Conceptueel model

Programma Pandemisch Parate Informatievoorziening (PP-IV)

Versiebeheer

VERSIE	DATUM	STATUS	AUTEURS	OMSCHRIJVING
0.1	10-5-2023	Concept	Rutger van der Poll, Holke Visser, Harry van Steenoven	Initieel concept
1.0	2-6-2023	Publiceerbaar concept	Rutger van der Poll, Holke Visser, Harry van Steenoven	Versie t.b.v. Marktconsultatie
1.1	20-06-2023	Bijgesteld concept		Opgeslagen werkversie bij aanpassing naam document in 'Conceptueel model Platform voor de Toekomst'
1.2	25-06-2023	Bijgesteld concept		Geconsolideerde versie na marktconsultatie
1.3	10-08-2023	Bijgesteld concept		Nieuwe werkversie t.b.v verwerken reviewcomments
1.4	10-10-2023	Bijgesteld concept	Eltjo van Wijk, Ronald Leeuwestein, Rutger van der Poll, Harry van Steenoven	Nieuwe werkversie Security paragrafen uitgewerkt IAM paragrafen uitgewerkt
1.5	13-10-2023	Bijgesteld concept		Nieuwe werkversie
1.5.1	10-11-2023	Bijgesteld concept	Harry van Steenoven	Commentaren Marco B. verwerkt. Glossary of terms toegevoegd
1.9	11-03-2024	Bijgesteld concept	Harry van Steenoven Rutger van der Poll	Klaar voor vaststelling
1.9	10-05-2024	Bijgesteld concept	Miranda van Helvert	Controle communicatie
1.9	29-05-2024	Bijgesteld concept	Harry van Steenoven	Koppel Services heringedeeld en herschreven
1.9.5	11-06-2024	Versie voor aanbesteding	Harry van Steenoven	Werkdocument tbv aanbesteding IZB

Inhoudsopgave

Referenties

Referenties Intern

Ref. nr.	Document	Versie	Auteur	Documentlocatie
IR003	Visie op Informatiebeveiliging en Privacybescherming (IB&P)	V1.0 / 27 april 2021		
IR004	Doelarchitectuur Identity and Access Management	V1.0 / 18 oktober 2022	R. Klarenbeek	
IR005	Kaderstelling privacy - dataplatform	V2.0 / 7 april 2023	M. van Delzen	
IR006	Bijlage 07 - Kaderdocument conceptueel model	V1.9 / 31/5/2024	R. van der Poll H. van Steenoven H. Visser	
IR008	Doelarchitectuur Informatievoorziening IZB.pptx	V0.9 / 20230713	RIVM / GGD GHOR Nederland	
IR015	Cloud Strategie	V0.9.3 / 29-05-2024	R. van der Poll H. van Steenoven	Programma Pandemische Parate IV > 03 Productteams > 01 IT Basisvoorzieningen > 01 Algemeen > 11 . Werkmap > 00. Richtlijnen en beleid >

Referenties Extern

Ref. nr.	Document	Auteur/Versie	Documentlocatie
ER001	PuRA	1.0	https://www.noraonline.nl/wiki/PURA_(Publieke_gezondheid_Referentie_Architectuur)
ER002	NORA (online)	NORA 2022	https://www.noraonline.nl
ER003	Principes Informatiestelsel voor de zorg	Informatieberaad Zorg / 23-01-2019	https://www.informatieberaadzorg.nl/over-het-informatieberaad/publicaties/publicaties/2019/1/23/deel-1-principes-informatiestelsel-voor-de-zorg
ER005	ISO/IEC 25010-2011	ISO	https://nl.wikipedia.org/wiki/ISO_25010#Productkwaliteit_(Product_quality)
ER006	Handreiking Interoperabiliteit tussen zoriginstellingen (15 nov 2019)	RSO Nederland	https://nictiz.nl/standaarden/overzicht-van-standaarden/handreiking-interoperabiliteit-tussen-zorginstellingen/
ER007	Gegevens uitwisseling in de zorg - EHDS	VWS	https://www.gegevensuitwisselingindezorg.nl/european-health-data-space-ehds
ER008	DIZRA - Manifest	DIZRA	Manifest - DIZRA (gitbook.io)
ER009	Kamerbrief Rijksbreed cloudbeleid 2022	CIO Rijk	https://open.overheid.nl/documenten/ronl-

