Gebaseerd op HLD IV IZB

Doelarchitectuur IV voor infectieziektebestrijding

editie 2024Q1

31 maart 2024

Ministerie van Volksgezondheid,
Welzijn en Sport

Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

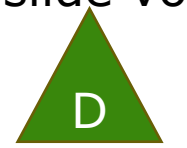
Documentbeheer en brondocumenten

Datum	Versie	Status
13 juli 2023	0.9	Initiële versie gebaseerd op brondocumenten “HLD” en “HLD Vervolg”
31 januari 2024	0.91	Consistentie naamgeving Doelarchitectuur
31 maart 2024	1.0	Verwerking review DI CIO VWS, toevoeging Nora principes mbt Betrouwbaarheid ivm Privacy en Security. Programma huisstijl toegepast.

Brondocument	Versie	Documentnaam	Datum
HLD Vervolg	1.0	HLD Vervolg versie 1.0 dd 20230524	24 mei 2023
HLD	1.1	HLD Final v11 27 sept 2022	27 september 2022

Leeswijzer

- In voorgaande ontwerpdocumenten (HLD en HLD Vervolg) zijn ontwerpprincipes vastgelegd, deze zijn opgenomen in dit document.
- Binnen het programma Pandemisch Parate IV voor de IZB vindt steeds kennisontwikkeling plaats gedurende de samenwerking tussen RIVM en GGD/GGDGHOR. Deze kennis levert weer een bijdrage tot aanvullende of scherpere architectuurrichtlijnen
- Van dit document zal 1x per kwartaal een nieuwe versie worden uitgebracht.
- Om de lezer zicht te geven op de Definitieve architectuur richtlijnen én op het onderhanden werk en backlog, is iedere slide voorzien van een status,
  - **D**efinitieve Ontwerpkeuze,



  - **I**n ontwikkeling,

  - **B**acklog

Maak voor de reguliere infectieziektebestrijding een informatievoorziening die geschikt is voor opgeschaald gebruik

Infectieziektebestrijding I

Infectieziektebestrijding omvat alle maatregelen en activiteiten die gericht zijn op het voorkomen, beheersen en behandelen van infectieziekten. Het is een tak van de volksgezondheid die zich richt op het beheersen van de verspreiding van infectieziekten binnen een bevolking. De belangrijkste doelstellingen van infectieziektebestrijding zijn het voorkomen van infecties en het minimaliseren van de impact ervan op individuen en gemeenschappen. Dit wordt bereikt door middel van verschillende strategieën en interventies, waaronder:

1. Surveillance: Het monitoren van infectieziekten om vroegtijdige detectie mogelijk te maken. Dit omvat het verzamelen, analyseren en interpreteren van gegevens over ziekte-incidentie, verspreiding en trends.
2. Preventie: Het nemen van maatregelen om de verspreiding van infectieziekten te voorkomen. Dit omvat onder andere vaccinaties, voorlichting over hygiënepraktijken, bevordering van veilig seksueel gedrag, gebruik van beschermende middelen en het bevorderen van gezonde leefstijl.
3. Controle: Het beheersen van de verspreiding van infectieziekten wanneer ze zich voordoen. Dit omvat het identificeren en isoleren van geïnfecteerde individuen, het behandelen van zieken, het traceren van contacten en het nemen van maatregelen om verdere verspreiding te voorkomen.
4. Onderzoek: Het uitvoeren van wetenschappelijk onderzoek naar infectieziekten, inclusief epidemiologisch onderzoek, om de oorzaken, risicofactoren, transmissiepatronen en effectieve behandelings- en preventiemethoden beter te begrijpen.
5. Samenwerking en coördinatie: Het samenwerken met verschillende belanghebbenden, waaronder gezondheidsorganisaties, laboratoria, medische professionals, beleidsmakers en de gemeenschap, om een gecoördineerde respons op infectieziekten te waarborgen.

Infectieziektebestrijding II

Enkele voorbeelden van infectieziektebestrijdingsinspanningen zijn onder andere:

- het bevorderen van vaccinaties tegen ziekten zoals mazelen, polio en griep;
- het uitvoeren van onderzoek naar nieuwe opkomende infectieziekten zoals COVID-19;
- en het ontwikkelen van richtlijnen en protocollen voor de bestrijding van infectieziekten in ziekenhuizen en andere zorginstellingen.

Infectieziektebestrijding speelt een cruciale rol bij het beschermen van de volksgezondheid en het voorkomen van epidemieën en pandemieën. Het vereist samenwerking en inzet op verschillende niveaus, van individuele gedragsverandering tot nationaal en internationaal beleid.

Managementsamenvatting: visie

De infectieziektebestrijding (IZB) in Nederland dient naadloos opgeschaald te kunnen worden in geval van een pandemie, met als kernuitvoerders RIVM en GGD'en. Dit houdt in dat er tijdens een pandemie grotere volumes verwerkt kunnen worden (**schaalbaar**) én dat er vlot nieuwe werkprocessen kunnen worden gestart en ondersteund met bestaande en nieuwe samenwerkingspartners (**wendbaar**). Kortom: tijdens een pandemie zullen meer én andere mensen, gegevens en processen betrokken zijn bij de infectieziektebestrijding. Ook blijft tijdens een opschaling de informatievoorziening robuust en **betrouwbaar**.

Het belangrijkste richtinggevende principe is:

Maak voor de reguliere infectieziektebestrijding een informatievoorziening die geschikt is voor opgeschaald gebruik.

De belangrijkste ontwerpkeuzes voor de informatievoorziening (IV) voor die reguliere infectieziektebestrijding zijn:

- Datacentrisch: eenduidige en veilige data vormen het fundament.
- Modulair: IT-bouwblokken vormen de basis van de informatievoorziening.

Managementsamenvatting: Architectuurprincipes voor de informatievoorziening IZB

- Met het bovenste ontwerpprincipe als basis, adopteren wij de volgende principes uit de NORA als de meest significante om de benodigde wendbaarheid, schaalbaarheid en betrouwbaarheid van de IV IZB te kunnen realiseren.

Ontwerp vanuit de reguliere situatie	Maak voor de reguliere infectieziektebestrijding een informatievoorziening die geschikt is voor opgeschaald gebruik.
Neem gegevens als fundament	Gebruik gegevens als fundament voor het ontwerp, realisatie en doorontwikkeling van de dienst en richt het beheer hiervan goed in.
Standaardiseer waar mogelijk	Standaardiseer waar het kan, maak specifiek waar het moet.
Informeer bij de bron	Maak bij de dienst gebruik van gegevens die afkomstig zijn uit een bronregistratie.
Maak diensten schaalbaar	Bereid de dienst voor op veranderende werklast of reikwijdte.
Bouw diensten modulair op	Maak bij de ontwikkeling van diensten gebruik van een modulaire indeling met een maximale interne samenhang en minimale externe koppelingen.
Pas doelbinding toe	Geef burgers en bedrijven de zekerheid dat informatie over hen alleen wordt gebruikt voor de doelen waarvoor deze oorspronkelijk is verzameld.
Beheers risico’s voortdurend	Maak in alle stappen van ontwerp en doorontwikkeling van de dienst de risico's inzichtelijk en stuur op een afgewogen beheersing ervan.
Verifieer altijd	Verifieer doorlopend de juiste werking van de componenten en beheersmaatregelen van de dienst.

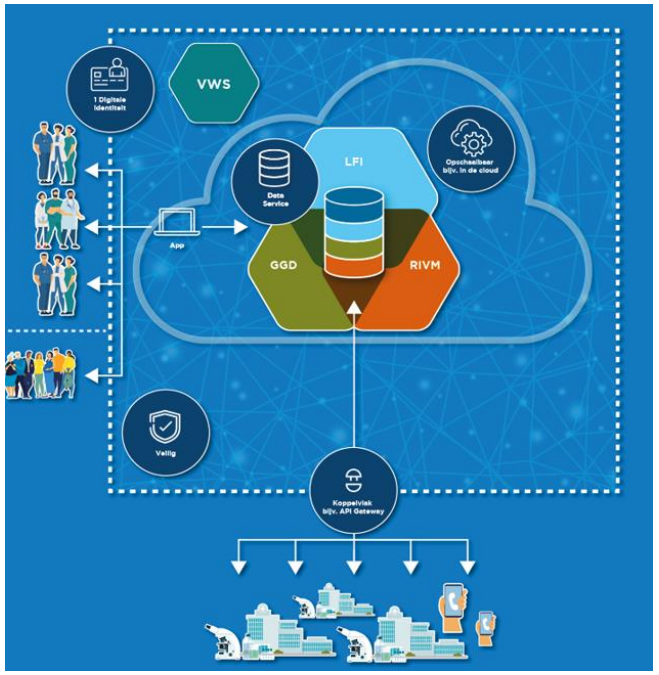
Managementsamenvatting: IV voor IZB “alsof het één is”

De doelarchitectuur geeft invulling aan de gezamenlijke opdracht om de IV naadloos (“alsof het één is”) op elkaar te laten aansluiten op het gebied van datacentrisch werken en IT-bouwblokken.

RIVM en GGD'en realiseren –als kernuitvoerders- een samenhangende informatievoorziening voor de infectieziektebestrijding (IZB) die geschikt is voor zowel regulier gebruik als opgeschaald gebruik in een pandemische situatie.

De informatievoorziening is logisch gezien één geheel ter ondersteuning van alle bedrijfsfuncties in de IZB.

- RIVM en GGD'en werken samen aan de uitvoering van de IZB in Nederland
- RIVM en GGD'en hebben daarnaast eigen –en andere- taken.
- De IV en IT ondersteuning van RIVM en GGD'en zijn de eigen verantwoordelijkheid van de individuele organisaties ter ondersteuning van het gehele eigen takenpakket.
- Ten behoeve van de (pandemisch parate) uitvoering van de IZB sluiten de IT/IV landschappen naadloos op elkaar aan (“alsof het één is”).



Managementsamenvatting: datacentrisch werken en domeinmodellen

- Data is voor ons een zeer waardevolle asset, we nemen de beschikbaarheid en kwaliteit van data als vertrekpunt.

- Datacentrisch werken impliceert:
  - Dat RIVM en GGD’en overeenstemming hebben over de betekenis en het gebruik van de data.
  - Dat we de data die we met elkaar delen kunnen vertrouwen (i.e. actueel, accuraat, correct, volledig, etc. is).
  - Dat we de data beveiligen.

- Onder een domeinmodel verstaan we: een model van een bepaald IZB-domein waarin informatie en het gebruik ervan in samenhang worden vastgelegd door inhoudelijke professionals én IV-specialisten.

- Gezamenlijk worden de domeinmodellen vastgesteld en onderhouden waarmee de betekenis van informatie in de kern van de IZB-systemen wordt vastgelegd. De regie op de data ligt dus bij RIVM en GGD’en en niet bij leveranciers van softwarepakketten.

- De wijze waarop de domeinmodellen worden opgesteld en onderhouden, is eenduidig tussen RIVM en GGD’en. We baseren ons op (inter)nationale standaarden en laten ons ondersteunen door standaardisatiepartijen zoals Nictiz.

- Er zijn domeinen waarbij het evident is, welk van de twee partijen in de lead zal zijn, bijvoorbeeld sequencing (RIVM), afspraken om te testen (GGD'en). Maar we hebben vooral geconstateerd dat de verwevenheid van de processen bij GGD'en en RIVM vraagt om een gezamenlijke uitwerking en vaststelling van de te gebruiken domeinmodellen.

- Voor informatie-uitwisseling in de keten hanteren we de uitwisselingsstandaarden, zoals die in de keten courant zijn. Waar nodig dragen we actief bij aan de totstandkoming van (inter)nationale standaarden.

Managementsamenvatting: basis infrastructuurvoorzieningen

- Naast alle voorzieningen die de bedrijfsfuncties in de IZB ondersteunen, onderkent de doelarchitectuur zg. ondersteunende IT voorzieningen, die zorgen dat de IV schaalbaar, wendbaar en betrouwbaar is.
- RIVM en GGD'en beschikken ieder over eigen generieke IT voorzieningen voor het ondersteunen van bijvoorbeeld Digitale Identiteit, Cloud hosting, Koppelvlak met ketenpartners, Securitymonitoring en Data. Daar waar we deze voorzieningen voorheen onafhankelijk van elkaar realiseerden, ontwikkelen we ze vanaf nu – in lijn met de doelarchitectuur – in gezamenlijke afstemming door.
- Deze afstemming tussen RIVM en GGD'en borgt dat de IV zich gedraagt “alsof deze één is”.
- *Toepassingsvoorbeelden:*
  - Voor zorgverleners en andere ketenpartners is er een eenduidig koppelvlak voor het leveren en/of raadplegen van data in de infectieziektebestrijding.
  - De voorziening Digitale Identiteit maakt het uniform “on-boarden” van grote aantallen (tijdelijke) medewerkers in korte tijd mogelijk.
  - Bij een beveiligingsincident heeft het SOC een totaalbeeld van risico’s en impact en kan daar direct op acteren.

Managementsamenvatting: structureel sturen op samenwerking

- De opdracht aan GGD'en en RIVM om gezamenlijk te komen tot een pandemisch parate infectieziektebestrijding, betekent een grote verandering voor beide organisaties in hoe zij hun informatievoorziening realiseren. Dit gaat niet vanzelf.
- Binnen het RIVM en de samenwerkende GGD'en worden vanuit de eigen taken en verantwoordelijkheden programma's en projecten opgestart voor de realisatie van een pandemisch parate IV voor de IZB. Daarbij is telkens een oordeel nodig op welke punten samenwerking vereist is.
- Voor de volgende gebieden adviseren wij om de governance in te richten voor de samenwerking op:
  - De architectuur van de IV voor de IZB.
  - Inrichten en onderhouden van de domeinmodellen.
  - Inrichten en onderhouden van de koppelvlakken ten behoeve van ketenpartners.
  - Het doorontwikkelen en het gebruik van infrastructuurvoorzieningen.
  - Bewaking van de informatiebeveiliging over de gehele keten.

Managementsamenvatting: aanbevelingen voor de realisatie

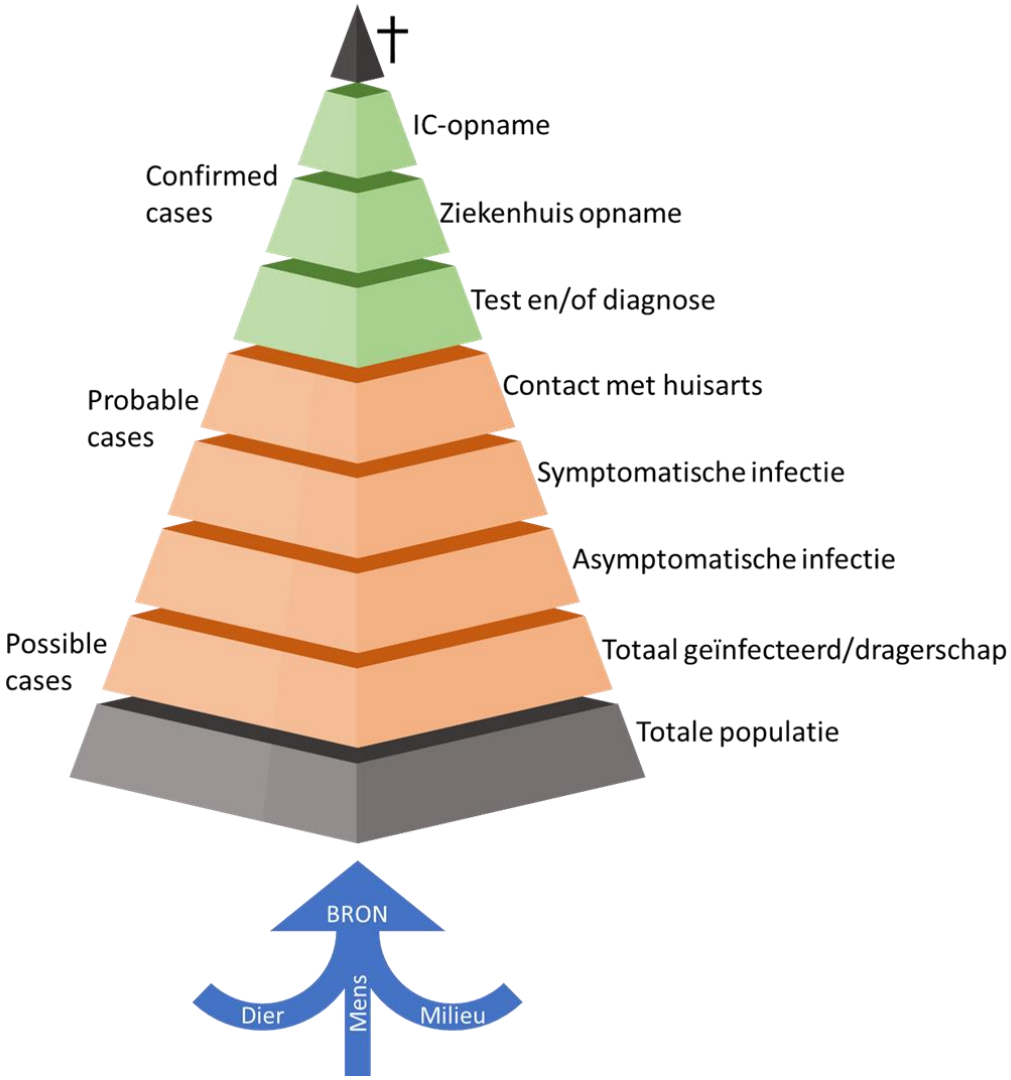
- Zorg voor een breed draagvlak voor de implementatie binnen de IZB
  - Maak er geen IT-feestje van. Zorg voor een goede aansluiting met professionals en bestuurders
- Zorg structureel voor een integraal beeld en besteed bij de verdere inrichting van de governance met name aandacht aan de onderwerpen:
  - Domeinmodellen.
  - Architectuur (voorzieningen, datasets etc.).
  - Juridische kaders.
  - Projectfinanciën en structurele kosten.
  - Risico's.
- Think big, take small steps:
  - Breng bestaande programma's en projecten binnen RIVM en GGD'en in lijn met deze architectuur.
  - Ondersteun lopende en geplande projecten om de beoogde voorzieningen te realiseren.
  - Wanneer het fundament voor de A-ziekten gerealiseerd is, breid dan gecontroleerd uit.
- Dit gaat niet lukken zonder een goed wettelijk kader en eenheid van taal!
  - Laat oa. de WPG wijzigingen aansluiten op de doelarchitectuur.

Managementsamenvatting: toepassing in de praktijk

In de huidige situatie bevindt de data over cases in de verschillende lagen van de surveillance-piramide zich ook in verschillende systemen met elk hun eigen definities, autorisaties en bereikbaarheid.

