwijndrecht

9.2.2 GGD Amsterdam

Gemeenten:

- Aalsmeer
- Amstelveen
- Amsterdam
- Diemen
- Ouder-Amstel
- Uithoorn

9.2.3 GGD Brabant-Zuidoost

Gemeenten:

- Asten
- Bergeijk
- Best
- Bladel
- Cranendonck
- Deurne
- Eersel
- Eindhoven
- Geldrop-Mierlo
- Gemert-Bakel
- Heeze-Leende
- Helmond
- Laarbeek
- Nuenen, Gerwen en Nederwetten
- Oirschot
- Reusel-De Mierden
- Someren
- Son en Breugel
- Valkenswaard
- Veldhoven
- Waalre

9.2.4 GGD Drenthe

Gemeenten:

- Aa en Hunze
- Assen
- Borger-Odoorn
- Coevorden
- De Wolden
- Emmen
- Hoogeveen
- Meppel
- Midden-Drenthe
- Noordenveld
- Tynaarlo
- Westerveld

9.2.5 GGD Flevoland

Gemeenten:

- Almere
- Dronten
- Lelystad
- Noordoostpolder
- Urk
- Zeewolde

9.2.6 GGD Fryslân

Gemeenten:

- Achtkarspelen
- Ameland
- Dantumadiel
- De Fryske Marren
- Harlingen
- Heerenveen
- Leeuwarden
- Noardeast-Fryslân
- Ooststellingwerf
- Opsterland
- Schiermonnikoog
- Smallingerland
- Súdwest-Fryslân
- Terschelling
- Tytsjerksteradiel
- Vlieland
- Waadhoeke
- Weststellingwerf

9.2.7 GGD Gelderland-Zuid

Gemeenten:

- Berg en Dal
- Beuningen
- Buren
- Culemborg
- Druten
- Heumen
- Maasdriel
- Neder-Betuwe
- Nijmegen
- Tiel
- West Betuwe
- West Maas en Waal
- Wijchen
- Zaltbommel

9.2.8 GGD Gooi en Vechtstreek

Gemeenten:

- Blaricum
- Gooise Meren
- Hilversum
- Huizen
- Laren
- Wijdemeren

9.2.9 GGD Groningen

Gemeenten:

- Eemsdelta
- Groningen
- Het Hogeland
- Midden-Groningen
- Oldambt
- Pekela
- Stadskanaal
- Veendam
- Westerkwartier
- Westerwolde

9.2.10 GGD Haaglanden

Gemeenten:

- 's-Gravenhage
- Delft
- Leidschendam-Voorburg
- Midden-Delfland
- Pijnacker-Nootdorp
- Rijswijk
- Wassenaar
- Westland
- Zoetermeer

9.2.11 GGD Hart voor Brabant

Gemeenten:

- 's-Hertogenbosch
- Bernheze
- Boekel
- Boxtel
- Dongen
- Gilze en Rijen
- Goirle
- Heusden
- Hilvarenbeek
- Land van Cuijk
- Loon op Zand
- Maashorst
- Meierijstad
- Oisterwijk
- Oss
- Sint-Michielsgestel
- Tilburg
- Vught
- Waalwijk

9.2.12 GGD Hollands-Midden

Gemeenten:

- Alphen aan den Rijn
- Bodegraven-Reeuwijk
- Gouda
- Hillegom
- Kaag en Braassem
- Katwijk
- Krimpenerwaard
- Leiden
- Leiderdorp
- Lisse
- Nieuwkoop
- Noordwijk
- Oegstgeest
- Teylingen
- Voorschoten
- Waddinxveen
- Zoeterwoude
- Zuidplas

9.2.13 GGD Hollands-Noorden

Gemeenten:

- Alkmaar
- Bergen (NH)
- Castricum
- Den Helder
- Dijk en Waard
- Drechterland
- Enkhuizen
- Heiloo
- Hollands Kroon
- Hoorn
- Koggenland
- Medemblik
- Opmeer
- Schagen
- Stede Broec
- Texel

9.2.14 GGD IJsselland

Gemeenten:

- Dalfsen
- Deventer
- Hardenberg
- Kampen
- Olst-Wijhe
- Ommen
- Raalte
- Staphorst
- Steenwijkerland
- Zwartewaterland
- Zwolle