			a79331dc7c088f2cb6259f591c3b4f2fbcc9b5f1/pdf
ER010	Beslisnota Rijksbreed Cloudbeleid 2022 voor TK	CIO Rijk	https://open.overheid.nl/documenten/ronl-90a53b115e1b0d560238803078f59fff467aa840/pdf
ER011	Nederlandse Cybersecurity strategie 2022-2028	NCSC	https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie
ER012	Nictiz API Strategie voor de Zorg	Nictiz	https://nictiz.nl/app/uploads/2022/10/API-strategie-P1_H1-en-H2-sept-2022-02.pdf
ER013	Nictiz API Requirements	Nictiz	https://nictiz.github.io/api-requirements-docs/v1.1.0/
ER014	LFI BRQ		
ER015	Actieplan Zorg-ICT-markt	Ministerie van VWS	https://www.rijksoverheid.nl/documenten/publicaties/2023/03/31/actieplan-zorg-ict-markt
ER016	Nationale visie en strategie gezondheidsinformatiestelsel	Ministerie van VWS, Nictiz, VZVZ, ZN	https://www.rijksoverheid.nl/documenten/publicaties/2023/03/31/nationale-visie-en-strategie-gezondheidsinformatiestelsel
ER017	Medicatieproces 9	Nictiz	https://informatiestandaarden.nictiz.nl/wiki/Mapping_architectuur#Mappings_en_transacties
ER018	MedMij afsprakenstelsel	MedMij	https://afsprakenstelsel.medmij.nl/display/MMverplicht/Rollen%2C+Core#Rollen,Core-AuthorizationServer
ER019	API Strategie Algemeen (Nederlandse API Strategie I)	Geonovum / Logius	https://docs.geostandaarden.nl/api/API-Strategie/
ER020	'Pas toe leg uit' standaarden (verplicht)	Forum Standaardisatie	https://www.forumstandaardisatie.nl/open-standaarden/verplicht

1 Inleiding

Dit document beschrijft op conceptueel niveau de opbouw van een datacentrisch platform ten behoeve van informatievoorzieningen (IV) voor de ondersteuning van de GGD'en en GHOR-bureaus bij de uitvoering van hun taken. In eerste instantie wordt het platform opgebouwd ter ondersteuning van infectieziektebestrijding (IZB) en Pandemische Paraatheid. Het platform dient echter dermate generiek te worden opgebouwd dat (delen van) het platform in de – nabije – toekomst ook voor andere toepassingen van GGD en GHOR ingezet kan worden, zoals het leveren van basisvoorzieningen (diensten) vanaf dit platform aan GGD'en GHOR-bureaus en koppelvlakken naar regionale platforms, applicaties en gebruikers. Het platform moet toegerust zijn om vanuit een datacentrische aanpak de uitvoering van een vastgesteld, gemeenschappelijk domeinmodel voor de publieke gezondheidszorg te faciliteren. Dit betekent dat een domeinmodel, dat onder andere bestaat uit een procesmodel en een informatiemodel inclusief de structuur van de metadata bij deze informatie, door het platform snel in actieve IV-componenten omgezet moet kunnen worden, zodat een IV-landschap aangeboden wordt van gebruikersinterface tot en met opslagsystemen. De omzetting van model naar actief applicatie-landschap moet zoveel mogelijk geautomatiseerd gebeuren.

Gebruik van het document/Leeswijzer
Het document is als volgt opgebouwd:

Hoofdstuk 1. Inleiding
Dit hoofdstuk beschrijft de inleiding, het doel, en de afbakening van het document.

Hoofdstuk 2. Uitgangspunten en kaders
In dit hoofdstuk worden de uitgangspunten en kaders beschreven die op het platform als geheel van toepassing zijn.