Concreet: we weten niet of de mensen, die via Infectieradar bepaalde symptomen hebben gemeld, dezelfde mensen zijn als de mensen, die in een HIS worden geregistreerd met diezelfde symptomen en dezelfde mensen zijn, waarvan de testresultaten in een LIMS worden vastgelegd door een laboratorium.

Door de data los te koppelen van de systemen en op het data-niveau (ic. via een domeinmodel) met elkaar te verbinden, kunnen we (veel beter en efficiënter dan nu) over de gehele piramide verbanden leggen, correlaties herkennen en conclusies trekken.



Managementsamenvatting: toepassing in de praktijk

Thuistest:

- **Nu:** een zelftest wordt niet bewaard. Voor de opvolging in de IZB-keten is een nieuwe test nodig. Relevante gegevens van de burger moet de burger verschillende keren opnieuw melden aan de GGD.
- **Straks:** er is een koppelvlak waar aanbieders van thuistesten gegevens bijvoorbeeld vanuit een app of een meetinstrument gelijk kunnen aanbieden aan GGD en RIVM. Door integratie met een toestemmingsregistratie in het domeinmodel, is altijd duidelijk voor welke doelen de gegevens gebruikt mogen worden.

Recht op inzage:

- **Nu:** als een burger inzage wil in zijn gegevens, zijn deze nu over verschillende applicaties verspreid en vraagt het veel integraties achteraf (of zelfs handwerk) om deze gegevens bij elkaar te brengen.
- **Straks:** in de domeinmodellen zijn de relaties tussen burgers en hun gegevens op voorhand gedefinieerd. Inzage kan via een koppelstandaard in één keer ingeregeld worden in een portaal voor de burger.

Voedselincident:

- **Nu:** er is geen informatie-uitwisseling voorbereid tussen supermarktketens, voedingsleveranciers, NVWA en de infectieziektebestrijding. Bij een voedselincident zal ad-hoc naar informatie gezocht worden en op dat moment naar de rechtmatigheid van de gegevensdeling gekeken moeten worden.
- **Straks:** RIVM en GGD betrekken NVWA en de voedingssector bij de definitie van de relevante informatie voor infectieziekten in relatie tot voedselveiligheid. Grondslagen zijn duidelijk. Een voedselincident is geoefend met het LFI. Bij een echt incident kunnen over de relevante producten direct verkoop- en distributiegegevens worden opgehaald en geanalyseerd.

Inhoudsopgave

Inleiding en aanleiding

We zijn voornemens om in de komende jaren het informatievoorzieningslandschap (IV-landschap en bijbehorende ICT-systemen) in het domein van de publieke gezondheid stap voor stap te verbeteren. In samenwerking met ketenpartners zal een landschap ontwikkeld moeten worden dat zowel in een koude als warme fase voldoet en recht doet aan de verschillende bestuurlijke en maatschappelijk verantwoordelijkheden.

Professionals moeten met deze systemen hun werk slagvaardig, flexibel en betrouwbaar kunnen uitvoeren, zowel in een koude, reguliere IZB, als in een warme fase, de opgeschaalde IZB. Samen werken we toe naar eenvoudig **schaalbare**, **wendbare** en **betrouwbare** systemen die, bij een uitbraak:

- grote hoeveelheden data kunnen verwerken en uitwisselen;
- burgers eenvoudig en betrouwbaar in staat stellen eigen data online te kunnen benaderen;
- kunnen opschalen in het aantal gebruikers;
- betrouwbaar blijven en een adequate verantwoording over de inzet van mensen en middelen naar het bestuur en publiek mogelijk maken.

Privacy en cyberveiligheid van gegevens staan daarbij als harde randvoorwaarden voorop. En burgers horen toegang tot hun gegevens te hebben, bijvoorbeeld via een Persoonlijke Gezondheidsomgeving (PGO). Om monitoring en onderzoek mogelijk te maken, moet ook de uitwisseling van gegevens tussen zorgverleners en onderzoekers eenvoudig kunnen.

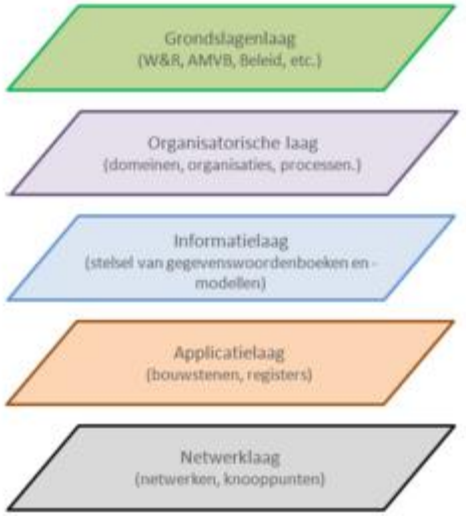
Deze doelarchitectuur beschrijft de kaders, principes en richtlijnen voor het IV/ICT landschap dat de infectieziektebestrijding in Nederland – zowel in een ‘’koude’ als in een ‘warme’ situatie – optimaal ondersteunt.

Wendbaar, Schaalbaar en Betrouwbaar

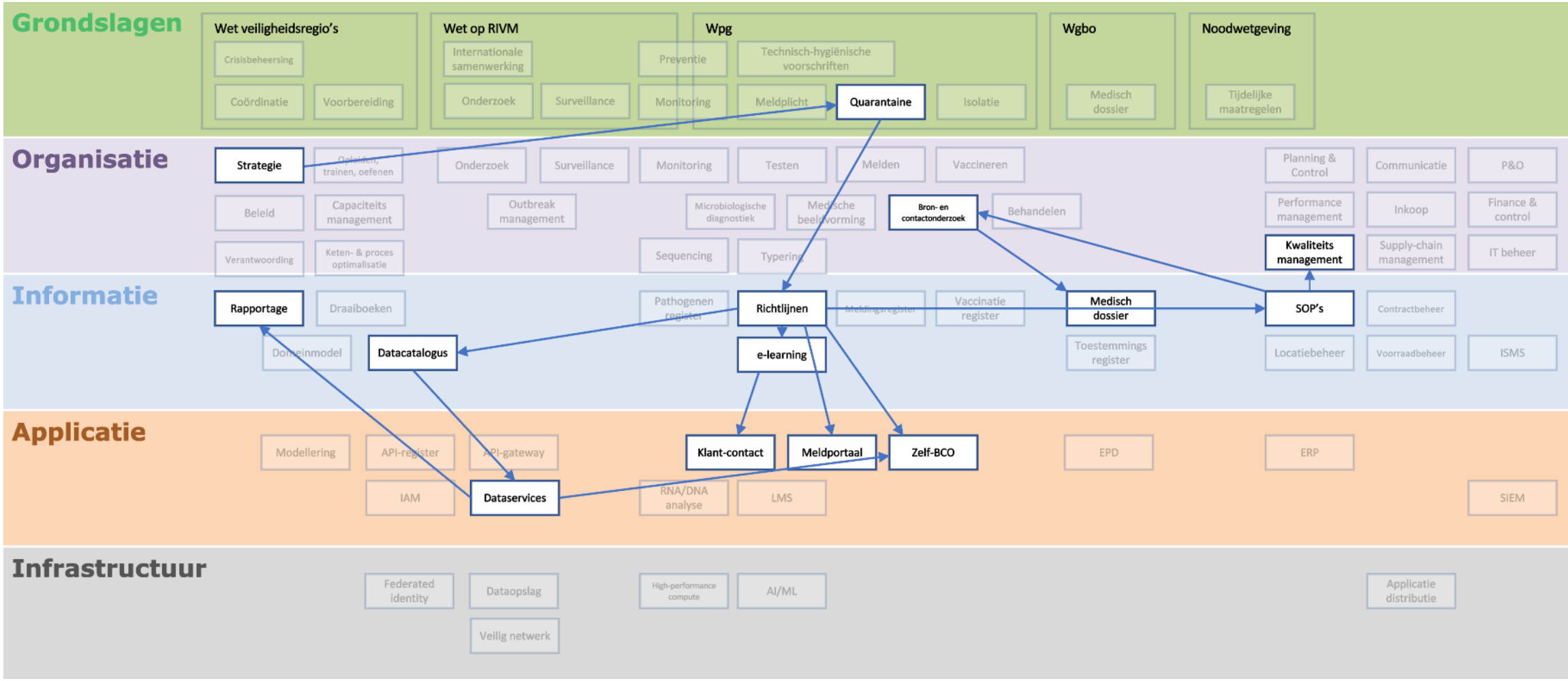
- Schaalbaar:
  - het vermogen van een IZB-systeem om snel te reageren op veranderende werklast;
- Wendbaar:
  - het vermogen van een IZB-systeem om snel gedrag aan te passen aan veranderende situaties;
- Betrouwbaar:
  - de waarschijnlijkheid dat een IZB-systeem zijn functie uitvoert binnen een gespecificeerde tijdsperiode onder gespecificeerde omstandigheden. (Engels: reliable)
  - de mate waarin een burger kan vertrouwen op het zorgvuldig gebruik van informatie in het IZB-systeem. (Engels: trustworthy)

Wendbaar, Schaalbaar en betrouwbaar op alle niveaus

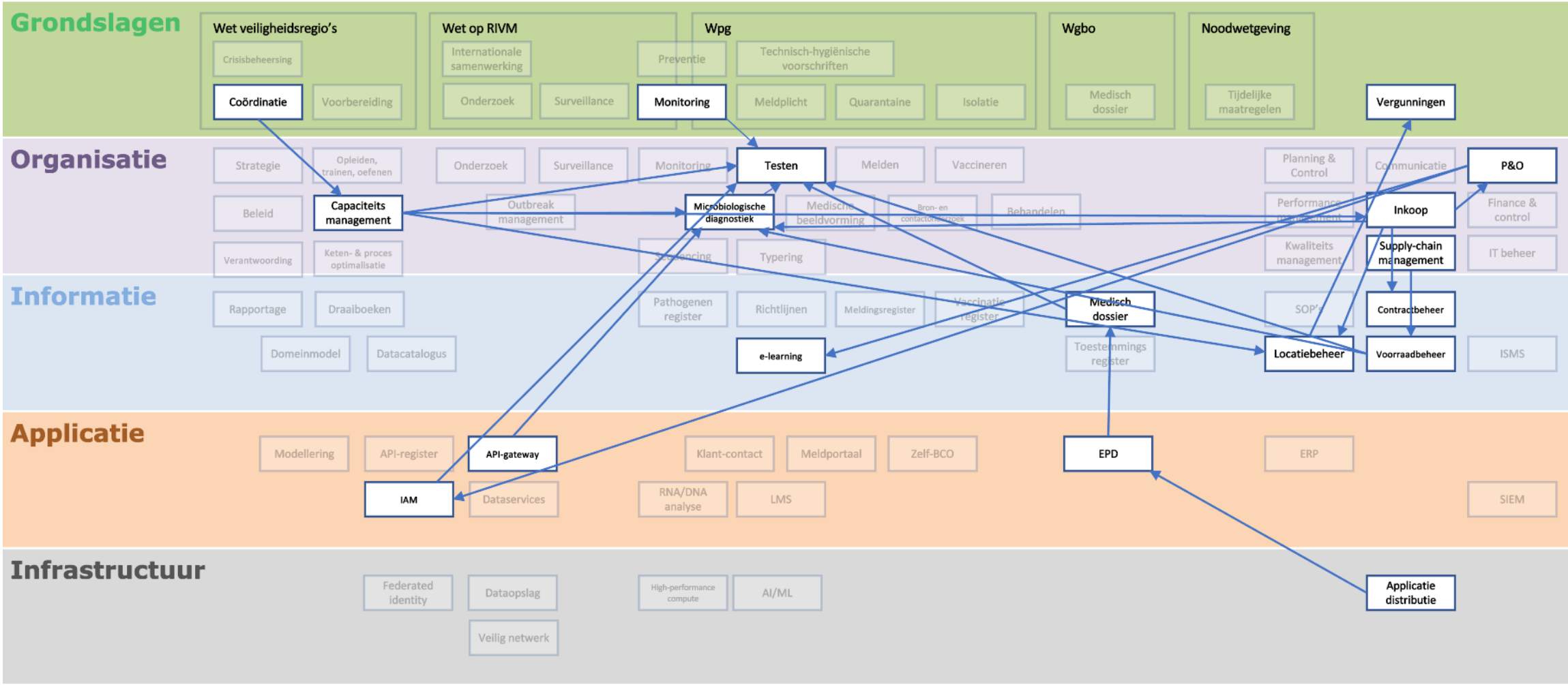
- Dit document geeft richting aan de IV middelen. Om te komen tot een pandemisch parate samenwerkingsketen is er echter meer nodig dan de IV middelen. We baseren ons op het NORA vijflaagsmodel
- Ter illustratie worden de volgende situaties gevisualiseerd:
  - Een wijziging van het quarantainebeleid
  - Uitbreiding van testcapaciteit
  - Hoogste beschikbaarheidsniveau



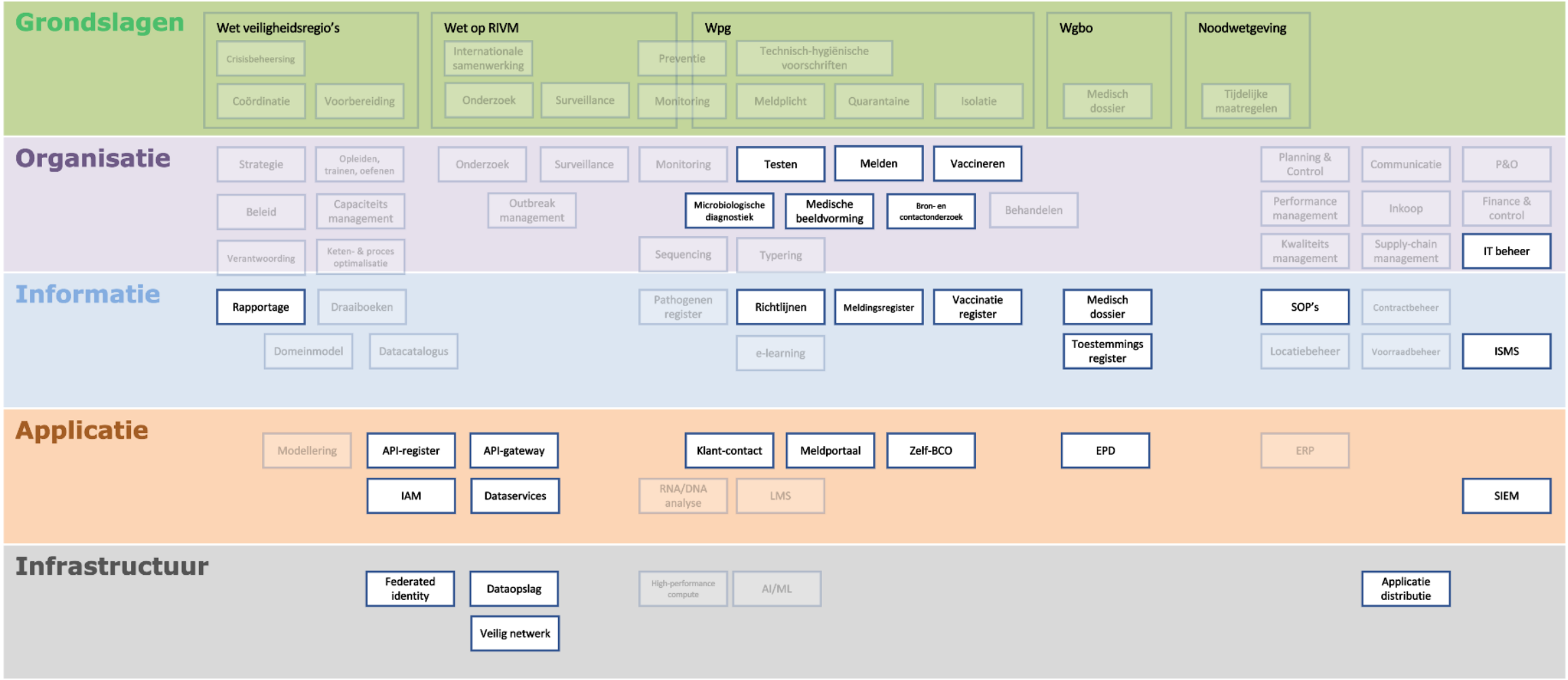
Wendbaar: voorbeeld wijziging quarantainebeleid



Schaalbaar: voorbeeld uitbreiding testcapaciteit



Betrouwbaar: voorbeeld hoogste beschikbaarheidsniveau



Afbakening IV/IT Landschap

- RIVM en GGD'en werken nauw samen met elkaar bij de bestrijding van infectieziekten, maar hebben daarnaast ook eigen –en andere- taken.
- Beide organisaties hebben dan ook hun eigen IV/ICT ‘landschap’ (bestaande uit - al dan niet onderling verbonden - apparatuur, netwerk, applicaties, systemen) om de uitoefening van al deze taken te ondersteunen.
- In het landschap van GGD vind je (nu nog) HpZone, CoronIT, terwijl in het landschap van RIVM systemen als Osiris, maar ook applicaties ten behoeve van Gezonde Leefstijl Interventie en Elektronisch Milieu Jaarverslagen te vinden zijn.
- Beide organisaties hebben hun eigen visie en strategie voor de door-ontwikkeling van hun landschap voor de diversiteit aan taken.
- Om de omvang van de IT landschappen niet verder te vergroten, is er voor gekozen om de IZB in te (blijven) richten in de bestaande situatie en dus geen scenario uit te werken om er nog een 3e gezamenlijk IT landschap aan toe te voegen.
- Ten behoeve van de (pandemisch parate) uitvoering van de IZB dienen de IT/IV landschappen wel naadloos op elkaar aan te sluiten.

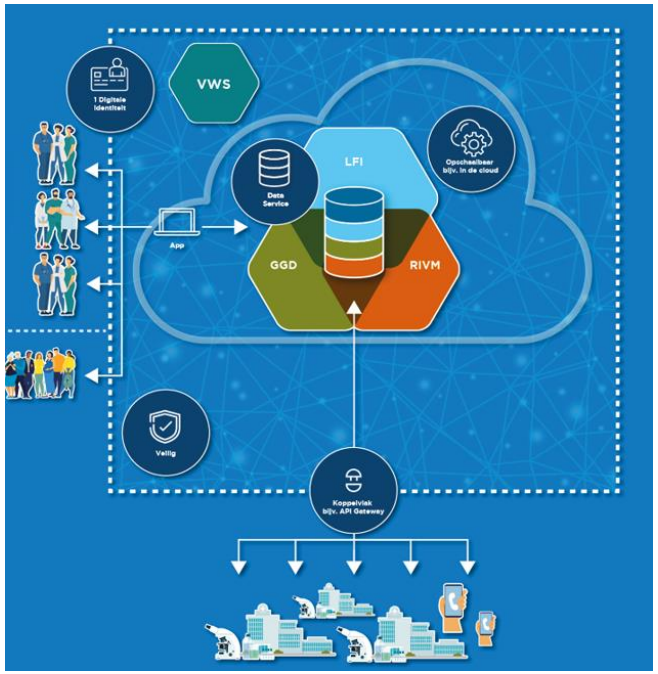
IV voor IZB “alsof het één is”

RIVM en GGD'en realiseren –als kernuitvoerders- een samenhangende informatievoorziening voor de infectieziektebestrijding (IZB) die geschikt is voor zowel regulier gebruik als opgeschaald gebruik in een pandemische situatie.