9.2.15 GGD Kennemerland

Gemeenten:

- Beverwijk
- Bloemendaal
- Haarlem
- Haarlemmermeer
- Heemskerk
- Heemstede
- Uitgeest
- Velsen
- Zandvoort

9.2.16 GGD Limburg-Noord

Gemeenten:

- Beesel
- Bergen (L)
- Echt-Susteren
- Gennep
- Horst aan de Maas
- Leudal
- Maasgouw
- Mook en Middelaar
- Nederweert
- Peel en Maas
- Roerdalen
- Roermond
- Venlo
- Venray
- Weert

9.2.17 GGD Noord- en Oost-Gelderland

Gemeenten:

- Aalten
- Apeldoorn
- Berkelland
- Bronckhorst
- Brummen
- Doetinchem
- Elburg
- Epe
- Ermelo
- Harderwijk
- Hattem
- Heerde
- Lochem
- Montferland
- Nunspeet
- Oldebroek
- Oost Gelre
- Oude IJsselstreek
- Putten
- Voorst
- Winterswijk
- Zutphen

9.2.18 GGD regio Utrecht

Gemeenten:

- Amersfoort
- Baarn
- Bunnik
- Bunschoten
- De Bilt
- De Ronde Venen
- Eemnes
- Houten
- IJsselstein
- Leusden
- Lopik
- Montfoort
- Nieuwegein
- Oudewater
- Renswoude
- Rhenen
- Soest
- Stichtse Vecht
- Utrecht
- Utrechtse Heuvelrug
- Veenendaal
- Vijfheerenlanden
- Wijk bij Duurstede
- Woerden
- Woudenberg
- Zeist

9.2.19 GGD Rotterdam-Rijnmond

Gemeenten:

- Albrandswaard
- Barendrecht
- Capelle aan den IJssel
- Goeree-Overflakkee
- Krimpen aan den IJssel
- Lansingerland
- Maassluis
- Nissewaard
- Ridderkerk
- Rotterdam
- Schiedam
- Vlaardingen
- Voorne aan Zee

9.2.20 GGD Twente

Gemeenten:

- Almelo
- Borne
- Dinkelland
- Enschede
- Haaksbergen
- Hellendoorn
- Hengelo (O)
- Hof van Twente
- Losser
- Oldenzaal
- Rijssen-Holten
- Tubbergen
- Twenterand
- Wierden

9.2.21 GGD West-Brabant

Gemeenten:

- Alphen-Chaam
- Altena
- Baarle-Nassau
- Bergen op Zoom
- Breda
- Drimmelen
- Etten-Leur
- Geertruidenberg
- Halderberge
- Moerdijk
- Oosterhout
- Roosendaal
- Rucphen
- Steenbergen
- Woensdrecht
- Zundert

9.2.22 GGD Zaanstreek/Waterland

Gemeenten:

- Edam-Volendam
- Landsmeer
- Oostzaan
- Purmerend
- Waterland
- Wormerland
- Zaanstad

9.2.23 GGD Zeeland

Gemeenten:

- Borsele
- Goes
- Hulst
- Kapelle
- Middelburg
- Noord-Beveland
- Reimerswaal
- Schouwen-Duiveland
- Sluis
- Terneuzen
- Tholen
- Veere
- Vlissingen

9.2.24 GGD Zuid-Limburg

Gemeenten:

- Beek
- Beekdaelen
- Brunssum
- Eijsden-Margraten
- Gulpen-Wittem
- Heerlen
- Kerkrade
- Landgraaf
- Maastricht
- Meerssen
- Simpelveld
- Sittard-Geleen
- Stein
- Vaals
- Valkenburg aan de Geul
- Voerendaal

9.2.25 Veiligheids- en Gezondheidsregio Gelderland-Midden

Gemeenten:

- Arnhem
- Barneveld
- Doesburg
- Duiven
- Ede
- Lingewaard
- Nijkerk
- Overbetuwe
- Renkum
- Rheden
- Rozendaal
- Scherpenzeel
- Wageningen
- Westervoort
- Zevenaar

Zwarte Woud 2
3524 SJ Utrecht
ggdghor.nl