Hoofdstuk 3. Functioneel perspectief
In hoofdstuk 3 worden de producten (deliverables) van het programma beschreven. Zowel de primaire functies van het platform als geheel, als de afgeleide (deel-) producten die als generieke voorzieningen worden aangeboden aan GGD'en en GHOR-bureaus.

Hoofdstuk 4. Non-functioneel perspectief
Hoofdstuk 4 beschrijft de niet-functionele (NFR) eisen die gesteld worden aan het op te leveren IV-platform.

Hoofdstuk 5. Conceptueel model
Hoofdstuk 5 beschrijft het platform op conceptueel niveau en de decompositie van de oplossing in de verschillende (virtuele) bouwblokken. De inleidende paragrafen geven een beschrijving van het platform en zijn bouwblokken als geheel.

De overige paragrafen zijn per bouwblok als volgt opgebouwd:

- Definitie: deze paragraaf geeft een korte definitie van het bouwblok waarbij ook de relatie met te leveren diensten is beschreven;
- Eisen vanuit LFI: de LFI Business Requirements van toepassing op het bouwblok en wat dit voor het bouwblok betekent;
- Inrichting: in deze paragraaf wordt het bouwblok beschreven aan de hand van zijn componenten en functies;
- Onderdelen van het bouwblok: een nadere beschrijving van de onderdelen van het bouwblok zoals deze onder inrichting is weergegeven;

- Koppelvlakken: de paragraaf Koppelvlakken geeft weer met welke andere bouwblokken het bouwblok is verbonden en op welke manier;
- Architectuurbesluiten: in deze paragraaf wordt een overzicht gegeven van de bouwblok-specifieke architectuur-besluiten.

2 Kaders

Het platform dient te voldoen aan eisen die geformuleerd zijn in wetten, regelgeving, beleid, etc. "Kaders" is de algemene term die in dit document gebruikt wordt om dit soort bronnen van eisen aan te duiden. Eisen kunnen algemeen of meer concreet van aard zijn. Eisen die meer algemeen zijn, worden ook wel *principes* genoemd. In de Nederlandse Overheid Referentie Architectuur (NORA), die de basis is van de publieke gezondheid Referentie Architectuur (PURA), wordt *principe* als volgt gedefinieerd: "*Een normatieve uitspraak die richting geeft aan het in samenhang ontwerpen en realiseren van overheidsdiensten voor burgers en bedrijven*".

De volgende soorten kaders worden onderscheiden:

- Kaders publieke gezondheid
    - Uitwerking iStrategie 2024-2027 GGD GHOR Nederland
    - LFI Business Requirements
    - Doelarchitectuur IZB
    - PURA (NORA)
- Zorg-ICT kaders (standaarden, normen)
    - NEN7510 – NEN7512 – NEN7513
    - NEN7503 - Gegevensuitwisseling in de zorg - Elektronische verwerking en uitwisseling van gegevens voor het voorschrijven en ter hand stellen van medicatie
    - NEN7518 - Identificatie & authenticatie (in ontwikkeling)
    - NEN7520 – Autorisatie (in ontwikkeling)
    - NEN7540 - BgZ-uitwisseling tussen instellingen voor medisch specialistische zorg
    - NTA 7516 - Medische informatica - Eisen voor veilige e-mail en chatapplicaties (uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie)
    - MedMij
    - Nationale visie en strategie op het gezondheidsinformatiestelsel
    - Nictiz: Medicatieproces 9
    - Nictiz: API Requirements for Dutch Healthcare
    - Ministerie van VWS: Actieplan Zorg-ICT-markt
    - Architectuurprincipes DIZRA (Manifest)
- Overheidskaders (Wet- en regelgeving, overheidsbeleid)
    - Wetgeving
        - Wpg – Wet publieke gezondheid
        - AVG – Algemene verordening gegevensbescherming
        - WGBO - Wet op de Geneeskundige Behandelovereenkomst
        - Woo – Wet open overheid
        - Wegiz – Wet elektronische gegevensuitwisseling in de zorg
        - Wabb - Wet algemene bepalingen burgerservicenummer
        - Wabvpz - Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
        - Wdo - Wet digitale overheid
        - Wbni - Wet beveiliging netwerk- en informatiesystemen (cybersecuritywet)
        - Wkkgz - Wet kwaliteit, klachten en geschillen gezondheidszorg; 'de kwaliteitswet
        - WVR – Wet veiligheidsregio's
        - Archiefwet
        - Algemene Wet Bestuursrecht
        - Besluit digitale toegankelijkheid overheid
        - Wet Diaz - Wet digitale identificatie en authenticatie in de zorg
        - Wet Computercriminaliteit III