De doelarchitectuur geeft invulling aan de gezamenlijke opdracht om de IV naadloos (“alsof het één is”) op elkaar te laten aansluiten op het gebied van datacentrisch werken en IT-bouwblokken.

De informatievoorziening is logisch gezien één geheel ter ondersteuning van alle bedrijfsfuncties in de IZB.

- Dit document geeft richting aan de gezamenlijke taak om de IV voor IZB naadloos (“alsof het één is”) op elkaar te laten aansluiten op het gebied van:
  - Betekenis van informatie (Domeinmodel)
  - Inrichting van technologie (Basisvoorzieningen)



Architectuurprincipes voor de informatievoorziening IZB

- Met het bovenste ontwerpprincipe als basis, adopteren wij de volgende principes uit de NORA als de meest significante om de benodigde wendbaarheid, schaalbaarheid en betrouwbaarheid van de IV IZB te kunnen realiseren.

Ontwerp vanuit de reguliere situatie	Maak voor de reguliere infectieziektebestrijding een informatievoorziening die geschikt is voor opgeschaald gebruik.
Neem gegevens als fundament	Gebruik gegevens als fundament voor het ontwerp, realisatie en doorontwikkeling van de dienst en richt het beheer hiervan goed in.
Standaardiseer waar mogelijk	Standaardiseer waar het kan, maak specifiek waar het moet.
Informeer bij de bron	Maak bij de dienst gebruik van gegevens die afkomstig zijn uit een bronregistratie.
Maak diensten schaalbaar	Bereid de dienst voor op veranderende werklast of reikwijdte.
Bouw diensten modulair op	Maak bij de ontwikkeling van diensten gebruik van een modulaire indeling met een maximale interne samenhang en minimale externe koppelingen.
Pas doelbinding toe	Geef burgers en bedrijven de zekerheid dat informatie over hen alleen wordt gebruikt voor de doelen waarvoor deze oorspronkelijk is verzameld.
Beheers risico’s voortdurend	Maak in alle stappen van ontwerp en doorontwikkeling van de dienst de risico's inzichtelijk en stuur op een afgewogen beheersing ervan.
Verifieer altijd	Verifieer doorlopend de juiste werking van de componenten en beheersmaatregelen van de dienst.

Ontwerp vanuit de reguliere situatie

Statement	Maak voor de reguliere infectieziektebestrijding een informatievoorziening die geschikt is voor opgeschaald gebruik.
Rationale	De infectieziektebestrijding (IZB) in Nederland dient naadloos opgeschaald te kunnen worden in geval van een pandemie, met als kernuitvoerders RIVM en GGD'en. Processen en applicaties, die tijdens een pandemie nodig zijn maken gebruik van de data, die in de reguliere situatie wordt gegenereerd en gebruikt. Het komt de leerbaarheid, beheerbaarheid van de IV/ICT voorzieningen ten goede, als deze regulier al in gebruik zijn; eventuele fouten worden gesignaleerd en opgelost. Kortom: routine in gebruik, routine in dataverwerking en routine in het beheer van de voorzieningen vergroot het vermogen om op te schalen in geval van een pandemie.
Implicaties	We voeren geen projecten uit, waarvan het resultaat/de resultaten uitsluitend in een pandemische situatie worden gebruikt. Voor voorzieningen, die worden ontworpen en gebouwd om alleen in geval van een pandemie gebruikt te worden, is alleen een argumentatie waarom wordt afgeweken van dit principe niet voldoende. Er moet worden geborgd dat deze: - Volgens een vooraf bepaalde cyclus worden getest met herijkte requirements - Volgens een vooraf opgesteld plan worden meegenomen in de OTO-cyclus

Neem gegevens als fundament

Statement	Gebruik gegevens als fundament voor het ontwerp, realisatie en doorontwikkeling van de dienst en richt het beheer hiervan goed in.	
Rationale	De kwaliteit en toegankelijkheid van gegevens bepaalt de waarde van de dienst. De onderliggende gegevens kennen meestal een veel langere levenscyclus dan de systemen waarin deze verwerkt worden. Als gegevens op duurzame wijze toegankelijk zijn gemaakt voor mens én machine kunnen deze gegevens dienen als fundering voor verschillende diensten in verschillende toepassingen, door de tijd en over de hele keten heen. Daarom is het essentieel dat het beheer van gegevens in de keten op orde is, vanaf het ontstaan ervan tot en met de vernietiging (conform bewaartermijnen). Voorzieningen die worden ontworpen en gebouwd om tzt in het geval van een pandemie pas gebruikt te worden zullen qua functionaliteit en technologie achterhaald zijn op het moment, dat zij nodig blijken te zijn.	
Implicaties	Beschrijf informatieobjecten in een model Bevorder hergebruik van gegevens Draag zorg voor juiste en actuele en volledige informatie Hanteer bewaartermijnen voor informatie Leg auditlogs vast bij de bronregistratie van het gegeven Leg de context van een informatieobject vast in metadata Maak gegevens herleidbaar tot de bron (herkomst)	Maak zoveel mogelijk data beschikbaar als open data Pas de FAIR dataprincipes toe Sla informatie op in een duurzaam toegankelijk bestandsformaat Stel van ieder gegeven de kwaliteit vast Stel voor ieder gegeven de unieke bron vast Stel één verantwoordelijke vast voor ieder gegeven Voorkom verlies van informatie

Standaardiseer waar mogelijk

Statement	Standaardiseer waar het kan, maak specifiek waar het moet.	
Rationale	Standaardisatie reduceert variëteit en kosten, en zorgt voor een betere interoperabiliteit en beveiliging. Hiermee komt bovendien een grotere wendbaarheid tot stand. Door te kiezen voor open standaarden wordt vendor lock-in voorkomen.	
Implicaties	Gebruik de standaard met het meest specifieke werkingsgebied Gebruik een actueel register met standaarden Gebruik gestandaardiseerde referentiedata Gebruik open standaarden voor modellering Gebruik standaard oplossingen (implicatie) Gebruik standaard oplossingen zonder maatwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS Maak afspraken over nieuwe (en oude) versies van standaarden Pas je eigen proces en organisatie aan aan de standaard oplossing Pas open standaarden toe Pleeg onderhoud op de toegepaste standaarden

Informeer bij de bron

Statement	Maak bij de dienst gebruik van gegevens die afkomstig zijn uit een bronregistratie.	
Rationale	Voor betrouwbare dienstverlening is het hergebruik van de juiste informatie en documenten van cruciaal belang. Om de kwaliteit over de juistheid van een gegeven te borgen, moet duidelijk zijn welke organisatie bepaalt wat de juiste informatie is. Uitgangspunt is dat er voor gegevens waar de overheid gebruik van maakt, altijd één bron bestaat, die leidend is.	
Implicaties	Bepaal autorisaties met metadata Bevorder hergebruik van gegevens Geef de voorkeur aan halen i.p.v. brengen van gegevens Gegevens eenmalig uitgevraagd, uniek opgeslagen, meervoudig gebruikt Koppel bronsystemen op basis van een passende classificatie Weet welke (bron)gegevens in huis zijn	Registreer gegevens bij de bron Stel de juridische aansprakelijkheid per gegevensobject vast Stel voor ieder gegeven de unieke bron vast Verwijs naar de bron

Maak diensten schaalbaar

Statement	Bereid de dienst voor op veranderende werklast of reikwijdte.
Rationale	Een schaalbare dienst kan omgaan met zowel verwachte als onverwachte intensivering of extensivering. Dit waarborgt de beschikbaarheid van de dienst en hiermee ook de wendbaarheid. Het voorkomt het ad hoc en onder hoge tijdsdruk realiseren van het opschalen van de dienst.
Implicaties	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS

Bouw diensten modulair op

Statement	Maak bij de ontwikkeling van diensten gebruik van een modulaire indeling met een maximale interne samenhang en minimale externe koppelingen.	
Rationale	Door diensten modulair op te bouwen en te ontkoppelen wordt de flexibiliteit vergroot, wat leidt tot meer wendbaarheid, meer hergebruik en duurzaamheid.	
Implicaties	Diensten vullen elkaar aan (implicatie) Koppel bronsystemen op basis van een passende classificatie Ontwerp diensten met oog voor doelbinding en grondslag Ontwerp op modulaire wijze	Scheid proces van data Scheiding van datasets Verwerk bericht-interactie persistent Wissel gegevens tussen (web)applicaties uit met API’s Zorg voor open specificaties

Pas doelbinding toe

Statement	Geef burgers en bedrijven de zekerheid dat informatie over hen alleen wordt gebruikt voor de doelen waarvoor deze oorspronkelijk is verzameld.	
Rationale	Afspraken over het gebruik van informatie zijn nodig voor een vertrouwen in de dienstverlening. Door informatie niet te gebruiken voor andere processen of diensten binnen de overheid, wordt zekerheid naar burgers en bedrijven geboden.	
Implicaties	Leg de doelbinding vast in de metadata van het gegevensobject Leg de grondslag en het doel van de gegevensverwerking vast Minimaliseer het gebruik van gegevens Neem oorspronkelijke grondslag mee bij hergebruik diensten	Ontwerp diensten met oog voor doelbinding en grondslag Stel betrokkenen op de hoogte van het doel waarvoor gegevens verzameld worden Stel de juridische aansprakelijkheid per gegevensobject vast

Beheers risico's voortdurend

Statement	Maak in alle stappen van ontwerp en doorontwikkeling van de dienst de risico's inzichtelijk en stuur op een afgewogen beheersing ervan.	
Rationale	Wanneer helder in beeld is welke gevaren en bedreigingen van toepassing zijn voor de dienst, kun je gepaste beheersmaatregelen nemen. De manieren waarop componenten kunnen falen of hoe er misbruik van kan worden gemaakt zijn onderdeel van de risicoanalyse. Telkens kan dan de afweging worden gemaakt in welke mate de kosten en inspanningen van verdere mitigatie in verhouding staan tot de gevolgen als een risico zich voordoet. De bereidheid van de overheidsdienstverlener om restrisico's te accepteren maakt onderdeel uit van de afweging. Door risico's tijdig te onderkennen zijn beheersmaatregelen effectiever en efficiënter te implementeren.	
Implicaties	Bepaal de continuïteitseisen	Maak beveiligingsmaatregelen zo gebruiksvriendelijk mogelijk
	Bewaak de continuïteit en stel een calamiteitenplan op	Reduceer rest-risico's
	Borg de vertrouwelijkheid van gegevens in maatregelen	Segmenteer het netwerk
	Controleer de verwerking van gegevens	Stel onweerlegbaarheid vast
	Evalueer de risicoanalyse bij veranderingen	Versleutel gegevens in rust en transport
	Garandeer de beschikbaarheid van systemen	Zorg dat software up-to-date is
	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	

Verifiëer altijd

Statement	Verifieer doorlopend de juiste werking van de componenten en beheersmaatregelen van de dienst.	
Rationale	Vertrouwen in het service-niveau van een overheidsdienstverlener, in de beschikbaarheid van een dienst, in de betrouwbaarheid van informatie, in de werking van een component, of de adequaatheid van beheersmaatregelen, is alleen gerechtvaardigd als de componenten en beheersmaatregelen van de dienst doorlopend wordt geverifieerd.	
Implicaties	Hanteer het zero-trust model	Segmenteer het netwerk
	Maak stelselafspraken over identificatie en authenticatie	Stel onweerlegbaarheid vast
	Maak toegang tot applicaties en gegevens afhankelijk van authenticatieniveau	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces
	Richt een sterke logging en audit-trail in	Verifieer de werking van algoritmes
		Verleen alleen strikt noodzakelijke toegangsrechten

Bedrijfsfunctiemodel IZB

- Het bedrijfsfunctiemodel IZB geeft – op het hoogste niveau – de verschillende functies weer, die moeten worden ingevuld (en daarmee ook ondersteund door IV/ICT) om infectieziekten effectief te kunnen bestrijden.
- Tijdens de sessies om te komen tot het HLD is – op basis van het voorbeeld van de ziekenhuis referentie architectuur (ZiRA) - de eerste aanzet tot een bedrijfsfunctiemodel IZB gedaan samen met domeinexperts.
- Dit bedrijfsfunctiemodel IZB wordt weergegeven op de volgende pagina.
- Het bedrijfsfunctiemodel IZB wordt nader uitgewerkt en ingevuld. De (nu nog) hoog over functies zullen binnen de twee organisaties (RIVM en GGD) nader worden uitgewerkt aan de hand van de proces- en informatielagen (uit het vijflaagsmodel van de NORA).
- Het opstellen van het bedrijfsfunctiemodel IZB legt de verschillen in begrippen tussen betrokkenen binnen het IZB bloot. Het benadrukt de noodzaak te komen tot eenheid van begrip en taal via het IZB domeinmodel.

Sturingsfuncties

Outbreak Management | Beleid | Verantwoording | Strategie (Scenario-ontwikkeling) | Performance Management | Planning & control | Kwaliteits-management

Communicatie
- Informeren
- Voorlichten
- Adviseren
- Stakeholder mgt
- CRM / relatiebeheer

Primaire functies

Bevolking

Doelgroep

Individu

Leefomgeving

Diagnostiek
- Testen
- Beeld-vorming

Aanvullend onderzoek
- Sequencing
- Typering

Melding

Surveillance
- Signalering
- Monitoring
- Humaan (o.a.Bron en contact-onderzoek)
- Dierlijk (Zoönose)
- Milieu (Riool)
- Kiem-surveillance

Interventie (preventief/correctief)
- Maatregelen (isolatie, quarantaine, tijdelijke sluiting)
- Therapie/behandeling
- Vaccineren
- Innovatieve (digitale) interventies

Wetenschappelijk onderzoek en innovatie

(Bedrijfs)ondersteunende functies

Supplychain Management | Inkoop | Capaciteit Management | Personeel & Organisatie | Keten- & Proces Optimalisatie | IV/ICT Beheer | Financiën & Control | Facilitair Management | Opleiden Trainen en Oefenen (OTO)

Bedrijfsfuncties – Primaire functies

Primaire functies zijn direct gericht op het uitvoeren van de infectieziektebestrijding.

Functie	Uitleg
Diagnostiek	(Medisch) onderzoek (al dan niet in een laboratorium) om een diagnose te stellen, of het verloop van een therapie te volgen.
Aanvullend onderzoek	
Melding	De mogelijkheid van het doen van een melding van het (vermoeden van) voorkomen van een meldingsplichtige ziekte.
Surveillance	Het continu bewaken van het voorkomen en verspreiden van infectieziekten.
Interventie (preventief/ correctief)	Het kunnen uitvoeren van maatregelen die tot doel hebben preventie te bevorderen en/of correctief te werken.
Communicatie	Overdracht of uitwisseling van informatie.

Bedrijfsfuncties – Sturingsfuncties

Sturingsfuncties hebben betrekking op het kunnen uitvoeren van sturing op de keten en losse functies binnen de IV voor de IZB

Functie	Uitleg
Outbreak management	Het nemen van maatregelen om een uitbraak van een infectieziekte te voorkomen, c.q. te beheersen.
Beleid	De richtlijnen voor diagnose en behandelmethoden, en ook aangescherpte criteria voor opname en ontslag van besmette patiënten, worden opgesteld door het landelijke Outbreak Management Team (OMT) en uitgevaardigd door de minister van VWS.
Verantwoording	Verantwoording wordt afgelegd aan de Tweede Kamer.
Strategie	Het bepalen van strategische keuzes zoals analyseren, doorrekenen en ontwikkelen van scenario's over het verloop van infectieziekten.
Performance management	Kijkend naar de organisatie(s), de processen, de KPI's, hoe goed doen we het werk en de uitvoering? Laten we ergens nog efficiëntie liggen?
Planning & Control	Een heldere planning & control biedt op alle niveaus binnen de organisatie houvast om op een juiste wijze (bij)sturing te kunnen geven aan de (financiële) processen binnen een organisatie.
Kwaliteits-management	Kwaliteitsmanagement is de tak van het management die streeft naar een zo hoog mogelijke kwaliteit van een product, productieproces, dienst of organisatie.
Communicatie	Het beheer van alle soorten communicatie naar de bevolking van Nederland, specifieke doelgroepen en/of individuen. Heeft directe relatie met functies binnen de (bedrijfs-)ondersteunende functies en primaire functies.

Bedrijfsfuncties - Wetenschappelijk onderzoek

Wetenschappelijk onderzoek betreft het al of niet wetenschappelijk onderzoeken op medisch en niet-medisch gebied en zowel digitaal als niet-digitaal

Functie	Uitleg
Surveillance	Het betreft wetenschappelijk onderzoek naar mogelijkheden tot kiemsurveillance. Binnen dit kader valt ook het onderzoek naar de bijwerkingen van de medische middelen (vaccins/medicatie) waarbij effectiviteit en efficiëntie continu beoordeeld worden.
Interventie	Het onderzoek naar mogelijkheden van innovaties (medische en niet-medisch, digitaal en niet-digitaal) die van toepassing kunnen zijn binnen het functiehuis van de LFI en uitvoeren van de IZB.
Communicatie	

Bedrijfsfuncties – (Bedrijfs) ondersteuningsfuncties

(Bedrijfs)ondersteuningsfuncties vormen de basis, het fundament, van het stelsel. Zonder één van deze functies is het geheel niet bruikbaar om pandemisch paraat te zijn.

Functie	Uitleg
Supply Chain management	De volledige omvang van Supply Chain Management, o.a. planning, voorraad, logistiek.
Inkoop	Direct naast SCM voor het beheren van contracten en het contact met leveranciers (in de meest brede zin).
Capaciteitsmanagement	Naast SCM om vanuit performancemanagement en SCM de capaciteit te monitoren en te sturen.
P&O	Personeel en Organisatie
Keten- en procesoptimalisatie en verandering	Naast de innovatie binnen het (wetenschappelijk) onderzoek kunnen ook dagelijkse signalen leiden tot verandering, optimalisering en/of verbetering van de keten en de processen.
IV-/ICT-beheer	
OTO	Een mogelijkheid voor het uitvoeren van: Opleiden, Trainen, Oefenen. Deze bedrijfsfunctie maakt het mogelijk om in een reguliere situatie te bekijken wat de effecten zijn en hoe de processen lopen bij opschaling in het geval van een pandemische besmetting.
Finance & Control	Het beleid, de procedures en maatregelen, die een organisatie inzet om het gebruik en de allocatie van haar financiële middelen te kunnen sturen.
Facilitair Management	Realisatie en beheer van vaste en tijdelijke locaties tbv uitvoering van de primaire taken

Ontwerpkeuzes

- Datacentrisch
- Modulair

"In een datacentrische architectuur zijn de gegevens het primaire en blijvende bedrijfsmiddel, terwijl applicaties komen en gaan. In een datacentrische architectuur gaat het datamodel boven de implementatie van welke applicatie dan ook. Het datamodel blijft aanwezig en blijft valide, lang nadat een applicatie is verdwenen."

Dave McComb (2019)

Datacentrisch, wat betekent dat?

De basisgedachte van datacentrisch werken en denken is:

- data worden losgekoppeld van werkprocessen en applicaties.
- data worden iedere keer opgevraagd bij de bron, in plaats van ze veelvuldig te kopiëren en op te slaan.

Datacentrisch werken stelt de gegevens in logische zin centraal. Dit zegt dus niets over de plek waar gegevens fysiek worden opgeslagen.

Datacentrisch, de rationale

- **Data is voor ons een zeer waardevolle asset, we nemen de beschikbaarheid en kwaliteit van data als vertrekpunt.**
- Voor de wendbaarheid en de opschaling van processen en systemen is een stabiel, eenduidig datafundament cruciaal, zodat een groot aantal **verschillende** partijen onder tijdsdruk effectief kunnen blijven handelen op basis van **dezelfde** informatie(gegevens). Cruciaal: in een crisissituatie is er geen tijd om het eens te worden over de betekenis van data.
- Levensduur van data is veelal langer dan die van processen en applicaties.
- Essentiële aspecten van data vormen een integraal onderdeel van die data (in plaats van verschillende applicaties, systemen en processen met elk hun eigen interpretatie):
  - **Semantiek** (duiding)
  - **Vertrouwen** (kwaliteit etc.)
  - **Beveiliging** en **privacy**
- Stelt ons in staat om – daar waar nodig en/of nuttig – te komen tot een uniforme aanpak.
- We willen af van de situatie waarbij data van applicatie naar applicatie naar applicatie worden getransporteerd, en onderweg de betekenis ervan verloren gaat of verandert. Als data niet meer telkens verplaatst hoeft te worden, draagt dit bij aan de tijdigheid (near-realtime) en de kwaliteit van die data én de kwaliteit van het resultaat van de verwerking op/met die data.
- Burgers en professionals hebben veel ‘toegangspaden’. Het is dan van belang dat die paden wel naar dezelfde data en resultaten leiden. Bijvoorbeeld persoonlijke gezondheidsdossiers en toestemmingen (MITZ) voor burgers baseren zich op dezelfde gegevens als applicaties voor de professionals.
- We willen soevereiniteit over onze data. We tolereren niet dat data ‘gegijzeld’ zitten in de applicaties van leveranciers.

Datacentrisch, de rationale (2)

Data-soevereiniteit, wat is dat?

- Data-soevereiniteit verwijst naar het concept waarbij de bij de IZB betrokken organisaties controle hebben over hun eigen gegevens, inclusief:
  - De betekenis,
  - Wie er toegang toe heeft en,
  - Hoe ze worden gebruikt.
  - Waar deze worden opgeslagen,
- Het draait om het idee, dat data-eigenaren zelf de zeggenschap moeten hebben over hun gegevens, ongeacht waar deze zich bevinden of worden verwerkt.

Afhankelijkheid van data

Infectieziektebestrijding is sterk afhankelijk van de tijdige beschikbaarheid van correcte en complete data

Voorbeelden van data en bronnen die een rol spelen binnen de IZB. Deze bronnen bevatten inhoudelijke data met betrekking tot een/de infectieziekte, maar ook sturingsgegevens over bijvoorbeeld de uitvoering en de processen.

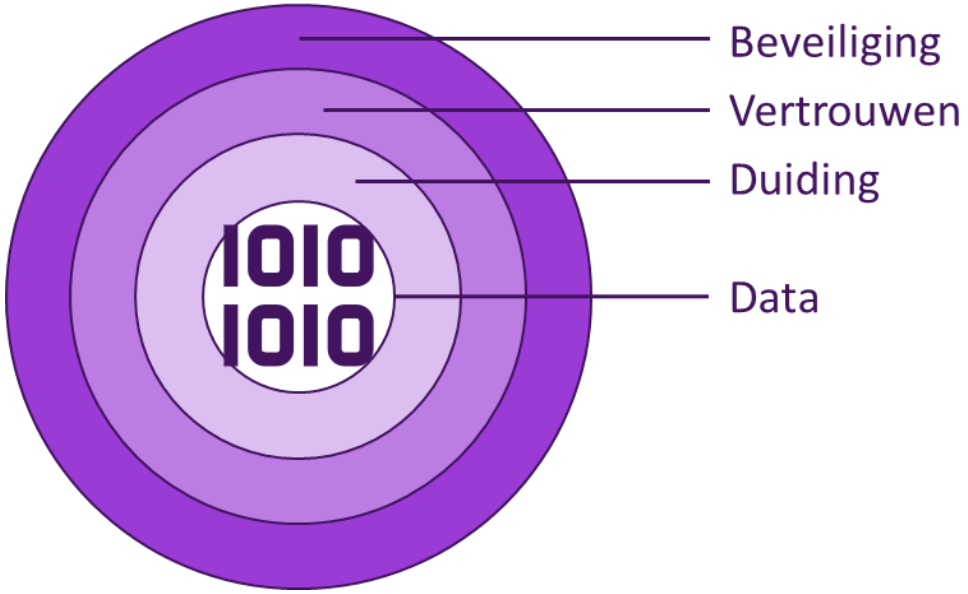
Probleem	Uitleg
Omgevingsdata	Riool, kiem, surveillance. Dit betref data uit de (leef)omgeving, dus niet mens- of diergebonden, over het voorkomen van de infectieziekte in de meest uitgebreide, denkbare vorm.
Test- en diagnostische data	Het betreft alle data vanuit o.a. laboratoria op basis waarvan een conclusie kan worden getrokken. Hierbij wordt niet beperkt tot data op basis van een bloed-/speekselmonster, maar wordt uitdrukkelijk ook beeldmateriaal en mogelijk ook andere vormen van diagnostiek bedoeld.
Vaccinatieregistratie	Vaccinatie ≠ inenten. Deze registratie bevat dus vastlegging van de toediening van een vaccin.
Opnames	Ziekenhuis, IC. Voor het kunnen traceren van effectiviteit en efficiëntie van een vaccin, kan met deze dataset, bestaande uit ziekenhuisopnames en IC-opnames, gemonitord worden. Daarnaast ook de mogelijkheid om vóór er een vaccin beschikbaar is, de bezetting te kunnen monitoren en eventueel te vergelijken.
Sterftecijfers	Als voorgaande, maar nu beschouwd op mortaliteit van de infectie.
QC en procesdata	
Voorraden en logistieke data	Informatie over waar welke hoeveelheden middelen zich bevinden en/of in bestelling staan.
HR-data	P&O-gegevens; alle personeelsgegevens die van belang zijn voor de beoordeling, ontwikkeling en inzet van mensen.
Afspraken en locaties	Ten behoeve van bijvoorbeeld testen, vaccinatie, consult.
Context data	Scholen, instellingen, locaties.
Openbare bronnen	CBS, Google, (social) media etc.
Sequence data	Gedigitaliseerde informatie over nucleïde acide, proteïne of andere polymeresequenties, afkomstig van next generation en/of whole genome sequencing.
Protocollen en richtlijnen	Van professional, burger etc.
Voorlichtingscontent	Voorlichtingsmateriaal voor professionals en publiek
Toestemmingen en machtigingen	Toestemmingen van natuurlijke personen voor het gebruik van hun (persoons)gegevens, alsmede machtigingen van natuurlijke personen om andere natuurlijke personen daarover te laten beslissen.
Vragenlijsten	Enquêtes, zoals die onder andere gebruikt worden bij bron- en contactonderzoek.
Persoonsgegevens	Informatie over een geïdentificeerde of identificeerbare, natuurlijke persoon, afkomstig van basisregistraties (brp), coa en/of verkregen door middel van informed consent.
Medisch dossier	De schriftelijk of elektronisch vastgelegde gegevens met betrekking tot de verlening van zorg aan een cliënt. Bijvoorbeeld op basis van de Wet Geneeskundige Behandelovereenkomst.

Op te lossen dataproblemen

Welke dataproblemen zijn er op te lossen?

De hiernaast benoemde problemen in de huidige situatie op basis waarvan gesteld is dat Nederland niet voldoende pandemisch paraat was zijn onder andere genoemd. Door naar een datacentrisch ontworpen en ingericht landschap te gaan wordt beoogd deze problemen op te lossen.

Probleem	Uitleg
Data lost in traffic	Betrouwbaarheid van connecties tussen systemen. De volledigheid van uitwisseling is niet te garanderen.
Data lost in translation	Geen goede afstemming gebruikt datamodel, identifiers en standaarden.
Data vertraagd	Data wordt bulkgewijs aangeleverd waardoor onduidelijk is wat de actuele status is. De sturing werkt altijd op verouderde data.
Data niet schaalbaar	De omvang van de data in het bestrijden van de pandemie was niet bekend, waardoor een best guess nog niet genoeg bleek om de werkelijke omvang van de data die over en weer werd uitgewisseld, te bepalen.
Servicelevels in ketens	Indien een keten van 3 partijen elk een servicelevel van 80% heeft, betekent dit dat de keten 'slechts' een servicelevel van 51,2% (80%*80%*80%) heeft.
Datakwaliteit	Door de vele en diverse vrije invulvelden (typering van de inhoud van het veld is wel eenduidig) kan niet gegarandeerd worden dat de inhoud ook correct is.
Ingangen	Burger en professionals hebben (te) veel plaatsen (zoals websites) waar ze informatie halen/brengen, waardoor onduidelijk is waar welke data 'ligt', en is het verkrijgen van een totaalbeeld door de burger of professional niet mogelijk.
Externe partijen	Er zijn veel externe partijen betrokken in de bestrijding van de COVID-19-pandemie. Dit vroeg veel ad-hoc koppelingen met issues betreffende veiligheid, toegang en integratie, waardoor het verkrijgen van een totaalbeeld of een volledig beeld niet mogelijk of zeer moeizaam bleek.
Traag	Trage applicaties voor nieuwe processen. Er was in de aanvang van de bestrijding van de COVID-19-pandemie niet duidelijk welke omvang de diverse applicaties, systemen en datasets zouden krijgen, en welke eisen daarmee aan rekenkracht, opslagcapaciteit en doorvoer gesteld moesten worden. Het opschalen van diverse componenten was niet altijd even makkelijk, waardoor het geheel trager reageerde dan wenselijk.



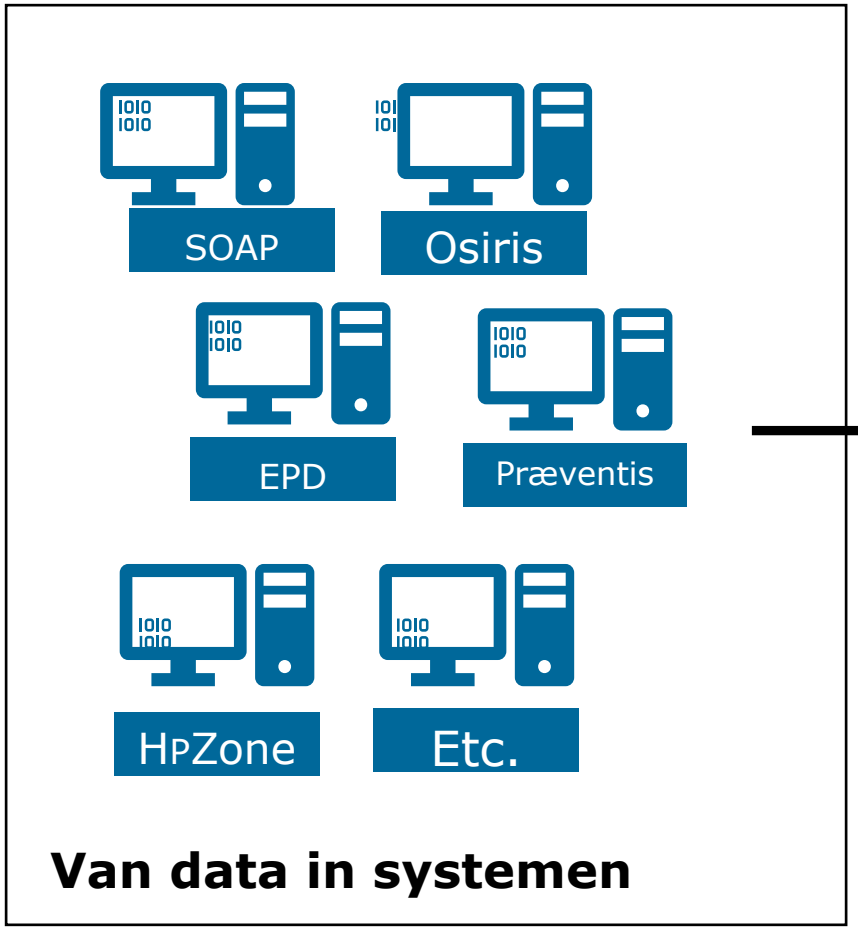
Datacentrisch, wat impliceert dat? (I)

- Datacentrisch impliceert dat we **vooraf** nadenken (èn dus ook moeten meenemen in aanbestedingen, programma's van eisen, etc.) over:
  - Data
  - Duiding
  - Vertrouwen
  - Beveiliging

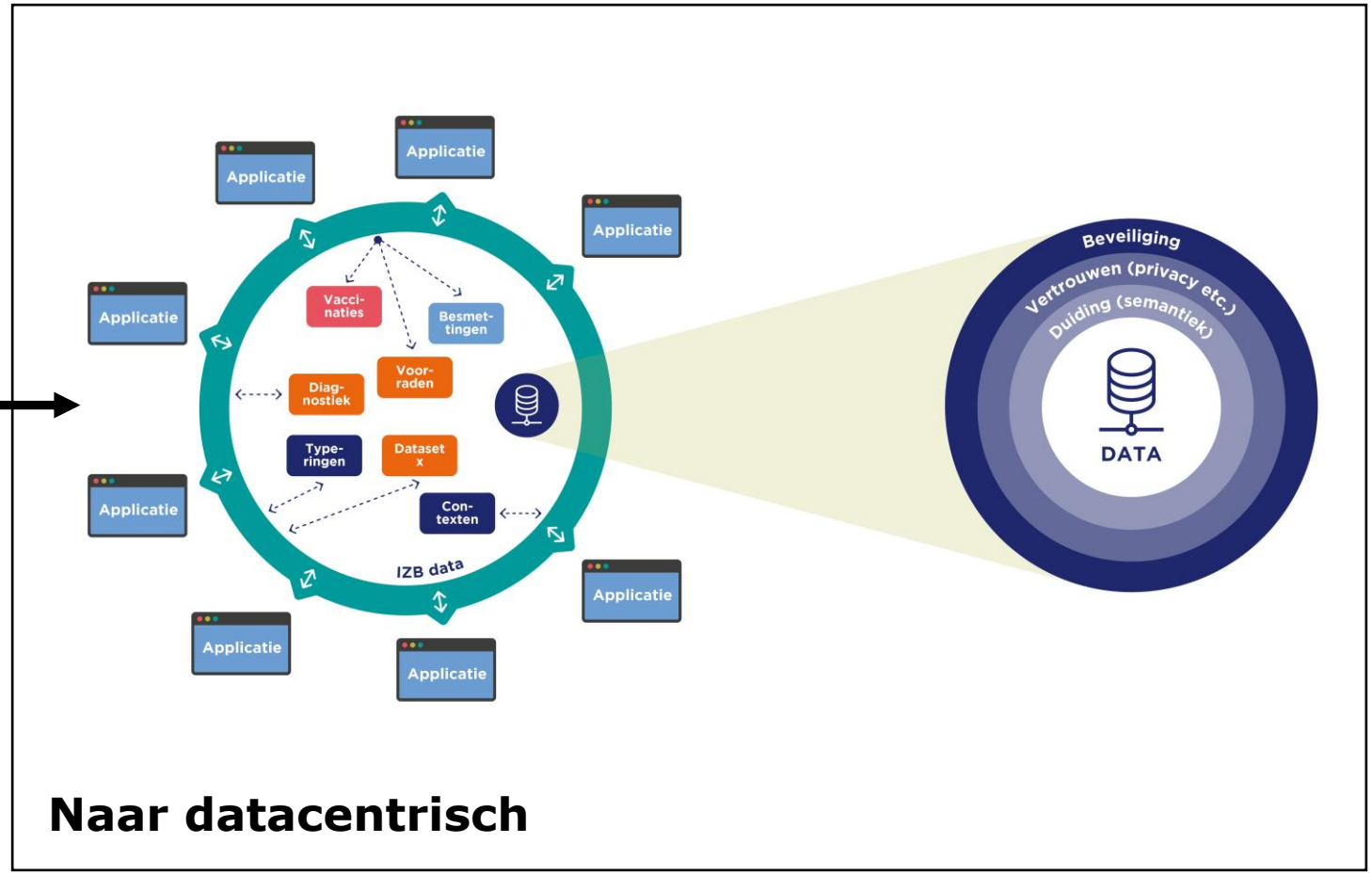
Datacentrisch, wat impliceert dat? (II)

- **Data**
  - Ieder data-element (kleinste eenheid van data) heeft één bron.
  - Ieder data-element kent één verantwoordelijke, die instaat voor de betekenis, toegangsrechten, gebruik en kwaliteit ervan.
  - De data bestaat onafhankelijk van het gebruik ervan door applicaties.
- **Duiding**
  - Betekenis is vastgelegd in een domeinmodel.
  - Businessrules zijn onderdeel van het domeinmodel.
  - We sluiten aan bij (inter)nationale standaarden (OpenEHR, loinc, snomed, cdisc, etc.) en dragen daar waar nodig of mogelijk aan bij.
- **Vertrouwen**
  - gaat over de kwaliteit van de data, het monitoren van die datakwaliteit, en de processen waarmee de kwaliteit wordt geborgd. Kwaliteitsdimensies zijn:
    - Accuratesse
    - Compleetheid
    - Consistentie
    - Uniciteit
    - Validiteit
    - Tijdigheid
    - Courantheid
    - Conformiteit Integriteit
- **Beveiliging**
  - De data is beschikbaar.
  - De data is beveiligd opgeslagen.
  - De toegang tot de data is beveiligd.