        - Wet BRP - Wet basisregistratie personen
        - VIR - Besluit voorschrift informatiebeveiliging rijksdienst 2007
        - VIRBI 2013 - Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013
        - NIS2 - Network & Information Systems - richtlijn Netwerk en Informatiebeveiliging (NIB)
    - Rijksbreed cloudbeleid 2022
    - BIO - Baseline Informatiebeveiliging Overheid
    - Besluit vaststelling bewaartermijn logging
- Europese kaders
    - eID / EUDI Wallet
    - European Health Data Space (EHDS)
    - Cyber Resilience Act (CRA)
- Privacy en security kaders

De kaders en implicaties zijn, voor zover beschikbaar, per bouwblok uitgewerkt in 'Bijlage 07 - Kaderdocument conceptueel model [REF:IR006]. Alleen de LFI Business Requirements zijn opgenomen in dit document.

3 Functioneel perspectief

3.1 Doelarchitectuur Infectieziektebestrijding

Vanuit het programma Pandemisch Parate Informatievoorziening (PP IV) is in samenwerking met LFI (Landelijke Functie Opschaling Infectieziektebestrijding (LFI), ondergebracht bij het RIVM) en RIVM een gezamenlijke doelarchitectuur (voorheen: High Level Design (HLD)) opgesteld voor een IV-platform ten behoeve van infectieziektebestrijding (IZB) in reguliere en pandemische situaties. In pandemische situaties zal in opgeschaalde versie gebruik gemaakt worden van dezelfde faciliteiten als in de reguliere situatie, waarbij de regie tijdens een pandemie wordt uitgevoerd door de (LFI).

Bron: doelarchitectuur IZB

De doelarchitectuur (en de voorloper daarvan, het HLD) is gebruikt als opdrachtbeschrijving voor het ontwerp van het generieke platform ten behoeve van GGD'en, zoals beschreven in dit document.

3.2 Datacentrisch platform

Doel van het programma is het leveren van een informatievoorziening (platform) op basis van een datacentrische architectuur. Met datacentrisch wordt bedoeld dat data gescheiden is van de applicatiefunctionaliteit en dat model, betekenis en gebruik van de data centraal staan bij het ontwerp en de realisatie van de informatievoorziening. De datacentrische aanpak is een reactie op de applicatie-centrische aanpak waarbij data alleen maar beschikbaar is via de applicatie en een applicatieafhankelijk datamodel. Vaak wordt de data in een centrale relationele database opgeslagen.

Datacentrisch betekent niet dat data centraal opgeslagen wordt. Integendeel, door de applicatie van de data te scheiden middels een data service is men vrij om een eigen opslag te kiezen: bijvoorbeeld een gedistribueerde niet-relationele database.

De informatievoorziening zal gebaseerd zijn op een domeinmodel. Een domeinmodel is een verzameling van beschrijvende en formele modellen waarin het IZB-werkveld vanuit verschillende perspectieven belicht, onder andere vanuit het perspectief van de activiteiten, de informatie, de techniek of de wet- en regelgeving.
het domeinmodel IZB wordt uitgelegd in Bijlage 12 – Domeinmodelleren.docx,

Dit betekent enerzijds dat het platform de mogelijkheid biedt om vanuit een gegeven domeinmodel (voor publieke gezondheid) heel snel de applicatieve toepassingen te ontwikkelen (genereren) die voor de ondersteuning van zorgtaken nodig zijn ('*ontwikkel* modus'). Anderzijds moet het platform de applicaties als infrastructuur ondersteunen in reguliere én in pandemische situaties ('*run* modus').