Applicatie-centrisch versus datacentrisch



Van data in systemen



Naar datacentrisch

Samenwerking tussen bestaande en datacentrische systemen

- Een datacentrisch landschap is een stip op de horizon, een toestand die incrementeel wordt behaald op de volgende wijze:
  - Bij grootschalige vernieuwing of vervanging van bestaande applicaties: pas de nieuwe DC principes toe.
  - Bestaande applicaties integreren met behulp van
    - API laag leggen bovenop bestaande applicaties/data
    - Data aggregatie toepassen om bestaande data (read only) te integreren (ETL, Datawarehouse, Datavirtualisatie)
  - Herinrichting van de data huishouding, zodat een geheel van voorzieningen, faciliteiten, functies en systemen ontstaat, waarmee data - in overeenstemming met wet- en regelgeving en beleid - vindbaar, toegankelijk, deelbaar en herbruikbaar (FAIR)wordt gemaakt en invulling gegeven kan worden aan de datacentrische gedachte.
- Aansluiting maken tussen bestaande en nieuwe patronen via de basisvoorzieningen (volgend hoofdstuk) Data Intelligence en Koppelvlak

De rol van een domeinmodel in een datacentrische informatievoorziening

Een datacentrische informatievoorziening is een informatievoorziening, waarbij de applicatie functionaliteit 'losjes' gekoppeld is aan één enkel, eenvoudig, uitbreidbaar, federeerbaar, universeel, gedeeld en direct implementeerbaar **domeinmodel**.

- **'Losjes gekoppeld'**: de applicatie is niet door code gekoppeld aan het dataopslagsysteem maar de dataopslag kan probleemloos vervangen worden door een andere dataopslagsysteem. Een 'loosely coupled system' is een systeem waarin elk van de componenten geen of weinig kennis heeft of gebruikt van de definities van andere componenten.
- **Eén enkel**: niet één datamodel per applicatie, maar een gedeeld model, waarin verschillende disjuncte modellen met elkaar verenigd worden voor de hele organisatie.
- **Eenvoudig**: niet vele concepten per applicatie die niet gebruikt worden of voorkomen in meerdere applicaties maar een paar honderd concepten waarmee de hele organisatie beschreven kan worden.
- **Uitbreidbaar**: niet een nieuwe applicatie maken voor een nieuwe taak maar uitbreiden van bestaande functionaliteit.
- **Federeerbaar**: niet data verplaatsen maar een vraag over meerdere systemen tegelijk heen kunnen stellen.
- **Universeel**: niet verschillende data structuren transformeren maar alle datastructuren opdelen in de elementaire semantische bouwblokken.
- **Gedeeld**: niet data kopiëren maar data delen.
- **Direct implementeerbaar**: niet een apart conceptueel, logisch en technisch model maar één semantisch datamodel.

Bron: Dave McComb

De principes t.a.v. de datacentrische informatievoorziening

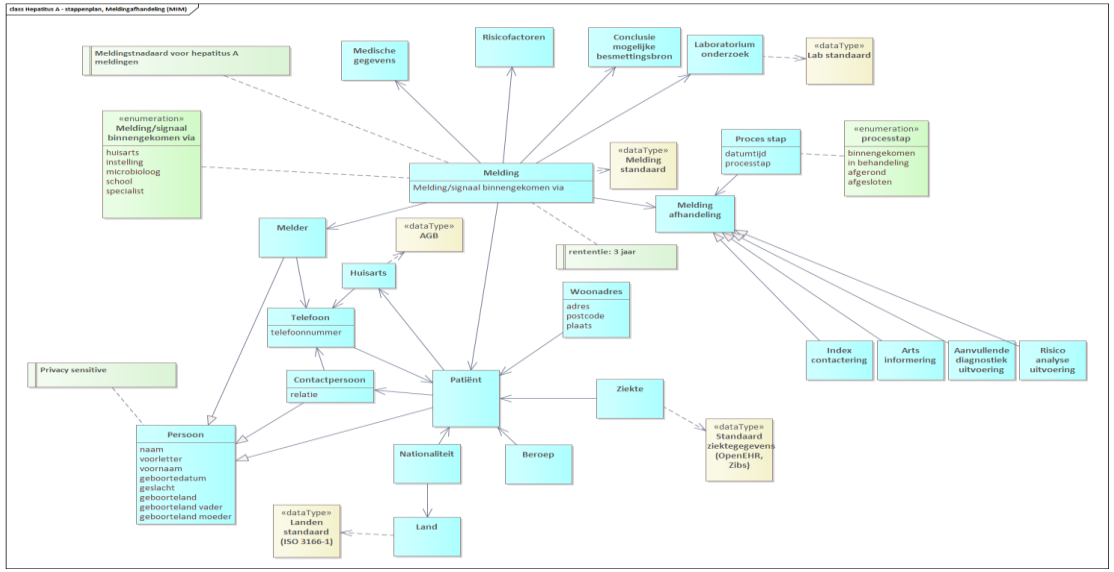
- **Datacentrisch werken gaat voor applicatie gerichte informatievoorziening.**
- **Concreet betekent dit:** Bij de oplossingsrichtingen gaat de voorkeur uit naar een splitsing tussen applicatie en dataopslag. De dataopslag moet daarmee beschikbaar kunnen worden gesteld binnen het IZB-domein. Mocht die splitsing er niet zijn, dan moet op z'n mist koppel (API) functionaliteit zijn die de kerngegevens van het geheel ontsluit.
- Uitzonderingen op deze regel zijn:
  - Als bij een aanbesteding geen van de opties deze splitsing aanbiedt.
  - Data van bedrijfsfuncties die in het kader van IZB niet deelbaar hoeven te zijn **en** waarvoor de organisatie zelf verantwoordelijk is. Hieronder vallen: HR-gegevens en financiële gegevens

Wat is een IZB domeinmodel?

- Een gestructureerde kennisbank over en voor de gezamenlijke infectieziektebestrijding in de:
  - reguliere
  - en pandemische fase
- Met als doel:
  - de verbetering van de communicatie en samenwerking in de IZB
  - en een pandemisch parate, wendbare, data-centrische, modulaire informatievoorziening
- Waarin:
  - informatie, betekenis, bedrijfsregels en datatoegang centraal staan en eenduidig zijn vastgelegd
  - in samenhang met processen enerzijds
  - en applicatiefuncties anderzijds
- Bestaande uit:
  - verschillende samenhangende weergaves voor verschillende stakeholders
- Ontwikkeld in:
  - verschillende modeleertalen
  - gebruik makend van verschillende soorten modelleer disciplines
  - door verschillende ontwikkelaars met verschillende methoden en verschillende vaktermen

Domeinmodel - wat

- Een domeinmodel is een weergave van betekenisvolle concepten uit de echte wereld die betrekking hebben op dat domein. De concepten omvatten de gegevens die bij het domein zijn betrokken en regels die het domein gebruikt met betrekking tot die gegevens. Een domeinmodel maakt gebruik van de natuurlijke taal van het domein.
- Een domeinmodel geeft invulling aan de semantiek, doelbinding, het vertrouwen en de beveiliging van de data en stuurt het juiste begrip en het juiste gebruik ervan.
- Een verzameling data over je data.
- Bevat de definitie, betekenis en structuur van:
  - Data/informatie
  - Bedrijfsregels
  - Bedrijfsgebeurtenissen
  - Bedrijfsactiviteiten
  - Bedrijfsfuncties
  - Verantwoordelijkheden en rollen
  - Autorisatiemodel
  - Resultaten
  - Privacyaspecten: doelbinding en grondslagen
  - Integriteitseisen
  - Bewaartermijnen
  - Schaalbaarheid
  - Pandemische eisen



- "An object model of the domain that incorporates both behavior and data." Martin Fowler.

Domeinmodel - waarom

We kunnen redeneren over ons eigen werkveld

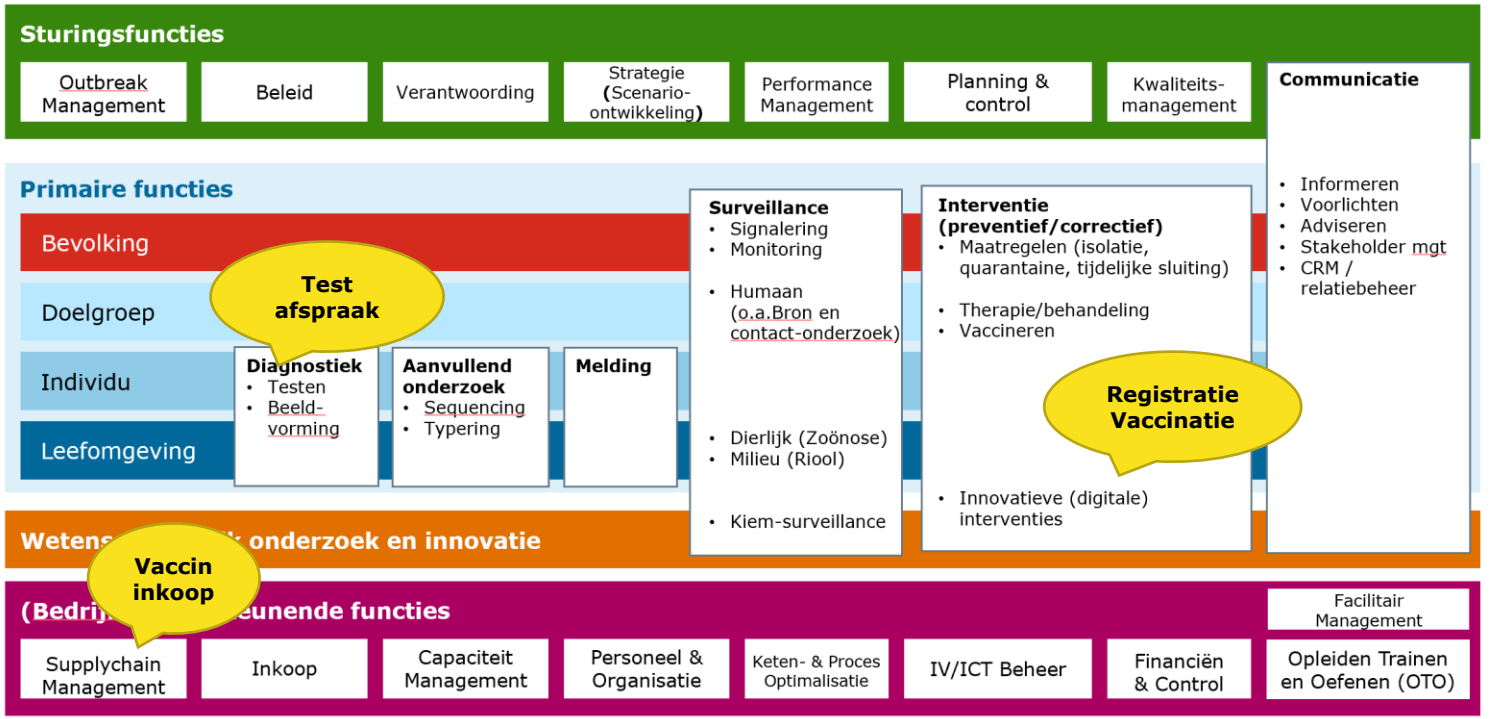
- Door het eenduidig vastleggen van het beeld van de werkelijkheid
- Zodat we duidelijkheid hebben over de betekenis, herkomst en totstandkoming van de data.
- Om de kwaliteit van je eigen informatiehuishouding op orde te hebben.
- Om ieder te laten beschikken over dezelfde hoogwaardige gegevens.
- Om het delen van gegevens met anderen beter (eenduidiger, sneller) te laten verlopen.
- Zodat we beter met elkaar kunnen communiceren.
- Zodat we beter kunnen samenwerken.
- Zodat de werking van de organisatie inzichtelijk is.
- Zodat we beter onze gemeenschappelijk doelen/resultaten kunnen behalen.
- Zodat we geruisloos over kunnen gaan van een regionale naar een landelijke aansturing en weer terug.
- Zodat we de toegang tot data kunnen verbeteren.

Domeinmodel - hoe

- Het maken en onderhouden van een domeinmodel is een proces, taal is levend, inzichten veranderen, mensen komen en gaan.
- We maken en onderhouden de domeinmodellen gezamenlijk:
  - IT en IZB professionals
  - Privacy en informatiebeveiliging
  - GGD, GGD GHOR Nederland, RIVM en LFI
- We volgen de Wegiz en sluiten aan bij de nog in te richten governance voor de doorontwikkeling van informatiestandaarden in de zorg (zie ook Afwegingen voor publiek houderschap van een stelsel van informatiestandaarden in de zorg)
- Aansluiten op ketenstandaarden voor uitwisseling met partners:
  - Logius, Nictiz, Laboratoria, VVT, Huisartsen,…
- Het opstellen van een domeinmodel wordt én via een praktische en formele benadering uitgevoerd:
  - Praktisch: start de analyse vanuit de ketenprocessen en keteninformatieobjecten → geeft overzicht en structuur en sluit aan bij de belevingswereld van professionals.
  - Formeel: abstraheer en detailleer de concepten tot een eenduidig model → geeft inzicht en details en sluit aan bij formele specificaties voor IT leveranciers.
- In de reguliere fase zal het domeinmodel steeds stabieler worden. De opgebouwde kennis én samenwerking ondersteunt het snel doorvoeren van wijzigingen in een opgeschaalde fase, als het model om uitbreiding of aanpassing vraagt.

Voorbeelden van de afbakening van domeinmodel

- Typisch voorbeeld gezamenlijk domeinmodel en bijbehorende datasets:
  - Vaccinatie gezet bij een persoon [Gezamenlijke definitie]
- Typisch voorbeeld afzonderlijk domeinmodel en bijbehorende datasets:
  - Vaccinlogistiek, inkoop bij farmacie [RIVM]
  - Testafspraken plannen [GGD]



Aanbeveling domeinmodel en datacentrisch werken (1/2)

- Ontwikkel en beheer een domein-model voor de infectieziektebestrijding.
- Breng de totstandkoming en het onderhoud van dit domeinmodel onder een gezamenlijke governance en beheer van RIVM en GGD.
- Beproef de scope van het domeinmodel, bepaal wat wel/niet onderdeel kan zijn van het model en bepaal de toepassingen van het model.
- Regel de governance in:
  - Werk aan één model op basis van gedeelde tool.
  - Zoek aansluiten bij andere organisaties/initiatieven: VWS, Nictiz, ZIN, Health-RI, LFI.
  - Zorg voor een nationale "health data authority". Nu heeft VWS deze regierol tijdelijk naar zich toe getrokken.
- Richt de data governance gezamenlijk (voor RIVM en GGD'en) in.
- Beleg de verantwoordelijkheid voor datadefinities bij de domeinexperts.
- Maak afspraken over de methodologie en de gereedschappen waarmee de domeinmodellen worden onderhouden.
- Wissel de domeinmodellen uit, geef inzicht in elkaars domeinmodellen en "naar buiten" (vgl. publicatie van open source).
- Bepaal wie de bronhouder is.
- Stem dit domeinmodel af met andere belanghebbenden in de infectieziektebestrijding, zoals:
  - Medisch Microbiologische Laboratoria
  - Zorgaanbieders (huisartsen, ziekenhuizen, zorginstellingen, etc.)
  - Overheden en internationale agentschappen zoals ECDC en de WHO
  - Etc.
- Domeindefinities zijn gedeeld tussen GGD'en en RIVM (en eventueel anderen), waarbij grondslagen en toegang zijn geborgd in de schil om de data heen (vertrouwen en beveiliging)

Aanbeveling domeinmodel en datacentrisch werken (2/2)

- Beschrijf domeinen consistent en richt centraal de datagovernance daarop in. Zorg hierbij voor de aansluiting op internationale initiatieven en wetgeving zoals de verordening tot oprichting van een Europese ruimte voor gezondheidsgegevens.
- Standaardiseer de registratie aan de bron (én standaardiseer op de koppelvlakken).
- Onderzoek het gebruik van klinische standaarden als ZIB's, OpenEHR, CDISC en FHIR voor de medische domeinen.
- Onderzoek de waarde van standaarden op het gebied van vastlegging van informatie én uitwisseling van informatie. Niet iedere standaard heeft dezelfde doelstelling en reikwijdte.
- Onderzoek het gebruik van standaarden voor: informatiemodellen, informatie-uitwisseling, woordenboeken en ontologieën.
- Organiseer voor alle domeinen de metadata en voorzieningen voor betekenis, vertrouwen en beveiliging, (dicht)bij de data. Betrek hierbij bijvoorbeeld ook de privacy-officers en juristen.
- Naar aanleiding van de werksessies is er een "POC datagedreven werken" opgestart door RIVM en GGD:
  - Binnen de Proof of Concept willen we aan de hand van een praktische use cases ervaring opdoen met diverse aspecten van datacentrisch werken. De use case is het registreren en melden van een Hepatitis A infectie.
  - De Proof of Concept wordt opgesplitst in een functioneel en een technisch deel. Het functionele deel zal eerst plaatsvinden en input verzorgen voor het technische deel van de PoC.

Modulair

- We ontwikkelen een modulair ingericht landschap voor infectieziektebestrijding. Door diensten modulair op te bouwen en te ontkoppelen wordt de flexibiliteit vergroot, wat leidt tot meer wendbaarheid, meer hergebruik en duurzaamheid.
- RIVM en GGD'en werken aan de (door)ontwikkeling van hun IV landschap om gezamenlijk de huidige monolieten te transformeren naar twee modulair ingericht landschappen, die zich voor de infectieziektebestrijding gedragen alsof het één is.
- In iedere iteratie van de doelarchitectuur werken we vanuit de backlog van het programma aan de architectuur-uitwerking voor de bouwblokken die nodig zijn om de diensten "alsof het één is" aan te bieden. Bijvoorbeeld voor klantreizen van de burger, of de inrichting van ketenprocessen.
- In de doelarchitectuur richten we ons nu eerst op de basisvoorzieningen.

Bouwblokken nader uitgelegd: Architecture & Solution Building Blocks

- In navolging van TOGAF gebruiken we in deze doelarchitectuur de term bouwblokken.
- Bouwblokken hebben de volgende generieke kenmerken:
  - Een bouwblok is een pakket functionaliteit dat is gedefinieerd om te voldoen aan de zakelijke behoeften van een organisatie.
  - Een bouwblok heeft een gedefinieerde grens en is over het algemeen herkenbaar als "een ding" door domeinexperts.
  - Een bouwblok kan samenwerken met andere, onderling afhankelijke, bouwblokken.
  - Een goed bouwblok heeft verder de volgende kenmerken:
    - Het neemt ook implementatie en gebruik mee in de overweging en evolueert om technologie en standaarden te benutten.
    - Het kan worden samengesteld uit andere bouwblokken.
    - Het kan een subassemblage zijn van andere bouwblokken.
    - Idealiter is een bouwblok herbruikbaar en vervangbaar en goed gespecificeerd.
- We onderscheiden twee verschillende typen bouwblokken:
  - ABB's (Architectural Building Blocks)
    - Vastlegging van architectuurvereisten, zoals eisen ten aanzien van de organisatie, data, applicatie of technologie
    - Geven sturing en begeleiding aan de ontwikkeling van SBB's
    - Zijn merkonafhankelijk en technologie-agnostisch
    - Beschrijven de dienstverlening en zijn daarmee meer dan technologie
  - SBB's (Solution Building Blocks), die kunnen worden verworven of ontwikkeld
    - Definiëren welke producten en componenten de beoogde functionaliteit zullen implementeren
    - Definiëren de implementatie zelf
    - Geven invulling aan de requirements vanuit het primair proces
- Waar in deze doelarchitectuur:
  - de term "**bouwblok**" wordt gebruikt, wordt – tenzij anders vermeld – een ABB bedoeld.
  - Een **basisvoorziening** is: een ABB die door RIVM en GGD onder consensus is gedefinieerd.

Rationale voor een modulair ingericht IV landschap

- Generieke en herbruikbare bouwblokken die bijdragen aan de kwaliteit van de dataontsluiting en de applicaties

EFFICIËNT

Er is een aantal bouwblokken beschikbaar, zodat dezelfde problemen niet door verschillende applicaties/systemen opgelost hoeven te worden (hergebruik).

LEERBAAR

Door één standaardapplicatiebouwblok aan te bieden, voorkomen we dat inhuurkrachten vandaag bij de ene GGD met de ene applicatie, en morgen bij een andere GGD met een andere applicatie moeten leren werken, om dezelfde taak te kunnen uitvoeren (opschaling in gebruik).

WENDBAAR

Het hebben van (bijvoorbeeld) een bouwblok voor digitale identiteiten en authenticatie maakt dat, in geval van een opschaling, op betrekkelijk eenvoudige wijze, extra en andere gebruikers kunnen worden toegevoegd.

TESTBAAR

Performance en schaalbaarheid van bouwblokken die in de opschaling nodig zijn, kunnen worden getest.

Overzicht van mogelijke generieke en herbruikbare bouwblokken

BASISVOORZIENINGEN

De fundamentele bouwblokken van het data-centrisch platform dat door RIVM en GGD in nauwe afstemming wordt gerealiseerd

- Digitale Identiteit (IAM)
- Data Services voor data centrisch werken
- Koppelvlakken
- Security Monitoring (SOC/SIEM)

APPLICATIES

Technologische bouwblok (soms inclusief de benodigde kennis en expertise), die een bepaalde functie faciliteert

Bijvoorbeeld:

- analyse & AI + ML
- callcenter (o.a. telefonie)
- applicatiedistributie
- koppelvlak zelfdiagnostiek (IoT)
- non-digital
- PGO-koppeling (DVA)
- RAD- / Low Code-platform
- toestemming registreren (AVG)
- track & trace
- open data/ open science

Toepassingen bedoeld voor eindgebruikers

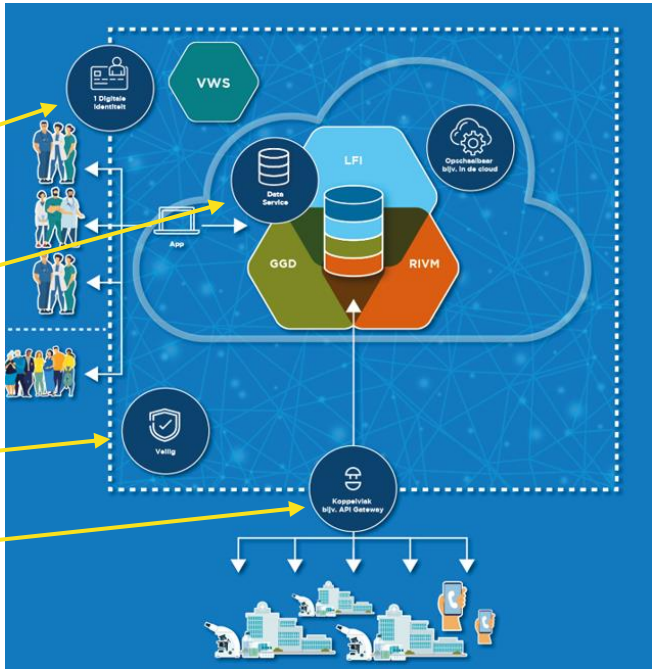
Bijvoorbeeld:

- Izb/bco-applicatie
- surveillancesysteem
- afsprakenmodule
- burgerportaal
- chatdiensten
- contentmanagement
- Finance & Control
- ITSM
- klantcontact (CRM)
- leveranciercontract (SRM)
- meldingenportaal
- BI/Dashboarding
- Risk & Compliance
- samenwerkingsportaal
- securitymonitoring (SOC/SIEM)
- Supply Chain Management (ERP)
- vragenlijstmodule
- webcare/ socialmedia-monitoring

Basisvoorzieningen

De basisvoorzieningen voor de informatievoorziening ten behoeve van de infectieziektebestrijding zijn:

- Digitale Identiteit (IAM)
- Data Services voor data centrisch werken
- Security Monitoring (SOC/SIEM)
- Koppelvlakken met ketenpartners



In de volgende hoofdstukken worden de basisvoorzieningen achtereenvolgens toegelicht. Tevens wordt het onderwerp cloud behandeld.

Basisvoorzieningen als dienst

Iedere basisvoorziening wordt geleverd als dienst. Daarom zijn de volgende aspecten onderdeel van de basisvoorziening:

- De door die technologie geleverde functionaliteit conform het ontwerp van de dienst.
- De onderliggende technologie (platform, infrastructuur, etc.).
- De afspraken over het gebruik, aansluitvoorwaarden, het servicevenster, het gebruiksvenster en gehanteerde standaarden.
- De wijze van aanroepen van de dienst en het resultaat van de dienst.
- De service en performancegarantie die geleverd worden door de dienst.
- Support.
- Gevraagde en geleverde BIV classificatie met betrekking tot privacy en security.
- Documentatie t.b.v. de ondersteuning voor de afnemer.
- Financiële afspraken, kostenmodel voor het gebruik.
- Beveiliging en privacykaders, inclusief periodieke audits en gateway reviews.

https://www.noraonline.nl/wiki/Beschrijf_de_dienst_nauwkeurig

Digitale Identiteit: wat is het?

Een digitale identiteit is de online representatie van een individu, organisatie of apparaat. Identiteiten en toegangsbeheer (IAM) zorgt ervoor dat de actoren voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste faciliteiten. IAM is dus van belang voor de digitale dienstverlening. Niet alleen voor het kunnen leveren van diensten, maar ook om te voorkomen dat aan de verkeerde actor wordt geleverd. IAM regelt drie belangrijke opeenvolgende voorwaarden voor digitale dienstverlening:

- Identificatie zorgt er voor dat bekend is **wie een actor is**.
- Authenticatie zorgt ervoor dat met een bepaalde zekerheid kan worden vastgesteld dat **een actor is wie hij zegt te zijn**.
- Autorisatie zorgt er voor dat bekend is **wat een actor mag of juist niet mag**. Autorisatie is het - vaak door middel van rollen - toekennen van rechten om specifieke data en diensten te gebruiken. Het autoriseren zelf is een verantwoordelijkheid van de beheerder van de data. Het leveren van bijvoorbeeld de rollen van een Digitale Identiteit is wel een onderdeel van de voorziening Digitale Identiteit

› Federatief identiteitenbeheer: een stelsel waarbinnen organisaties vertrouwen op elkaars identiteitenbeheer. Identiteitenbeheer is hiermee dus verlegd naar de eigen organisatie van de actor.

› Authenticatie zorgt ervoor dat een digitale identiteit onweerlegbaar is verbonden met een actor. In het geval van federatief identiteitenbeheer is ook het authenticatie beheer verlegd naar de partner.

Digitale Identiteit: wat heb je eraan?

- Een actor met een door een GGD afgegeven èn geauthentiseerde identiteit kan gebruik maken van diensten vanuit andere datadomeinen, bijvoorbeeld van het RIVM. Bijvoorbeeld: een GGD-medewerker kan, met de juiste rechten, een melding opvoeren binnen het datadomein *meldingen* geleverd en beheerd door het RIVM.
- Een actor met een door het RIVM afgegeven èn geauthentiseerde identiteit kan gebruik maken van de diensten van andere datadomeinen. Bijvoorbeeld: een data-aggregatiesysteem van het RIVM kan, met de juiste rechten, een afspraak inzien binnen het datadomein *afspraken* geleverd en beheerd door de GGD(en).
- Federatieve Digitale Identiteit draagt primair zorg voor authenticatie en niet de autorisatie. De autorisatie ligt vast bij elk datadomein. De eigenaar van een asset (data, dienst) is en blijft verantwoordelijk voor het bepalen van het autorisatieschema (toegang) tot en gebruik van dat asset.

Digitale Identiteit: inzichten

- De rollen (bijv fiatteur, arts infectieziektebestrijding, burger, epidemioloog, etc.) en autorisaties zelf zijn onderdeel van je domeinmodel.
- Het IDU-proces (In dienst/on-boarding, Doorstroming, Uit dienst/off-boarding) is een set van diensten van het HR domein en de input voor het uitvoeren van Identity & Access Management (IAM).
- De volgende uitdaging wordt gezien: Veel domeinen moeten veilig en betrouwbaar aan veel actoren van veel organisaties beschikbaar gesteld kunnen worden.
- Het vraagt een extra organisatorische inspanning om gewenste en/of vereiste niveau’s van beveiliging in relatie tot screeningsniveau van medewerkers in een federatief stelsel af te stemmen.
- De volgende quick win is geconstateerd: actoren van GGD'en en RIVM kunnen op basis van federatieve authenticatie van elkaars data en diensten gebruik maken.
- Zorg voor een goede monitoring van gebruikersacties en neem de logging ervan op in het SIEM.

Digitale Identiteit: besluiten

- Richt Identity & Access Management federatief in
  Organisaties gaan steeds meer samenwerken en willen daarbij externe of interne gebruikers toegang bieden tot IV-middelen. Dit gebeurt al dan niet in combinatie met SSO (Single Sign-On). Ondersteuning van gezamenlijk identiteitengebruik wordt geregeld met Federated Identity Management. Zie ook: Patroon voor federatie van identity management (NORA).

- Standaardiseer het proces van identificatie en authenticatie in een reguliere fase maar, laat voor wendbaarheid veel methoden (bv inlogmiddelen voor authenticatie) toe tijdens een pandemische situatie. Standaardisatie en uniformering draagt bij aan het snel kunnen onboarden van nieuwe gebruikers. Het uitsluiten van inlogmiddelen om standaardisatie te bewerkstelligen, gaat echter ten koste van de flexibiliteit.

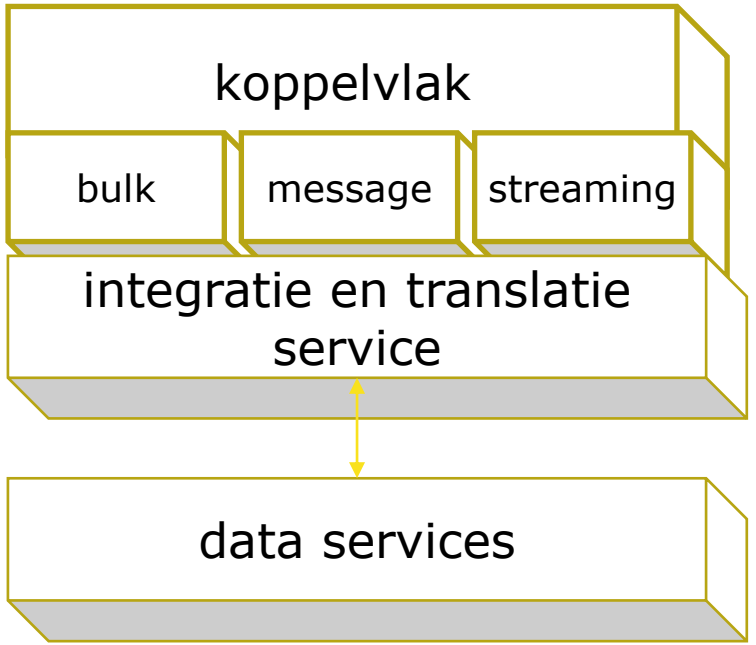
- Automatiseer zo veel mogelijk
  Het in hoog tempo opvoeren van nieuwe gebruikers, inclusief het toekennen van de juiste rechten, kan alleen wanneer deze handelingen zo veel als mogelijk geautomatiseerd plaatsvinden.

Digitale Identiteit: aanbevelingen

- Ontwerp voor alle doelgroepen van de Publieke Gezondheid (bijvoorbeeld niet-ingezetenen (ander (EU) land, vreemdelingen (v nummer), overige mensen zonder ID, militairen, anonieme registratie)
- Onderzoek EUID Wallet en aanvullende functionaliteit voor invulling Digitale Identiteit
- Stel de doelarchitectuur voor autorisaties op: wat doe je met rollen en autorisaties waar en welke consequenties heeft dat voor het ontwerp en de inrichting van een datacentrisch landschap?
  - Bepaal hoe autorisatie (wie mag wat met welke data in welke context?) binnen een federatief, datacentrisch landschap moet worden ingericht. Ondersteun daarmee geautomatiseerd toekennen van autorisaties.
  - Onderzoek hoe inzicht in en toekenning van autorisaties schaalbaar gemaakt kunnen worden.
  - Onderzoek de effectiviteit en haalbaarheid van verschillende autorisatie methodes.
  - Onderzoek hoe machtigingen worden vastgelegd.
- Stel vast op welke wijze "consent" wordt vastgelegd en gebruikt. Onderzoek of het onderdeel is van de voorziening.
- Onderzoek de toepasbaarheid van MITZ voor de toestemmingsregistratie voor burgers.
- Anticipeer op mogelijkheden waarbij burgers rechten over hun data via digitale voorzieningen kunnen wijzigen
- Onderzoek en ontwerp de situatie waarin een natuurlijk persoon (als professional /burger???) meerdere organisaties heeft waarvoor hij/zij werkt. Hoe is dit gebruiksvriendelijk te maken? Welk beleid is hiervoor?
- Werk uit hoe (en op basis waarvan) een vertrouwensrelatie tbv federatieve Digitale Identiteit gerealiseerd kan worden (procesafspraken, audits).
- RIVMtoegang draagt voor het RIVM zorg voor het authentiseren van externe gebruikers; zorg dat GGD-medewerkers met hun GGD-account via RIVMtoegang:
  - Voor de korte termijn: kunnen inloggen op de voor hen relevante systemen en applicaties van het RIVM, waar dit nu nog niet mogelijk is.
  - Voor de lange termijn: toegang hebben tot de voor hen relevante data en informatie binnen het RIVM.
- Bovenstaand punt geldt ook voor GGD met betrekking tot The Identity Hub (TIH).

Koppelvlak: wat is het?

- De koppelvlakvoorziening is de enige toegangspoortpoort naar de data
  - voor alle applicaties die van de data gebruik maken.
  - voor diensten van ketenpartners (Labs, VVT, huisartsen,..) waarmee data uitgewisseld wordt.
- Een koppelvlak verzorgt tevens de translatie van de gegevens naar de verschillende standaarden waarin afnemende applicaties deze kunnen gebruiken.
- Een koppelvlak biedt voorzieningen voor de technische beveiliging, waaronder beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensoverdracht.



Koppelvlak: wat heb je er aan?

- Het koppelvlak zorgt er bijvoorbeeld voor dat 1.000.000 (eis LFI) burgers per dag hun persoonlijke gegevens kunnen raadplegen.
- Applicaties kunnen (en moeten) alle relevante gegevens eenduidig via één loket lezen en schrijven bij de dataservices en hebben daardoor geen onderlinge koppelingen nodig wat een reductie in complexiteit inhoudt en de onderhoudbaarheid vergroot.
- Draagt bij aan de (verhoging van) informatiebeveiliging, o.a. doordat het aanvalsoppervlak wordt verkleind.
- Het koppelvlak kan leveringen faciliteren voor Open Data.

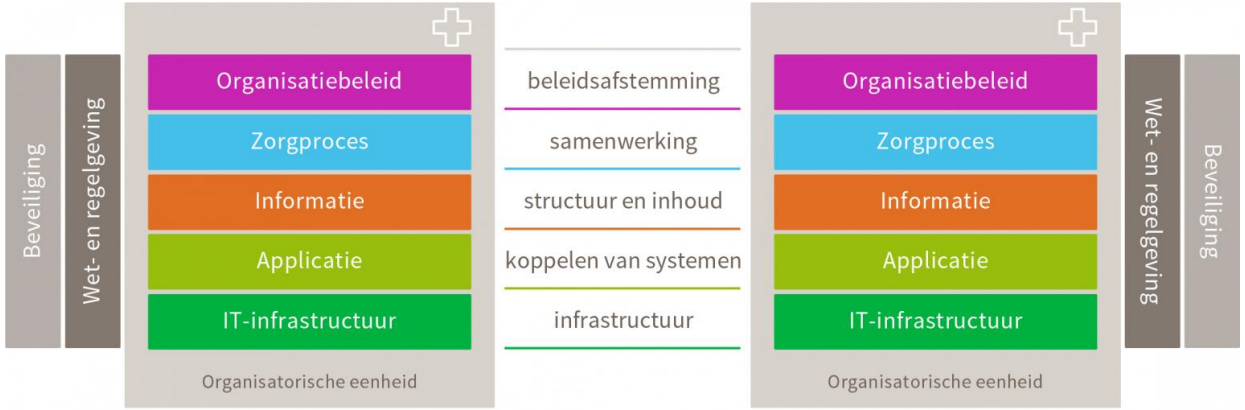
Koppelvlak: inzichten

- Paradoxale standaardisatie: werk in de reguliere situatie toe naar consolidatie op moderne koppelstandaarden, maar houd de mogelijkheid om bij opschaling alle formaten en methoden in het veld te kunnen ondersteunen voor de wendbaarheid.
- Vind niet het wiel uit: benut API-strategie van de overheid (Geonovum), API Strategie van Nictiz en koppelstandaarden zoals HL7 (FHIR).
- API's vragen om versiebeheer, lifecycle-management en onderhoud. Je wilt altijd weten welke applicaties welke API's (in welke versie) benutten. In de voorziening is daarvoor gereedschap vereist (API-management).
- Houd er rekening mee dat verschillende soorten data, afhankelijk van aard en omvang, op verschillende manieren gekoppeld kunnen worden (bijv. bulk-transfer voor sequencing, of GraphQL voor netwerken van contacten bij bron- en contactonderzoek, REST-API voor applicatie-integratie, berichtenverkeer met landelijk schakelpunt).

Koppelvlak: besluiten

- Applicaties krijgen uitsluitend toegang tot data via het koppelvlak. Applicaties wisselen dus geen data onderling uit met andere applicaties.
- Voor applicaties en diensten van ketenpartners bestaat iedere koppeling maar één keer.
- Paradoxale standaardisatie: stuur in de reguliere situatie op standaardisatie van koppelingen en het reduceren van complexiteit. Versterk de capability om met veel diversiteit aan koppelstandaarden om te kunnen gaan ten behoeve van de wendbaarheid bij opgeschaald gebruik.

- Ontwerp iedere API alsof het voor een externe klant is.
- Wanneer externe ketenpartners niet volgens het patroon van data-beschikbaarheid maar via het patroon van gegevensuitwisseling integreren met het IZB-landschap, hanteren wij het Nictiz interoperabiliteitsmodel:



Koppelvlak: aanbevelingen

- Data-integratie vraagstukken, waarin gegevens uit verschillende domeinen met elkaar geïntegreerd moeten worden, vragen om een nadere uitwerking van de architectuur: brengen we data-integratie onder in het koppelvlak, de dataservices of een “integratie service”?
  - Onderzoek de wijze waarop data uit verschillende datadomeinen, verdeeld over RIVM en GGD gecombineerd kunnen worden. Onderzoek of dit direct (tussen dataservices) of altijd via het koppelvlak dient te verlopen. Maw mogen dataservices van de ene organisatie direct (zonder tussenkomst van het koppelvlak) bij de andere organisatie dataservices benaderen?
  - Onderzoek of de kennis van de locatie van een dataservice bij de applicatie (via bv een directory) moet zijn of dat het koppelvlak de routering verzorgt waardoor de applicatie er geen kennis van hoeft te hebben.
  - Onderzoek hoe de toegang tot data tussen applicaties (via het koppelvlak) zich verhoudt tot communicatie van niet data-gerelateerde informatie (zoals bijvoorbeeld events).
- Bouw voort op de keuzes en ingeslagen weg met betrekking tot API-governance strategie RIVM en de API strategie voor de overheid.
- Start met het rationaliseren van de koppelingen tussen RIVM en GGD'en (met bedrijfsfuncties en datadomeinen als uitgangspunt).
- Stel een directory op van koppelpunten (API’s) voor de interne applicaties en externe keten.
- Onderzoek hoe de implementatie van het koppelvlak zich verhoudt tot bestaande samenwerkingsinitiatieven (community networks, LSP, NLX e.d).

SOC en SIEM: Wat is het?

- In de praktijk monitort een Security Operations Centre (SOC) de computer- en netwerkactiviteiten in een organisatie. Log-informatie van applicaties en apparaten in het bedrijfsnetwerk wordt verzameld en onderzocht op afwijkende zaken. De log-informatie kan afkomstig zijn van servers, (virtuele) werkplekken, firewalls, webapplicaties, antivirus-software en zelfs van industriële controlesystemen. Het draait dus om relevante informatie over de beveiliging van alle systemen en apparaten. Alle informatie leidt tot inzicht in hoe veilig het netwerk, de systemen en hard- en software functioneert in de organisatie.
  - Bron: Nationaal Cyber Security Centrum

- SIEM (Security Information & Event Management) is een stelsel van voorzieningen, dat voorziet in het continu, (near-) realtime monitoren van beveiligingsmaatregelen en afwijkend gedrag in infrastructuren. Het voorziet in lange-termijn opslag van verzamelde gegevens en in historische- en trendanalyse van die gegevens. SIEM biedt naast monitoring ook functies voor forensisch onderzoek.
  - Bron: NORA

Security Monitoring – wat heb je eraan?

GGD doet aangifte tegen twee ex-uitzendkrachten wegens vervalsen vaccinatiebewijzen

Twee uitzendkrachten die voor de GGD hebben gewerkt, zouden valse vaccinatiebewijzen hebben aangemaakt. Ze registreerden vaccinaties van mensen die helemaal geen prik hadden gekregen. Zij kregen daardoor ten onrechte een QR-code in de app CoronaCheck. De overkoepelende GGD GHOR Nederland heeft aangifte gedaan bij de politie in Arnhem en Almere.

Simone van Zwienen 04-04-22, 16:00 **Laatste update:** 04-04-22, 17:26

Oplichters sturen nep-emails over boosterprik om bankgegevens te ontfutselen

GOES - In het land gaat een nep-email rond waarin oplichters zich voordoen als de GGD-GHOR Nederland en mensen uitnodigen voor een 'verplichte'...

Doktersassistenten opgepakt voor handel in tientallen valse vaccinatiebewijzen

De politie heeft twee doktersassistentes aangehouden om handel in valse vaccinatiebewijzen. Uit onderzoek blijkt dat de vrouwen, die werkzaam zijn bij een praktijk in Amsterdam, tientallen mensen hielpen aan een vaccinatiebewijs zonder e

Binnenlandredactie 03-11-21,

GGD'er harkte tienduizenden euro's binnen met handel in nepvaccinaties: 'Kon moeilijk weigeren'

Na een anonieme tip kwam een 'uit de hand gelopen handeltje' in nepvaccinaties ten einde. Een inmiddels ontslagen GGD'er en een goede bekende hielpen mensen die geen prik, maar wél een qr-code wilden aan een groen vinkje in de coronasystemen. De twee zouden er 70.000 euro mee hebben verdiend. „Dit is gewetenloos gedrag in een maatschappelijk moeilijke tijd."

Omvangrijke QR-fraude GGD Schiphol: drie verdachten verstrekken valse codes

Drie medewerkers van de GGD-locatie Schiphol zijn aangehouden op verdenking van fraude met valse QR-codes. Het gaat om twee vrouwen van 24 en 48 jaar oud en een man van 22, zo laat het Openbaar Ministerie aan deze site weten.

Caspar Naber 12-11-21, 17:54 **Laatste update:** 14-11-21, 20:49

De verdachten werkten naar verluidt als uitzendkracht voor de GGD op de bewuste locatie. Leden van de Koninklijke Marechaussee hielden hen zondag

Het trio verscheen vrijdag voor de rechter-commissaris. De 24-jarige w kwam daarna vrij, de twee medeverdachten blijven vastzitten.

14 sep 2022 om 13:42 | Update: een dag geleden Lees 272 reacties

De rechtbank in Dordrecht heeft woensdag twee mannen veroordeeld voor het handelen in valse coronavaccinatiebewijzen. Ze kregen beiden een celstraf van twaalf maanden, waarvan negen maanden voorwaardelijk, en een werkstraf van 240 uur opgelegd.

Door onze techredactie

GGD GHOR Nederland ondervindt ernstige hinder door DDoS-aanvallen

21 juli 2021 Coronavirus

Als gevolg van enkele DDoS-aanvallen is het voor burgers sinds gisteren herhaaldelijk niet mogelijk om met hun DigiD-gegevens in te loggen op GGD-websites. Ook vanochtend leidde dit er tijdelijk toe dat verschillende websites onbereikbaar waren. Gedurende een DDoS-aanval kunnen burgers problemen hebben om:

– testuitslagen te bekijken;
– afspraken te maken voor een coronatest of vaccinatie;
– eerder gemaakte afspraken in te zien.

Actief misbruik van kwetsbaarheid in Apache Log4j 2

29 dec 2021

UPDATE 29-12-2021

Nieuw beveiligingslek leidt tot beveiligingsupdate Log4j 2.17.1

Op 28 december werd bekend gemaakt dat er opnieuw een kwetsbaarheid (CVE-2021-44832) ontdekt is binnen Log4j.Om de kwetsbaarheid te misbruiken moet een aanvaller eerst de mogelijkheid hebben om een aanpassing te doen aan het configuratiebestand. Deze nieuwe kwetsbaarheid is mede daarom minder ernstig ingeschaald.

Het advies blijft om beschikbare beveiligingsupdates te (laten) installeren:

tot evenementen. © Rob Engelaar

Onderzoek naar fraude met vaccinatiebewijzen, medewerkers GGD op non-actief

Een aantal medewerkers van GGD-regio's is op non-actief gesteld vanwege mogelijke fraude met vaccinatiebewijzen. Dat meldt minister De Jonge (Volksgezondheid) vanavond in een Kamerbrief.

SOC en SIEM: wat heb je er aan?

- Het inrichten van monitoring & logging over de keten heen helpt bij het detecteren en voorkomen van incidenten en monitort op afwijkend gedrag/fraude. Om deze maatregelen effectief in de keten in te zetten, is het nodig dat de organisatorische kant van cybersecurity goed geregeld wordt. Het is van belang dat bewustzijn wordt gecreëerd voor de risico's van cybersecurity op alle niveaus in de organisatie, inclusief gebruikers. Beleg daarnaast verantwoordelijkheden juist.
- Logbestanden spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Door te zorgen dat applicaties en systemen voldoende loginformatie genereren en deze informatie continu te verzamelen, kan proactief de beschikbaarheid, integriteit en veiligheid van de gehele keten worden bewaakt.
- Om beschermd en weerbaar te zijn tegen digitale aanvallen, is het nodig om zicht te hebben op de digitale infrastructuur binnen de organisaties en op wat daarbinnen allemaal gebeurt. Een onafhankelijk zelfstandig Security Operations Center (SOC) is een goed middel om zicht te houden op de beveiliging van bedrijfsinformatie en digitale dreigingen.
- SOC en SIEM zijn kostbare voorzieningen met veel schaarse expertise. Het gezamenlijk gebruik zorgt voor een beheersing van de kosten.

SOC en SIEM: wat heb je er aan?

- Hoewel er geen harde definitie bestaat van een SOC, laat de praktijk zien dat security monitoring de meest ingevulde taak is van een SOC. Daarbij wordt log-informatie van relevante applicaties en apparaten in het netwerk centraal verzameld en gecorreleerd om te zien of afwijkende zaken hebben plaatsgevonden. Het soort applicaties en apparaten waar log-informatie van verzameld wordt, kan zeer uiteenlopend zijn: van IDS, firewalls, webapplicaties, Active Directory servers en antivirus-software tot aan industriële controle systemen. Alle systemen die relevante informatie kunnen aanleveren om zicht te krijgen op de beveiliging of de status van het netwerk en de daarop aangesloten systemen, kunnen daarbij worden gebruikt.
- Bij de vraag welk soort informatie verzameld moet worden, vanaf welke systemen en op welke wijze deze moet worden gecorreleerd, gaat het niet om wat 'hoort', maar puur om wat voor de organisatie van belang is.
- Een SOC speelt de centrale rol spelen bij het afhandelen van security incidenten, nemen van preventieve maatregelen en secure onboarding van applicaties.
- Een hulpmiddel dat onlosmakkelijk verbonden is met een SOC is een Security Information & Event Management (SIEM) systeem. Het betreft software die in staat is om log-informatie vanuit verschillende bronnen te interpreteren en te correleren naar wat zich binnen en rondom het netwerk afspeelt op gebied van cyberaanvallen en andere beveiligingsincidenten. Het SOC kan gebruik maken van meerdere SIEM oplossingen en AI zodat detectie en response eerder kan plaatsvinden.

SOC en SIEM: inzichten

- Zowel RIVM als GGD'en hebben nog stappen te zetten op het gebied van asset management. Zo is applicatie portfoliomanagement bij het RIVM nog niet voldoende ingericht.
- We kunnen leren van Europese voorbeelden èn van aanwezige regionale kennis, oa, bij GGD GHOR Nederland.
- End-to-end monitoring is een noodzakelijke eis om beschikbaarheid, integriteit en veiligheid van de IT-landschappen – juist in opgeschaalde situatie – te kunnen borgen. Afhandeling van security incidenten wil je zo veel mogelijk automatiseren.
- Patronen veranderen → stilstand is achteruitgang. Hackers vinden continu nieuwe wegen en technologieën om toegang tot systemen te krijgen.
- De inzet van AI voor het signaleren van misbruik is nu wellicht nog next level, maar wel een level waar we naartoe moeten groeien.

SOC en SIEM: inzichten

- Cybercriminelen richten zich op het “window of opportunity”: de tijd tussen de ontdekking van een lek en het moment dat een security update is geïnstalleerd. Update en patch management is cruciaal voor de beveiliging van de keten. Dit betekent, dat we ook op dit gebied eisen aan onze leveranciers moeten stellen.
- Als partners in de infectieziektebestrijding moeten we voldoen aan de NEN 7510-norm; deze bestaat uit twee delen. NEN 7510-1 stelt eisen aan het informatiebeveiligingsmanagementsysteem en NEN 7510-2 geeft richtlijnen voor beheersmaatregelen. Internationaal is de norm bekend als ISO27001 + ISO2779.
- Vanaf 2024 treedt NIS 2 in werking. Het ligt voor de hand dat we ook daar aan zullen voldoen. De nieuwe Europese richtlijn NIS2 scherpt de regelgeving aan, op het gebied van cybersecurity. De reikwijdte van deze richtlijn wordt groter dan die van zijn voorganger en de boetes worden hoger. Met de introductie van de nieuwe Europese cybersecurity richtlijn wil de Europese Unie bedrijven dwingen hun cybersecurity op orde te brengen.

SOC en SIEM: besluiten

- SIEM by design
  Werk bij alle applicaties en voorzieningen - van het begin af - aan het identificeren van de events die relevant zijn voor securitymonitoring en zorg dat deze in het SIEM verzameld kunnen worden. Alle applicaties dienen verplicht aangesloten te worden op het SIEM. Deze eis dient al in de PvE/aankoopfase gewaarborgd te worden.
- Defense in-depth
  Waarborg toegang tot en bescherming van infrastructuur, applicaties en systemen door het toepassen van meerdere lagen van beveiliging.

SOC en SIEM: aanbevelingen

- Breng structurele afstemming tussen de CISO’s en SOC’s van RIVM en GGD'en tot stand.
- Onderzoek de toegevoegde waarde van een landelijk SOC voor de infectieziektebestrijding en – als die toegevoegde waarde blijkt – waar zo’n IZB SOC zou moeten landen. Denk hierbij ook aan bestaande instituties, zoals Z-CERT, het NCSC. Overweeg een “Gezondheids-SOC” onder sturing van het passende ministerie.
- Breng de waardeketen(s) in de infectieziektebestrijding in kaart. Met behulp van een risicoanalyse wordt in kaart gebracht wat de gevolgen zijn voor de organisatie in het geval van problemen met de beschikbaarheid, integriteit en vertrouwelijkheid van bepaalde informatie. Daarnaast wordt in kaart gebracht welke dreigingen bij de verwerking van informatie een onacceptabel risico vormen. Regel in, dat deze analyse jaarlijks wordt uitgevoerd.
- Adopteer NEN7510 voor álle betrokken SOC's
- Start Europese samenwerking met onze buurlanden m.b.t. kennisuitwisseling over security.
- Onderzoek welke aspecten van de Wegiz en NIS 2 relevant zijn voor de informatievoorziening van de infectieziektebestrijding en implementeer deze.
- Stem onderling de BIV-classificaties af.

Data Service: wat is het? (1/2)

- De Data Services zijn de IT onderdelen die de daadwerkelijke toegang tot data faciliteren. Werken met data doe je met de Data Services. Voor (een deel van) het domeinmodel is de bijbehorende Data Service verantwoordelijk voor het leveren (en bewerken) van data ervan. De data eigenaren zijn en blijven zelf verantwoordelijk voor het definiëren van de autorisaties tot hun data.

- Per onderdeel van het domeinmodel is er slechts één data service die verantwoordelijk is voor de daadwerkelijke interactie met de data. Het is de bron. Deze data service is als enige verantwoordelijk voor levering en interactie rond een deel van het domeinmodel.

- De data service stelt een data interface ter beschikking. Deze geeft toegang tot een bepaald dataobject (bijvoorbeeld: vaccinaties, meldingen of patiënten). Deze interface kan synchroon of asynchroon data leveren en verwerken.

Data Service: wat is het? (2/2)

- De data service voert (o.a.) de volgende taken uit:
  - Bewerkingen (lezen en schrijven) op de data.
  - Het autoriseren van toegang tot en wijzigingen van de data.
  - Validatie van data.
  - Logging van wijziging op de data en het datamodel, wie er toegang tot welke data heeft gevraagd en/of gekregen. Ten behoeve van beheer en audit doeleinden.
  - Opslag en archivering van data.
  - Mogelijkheid voor Backup en restore.
  - Data replicatie.
  - Het uitvoeren van wijzigingen op het datamodel.
- De vorm van de datasets die de data service levert worden bepaald door het domeinmodel.
- De data service kan overweg met veelvormige soorten data zoals tabellen, foto's, medisch dossiers opslagen middels verschillende technologieën: relationeel, graph, file, etc.

Data Service: wat heb je er aan?

- De Data Service zorgt ervoor dat organisaties langdurig kunnen beschikken over hun eigen bedrijfsinformatie, onafhankelijk van de ontwikkelingen in het applicatielandschap en leverancierskeuzes.

- Een Data Service maakt het mogelijk om het gebruik van data (lezen maar ook schrijven) door applicaties los te koppelen van de opslag van data. Daarmee is dit een verwezenlijking van de datacentrische gedachte.

- Middels Data Services kunnen verschillende groepen van data federatief gecombineerd worden tot een grote (virtuele) data set conform een domeinmodel.

Data Service: inzichten

- Binnen beide organisaties neemt de kennis toe over het inrichten van een datacentrische architectuur en het opstellen van een domeinmodel.
- Modelgedreven inrichting van data services brengt voordelen met zich mee om vanuit één enkele definitie grote delen van de dataservices te kunnen genereren en onderhouden.
- Via het koppelvlak kunnen verschillende data services gecombineerd worden aangeboden als een samengestelde dienst.
- Hanteer de terminologie van Nictiz voor system API's voor de data services en proces- en experience api's op het koppelvlak.

Data Service: besluiten

- Data Services is de enige basisvoorziening die interactie met de daadwerkelijke data faciliteert.
- Iedere Data Service levert informatie zoals gedefinieerd in het domeinmodel.
- Een Data Service minimaliseert de uitlevering van data in relatie tot het doel en de autorisatie waarvoor de Data Service bevraagd wordt.
- Per entiteit uit het domeinmodel is er slechts één data service die verantwoordelijk is voor de daadwerkelijke interactie met de data. Deze data service is als enige verantwoordelijk voor levering en interactie rond een deel van het domeinmodel.

Data Service: aanbevelingen

- Fail fast, fail often en leer van de ervaringen.
- Onderzoek de toepasbaarheid van een (domein-) modelgedreven methodiek voor implementatie van de voorziening Data Services.
- Onderzoek op welke wijze de voorziening Data Services moet gaan samenwerken met de verschillende (legacy) bronnen (wrapper als data-service, vertaling naar en van domeinmodel).
- Onderzoek hoe de data services en het koppelvlak precies moeten gaan samenwerken.
- Onderzoek hoe federatieve data-opslag binnen een gemeenschappelijk domeinmodel kan worden vormgegeven. Bijvoorbeeld de opslag van BCO gegevens van 25 verschillende GGD'en in afzonderlijke bronnen.
- Bepaal hoe de voorziening Data Services om zou moeten gaan met overlappende domeinmodellen.
- Bepaal hoe om te gaan met situaties waarbij er meerdere “bronnen” zijn bij een specifiek onderdeel van een domeinmodel.
- Bepaal de beste manier om IAM en autorisatie in relatie tot de Data Service vorm te geven.

Cloud: Wat is het?

- Cloudcomputing is een model voor het mogelijk maken van alomtegenwoordige, gemakkelijke, on-demand netwerktoegang tot een gedeelde pool van configureerbare computerresources (bijvoorbeeld netwerken, servers, opslag, applicaties en services) die snel kunnen worden geleverd en vrijgegeven met minimale beheerinspanning of interactie met de serviceprovider. (bron NIST)

Cloud: wat heb je er aan?

- Cloudcomputing is het “nieuwe datacenter”: volledig geautomatiseerd wordt IT als dienst beschikbaar gemaakt. Zo kun je je concentreren op de dingen die meerwaarde bieden voor een organisatie: functionaliteiten, producten en diensten en regie hebben focus.
- Een cloudomgeving is effectieve manier om technisch op te schalen bij een pandemie en geeft daarmee invulling aan de LFI-eis om in een pandemische situatie tijdig met grotere volumes data, gebruikers en transacties te kunnen omgaan.
- De beveiliging tegen externe dreigingen is hoog én kwetsbaarheden worden door cloudaanbieders snel opgelost.
- De cloud kent een hoge mate van innovatie in een tempo dat je verplicht moet volgen, het voordeel daarvan is dat daardoor je eigen IV landschap ‘fit’ houdt.
- Een cloudomgeving biedt real-time een hoge mate van inzicht in compliancy door de dashboards die cloudproviders standaard aanbieden.

Cloud: inzichten

- Cloud is in hoge mate beter schaalbaar en veiliger dan on-premise oplossingen; gelijktijdig zijn er politiek en maatschappelijk vragen over de inzet van diensten van leveranciers van buiten Europa.

- Er is een nieuw Rijksbreed cloudbeleid dat de inzet van public cloud onder voorwaarden mogelijk maakt.

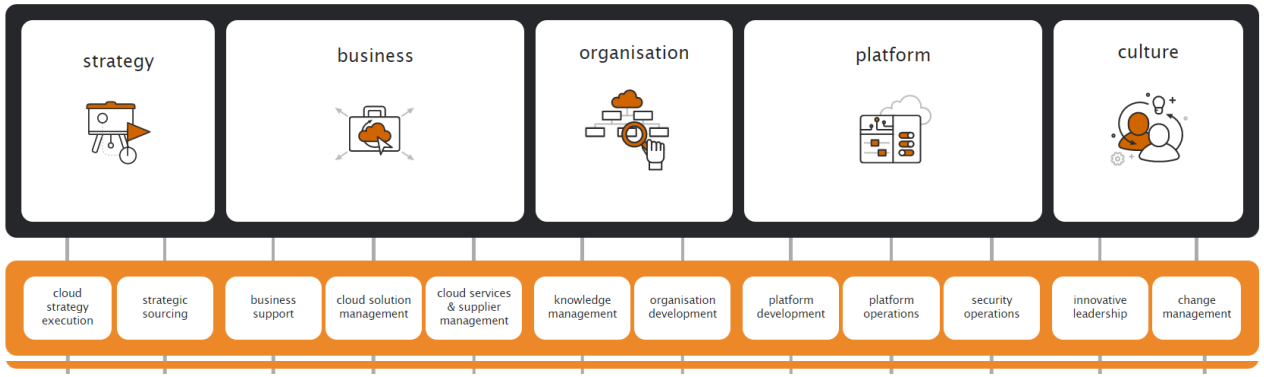
- Het RIVM heeft reeds ervaring met de inzet van public cloud en heeft een Cloud Competence Center ingericht. De inzet van cloud is een strategische keuze voor een andere wijze van organiseren van de IV en gaat verder dan de nieuwe technologische mogelijkheden.

- Cloud is voor RIVM geen doel op zichzelf. Wanneer cloudtechnologie goed wordt ingezet, helpt een migratie van (een deel van) je applicaties en data naar cloud je om een wendbare organisatie te worden, klaar om snel te kunnen innoveren ter beantwoording van de steeds veranderende vragen van nu en morgen. Dit betekent ook wel dat een cloudmigratie meer om het lijf heeft dan het simpelweg verplaatsen van applicaties.

Cloud: inzichten

- Cloud vraagt veel van de organisatie:
  - Ontwikkel- en beheerteams krijgen meer verantwoordelijkheid en autonomie op teamniveau en een directere relatie met de functionele vraag vanuit de opdrachtgevers.
  - Inzicht in de mate van beveiliging en compliance wordt beter en ook de snelheid waarmee kwetsbaarheden in de beveiliging worden gefixt is veel hoger.
  - Kosten van het gebruik van diensten veranderen; in plaats van maandelijkse kosten voor een datacenter, wordt bij cloud het daadwerkelijke gebruik in rekening gebracht.
- Cloud heeft dus niet alleen invloed op de IT-backbone van je organisatie, maar ook op processen en mensen.

- RIVM: Om een gestructureerd plan te kunnen maken die een integrale aanpak omarmt, wordt vanuit het RIVM Cloud Competence Center (CCC) gewerkt over de assen Strategie, Business, Platform, Organisatie en Cultuur, waarbij alle 5 de assen even belangrijk zijn en natuurlijk onderling afhankelijk. Het CCC richt zich op het verhogen van de cloud volwassenheid door de opbouw van onderstaande 12 cloud capabilities.



Cloud: besluiten

- Hanteer "cloud tenzij" als beleid.
  - Passend binnen het Rijksbreed cloudbeleid
  - Waarbij "tenzij" kan gelden wanneer voor een specifieke component de prestatie- en beveiligingseisen vanuit de opschaling aantoonbaar op een andere wijze behaald kunnen worden.

Cloud: aanbevelingen

- Gelijk beleid t.a.v. cloud van GGD'en en RIVM (bijv. Rijkscloudbeleid), anders kan je op andere niveaus (compliance, privacywetgeving) problemen tegenkomen in samenwerking. Stem de inrichtingsprincipes af.

- Richt de financiële administratie zodanig in, dat de kosten van opschaling ten tijde van een pandemie correct kan worden toegerekend en verantwoord.

- Onderzoek of er een aparte pandemische paraatheid-tenant moet worden gerealiseerd voor voorzieningen die ontstaan tijdens een opgeschaalde situatie waarin nieuwe data en toepassingen kunnen worden geplaatst.

- Sluit Service Level Agreements met cloudproviders af die voorzien in de eisen van de reguliere en de pandemische situatie. Onderzoek of de taken van de IZB vallen onder de definitie van “kritieke infrastructuur”.

Relevante ontwikkelingen en kaders

- Parallel aan de ontwikkeling van de doelarchitectuur zijn er verschillende externe ontwikkelingen en kaders die we willen adresseren.

Relevante externe ontwikkelingen en kaders

Parallel aan de ontwikkeling van de doelarchitectuur zijn er verschillende externe ontwikkelingen en kaders die we willen adresseren. Daarbij hanteren wij de volgende aanpak:

- Hergebruik kaderdocument (GGD) en opsomming wetgeving (RIVM)
- Benoem de relevante ontwikkelingen en (nieuwe) kaders zoals bijvoorbeeld EHDS, Zorginformatiestelsel, eID, eWallet, eIDAS,
- Geef een korte duiding per ontwikkeling en de wijze waarop er in deze doelarchitectuur rekening mee wordt gehouden.
- Ambitie (Langere termijn): maak (wettelijke) ontwikkelingen traceerbaar in een architectuur tool.

Relevante externe ontwikkelingen en kaders

Reeds onderkende ontwikkelingen:

- Nationale visie en strategie- gezondheidsinformatiestelsel
- Integraal ZorgAkkoord
- Afwegingskader AI
- Algoritmeregister
- EHDS
- Federatief datastelsel
- Common Ground
- Bouwblokken DICIO VWS
- VWS Cloudbeleid

Afkortingen

- Lijst van gebruikte afkortingen, begrippen en organisaties en de betekenis hiervan

Afkortingen (1/3)

Afkorting	Betekenis
Actiz	Branchevereniging van zorgorganisaties
AI	Artificiële Intelligentie
API	Application Programming Interface
Authenticatie	Vaststellen van de identiteit
Autorisatie	Vaststellen van de rechten van de identiteit
AVG	Algemene Verordening Gegevensbescherming
BBN	Basis Beveiligings Niveau
BCM	Business Continuity Management
BCO	Bron- en Contactonderzoek
BRP	Basisregistratie Personen (GBA + RNI)
BuZa	Ministerie van Buitenlandse Zaken
CBG	College ter Beoordeling van Geneesmiddelen
CBS	Centraal Bureau voor Statistiek
CIb	Centrum Infectieziektebestrijding
CiBG	Centraal Informatiepunt Beroepen Gezondheidszorg
COA	Centraal Orgaan opvang Asielzoekers
Covid/Covid-19	Corona Virus ID 19, identificatie van de ziekte veroorzaakt door SARS-CoV-2, Severe Acute Respiratory Syndrome – Corona Virus variant 2.
CRM	Customer Relationship Management
DJI	Dienst Justitiële Inrichtingen

Afkorting	Betekenis
DPG	Directeuren Publieke Gezondheid
DUO	Dienst Uitvoering Onderwijs
DVP	Dienst Vaccinvoorziening en Preventieprogramma's (uitvoeringsorganisatie binnen het RIVM)
DVA	DienstVerlener (Zorg)Aanbieder
EA	Enterprise Architecture
ECDC	Europees Centrum voor ziektepreventie en -bestrijding
EFSA	European Food Safety Authority
EHR	Electronic Health Record
EMA	European Medicines Agency
EPD	Elektronisch Patiëntendossier
ERP	Enterprise Resource Planning
EU FMD	Falsified Medicines Directive – European Commission
FHIR	Versieaanduiding van HL7 (Health Level 7)
FZ	Forensische Zorg
GBA	Gemeentelijke Basisadministratie Persoonsgegevens
GD	Gezondheidsdienst voor Dieren
GGD	Gemeentelijke/Gemeenschappelijke Gezondheidsdienst
GGD-EPI	Epidemiologie binnen de GGD
GGZ	Geestelijke gezondheidszorg
GHOR	Geneeskundige Hulpverleningsorganisatie in de Regio

Afkortingen (2/3)

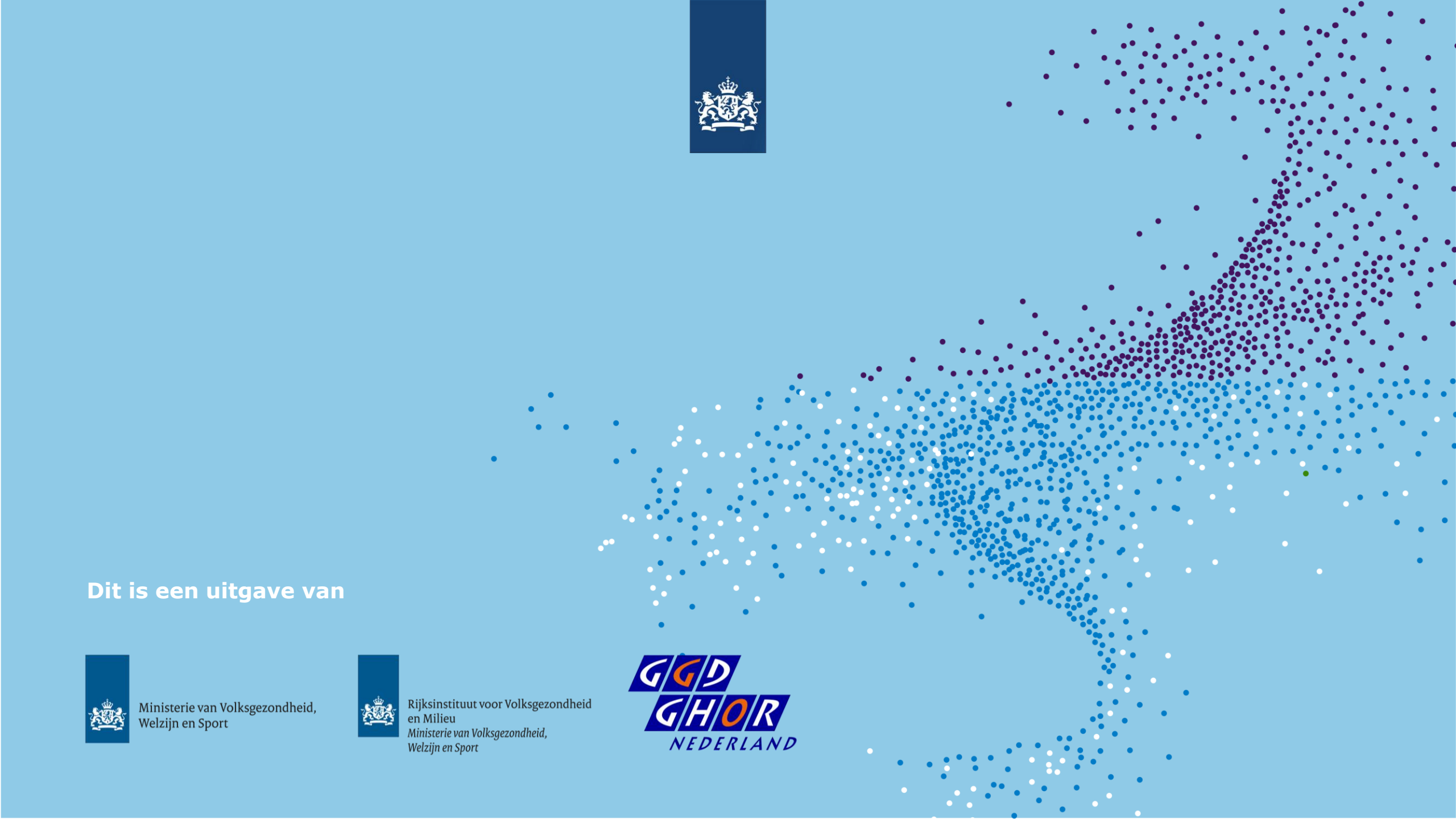
Afkorting	Betekenis
GZA	GezondheidsZorg Asielzoekers
HERA	Health Emergency preparedness and Response
HIV	Humaan Immunodeficiëntie-Virus
HLD	High Level Design
IC	Intensive Care
ICT	Informatie- en Communicatietechnologie
IGJ	Inspectie Gezondheidszorg en Jeugd (onderdeel van MinisterievVWS)
IoT	Internet of Things
IT	Informatietechnologie
ITSM	IT-servicemanagement
IV	Informatievoorzieningen
IZB	Infectieziektebestrijding
JGZ	Jeugdgezondheidszorg
KMAR	Koninklijke Marechaussee
Lareb	Landelijke Registratie en Evaluatie van Bijwerkingen
LCCB	Landelijke Coördinatie Covid-19 Bestrijding
LCI	Landelijk Coördinatie Infectieziektebestrijding
LEDA	Levensmiddelendatabank
LFI	Landelijke Functie Opschaling Infectieziektebestrijding
LHV	Landelijke Huisartsen Vereniging

Afkorting	Betekenis
LIMS	Laboratorium Informatie Management Systeem
LOI	Landelijk Overleg Infectieziektebestrijding
MCCb	Ministeriële Commissie Crisisbeheersing
Min. IenW	Infrastructuur en Waterstaat
Min. BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Min. Def.	Ministerie van Defensie
Min. JenV	Ministerie van Justitie en Veiligheid
Min. LNV	Ministerie van Landbouw, Natuur en Voedselkwaliteit
Min. OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
Min. SZW	Ministerie van Sociale Zaken en Werkgelegenheid
Min. VWS	Ministerie van Volksgezondheid, Welzijn en Sport
MIT	Maatschappelijk Impact Team
ML	Machine Learning
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NHG	Nederlands Huisartsen Genootschap
NHS	Neonatale Hielprikscreening
NICE	Nationale Intensive Care Evaluatie
Nictiz	Nederlands kenniscentrum voor landelijke toepassingen van ICT in de zorg
Nivel	Nederlands Instituut voor Onderzoek van de Gezondheidszorg
NVWA	Nederlandse Voedsel- en Warenautoriteit (Agentschap min. LNV)

Afkortingen (3/3)

Afkorting	Betekenis
OMT	Outbreak Management Team
OTO	Opleiden, Trainen, Oefenen
P&O	Personeel en Organisatie
P&O	Personeel & Organisatie
PBM	Persoonlijke BeschermingsMiddelen
PGO	Persoonlijke GezondheidsOmgeving
PIVA	PersoonsInformatievoorziening Nederlandse Antillen en Aruba
Probas	Protocollaire Basisadministratie
PSIE	Prenatale Screening Infectieziekten en Erytrocytenimmunisatie (zwangerenscreening)
PURA	Publieke gezondheid Referentie Architectuur
QC	Quality Control
R&O	Reiniging en Ontsmetting
RAD	Rapid Application Development
RIO	Registratie Instellingen en Opleidingen
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
RIVM-EPI	Epidemiologie binnen het RIVM
RNI	Registratie Niet-Ingezetenen
RVP	Rijksvaccinatieprogramma
SDC	Statistical Disclosure Control

Afkorting	Betekenis
SOA	Seksueel Overdraagbare Aandoening
SOC	Security Operations Center
SRM	Supplier Relationship Management
TBC	Tuberculose
TBV	Taken, Bevoegdheden en Verantwoordelijkheden
TLN	Transportvertegenwoordiger
UMC	Universitair Medisch Centrum
UMC	Universitair Medisch Centrum
VMML	Vereniging voor Medisch Microbiologische Laboratoria
VNO-NCW	Verbond van Nederlandse Ondernemingen - Nederlands Christelijk Werkgeversverbond
VVT	Verpleging, Verzorging en Thuiszorg
VZVZ	Vereniging van Zorgaanbieders voor Zorgcommunicatie
WBVR	Wageningen Bioveterinary Research
WHO	World Health Organization
ZiRA	Ziekenhuis Referentie Architectuur
Z&O	Zoönosen en Omgevingsmicrobiologie



Dit is een uitgave van

Ministerie van Volksgezondheid,
Welzijn en Sport

Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

GGD GHOR NEDERLAND