Dit wil zeggen dat het platform de voorzieningen moet leveren waarmee:

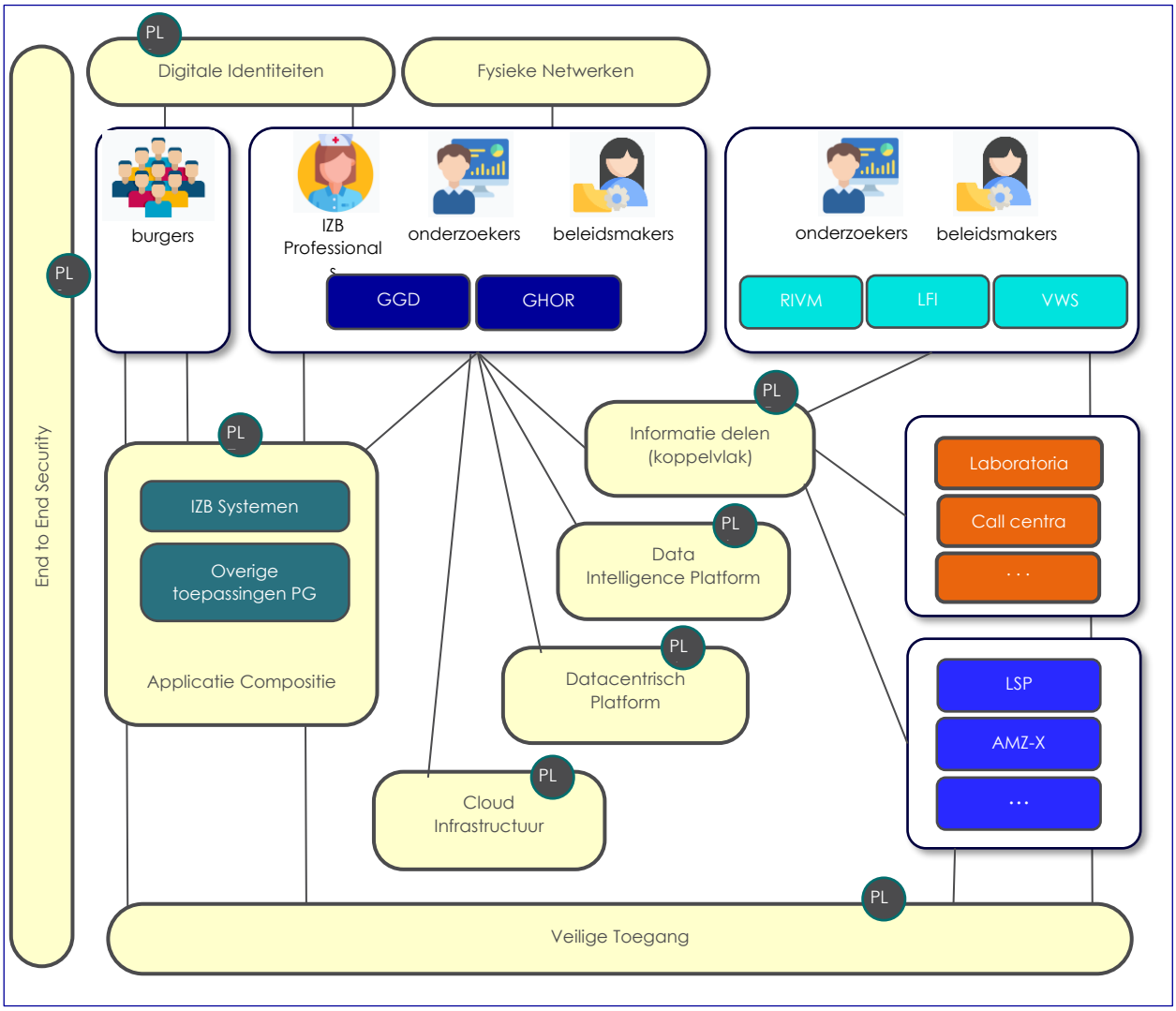
- Op basis van een gegeven domeinmodel eenvoudig, snel en uniform applicaties kunnen worden gecreëerd voor ondersteuning van de bedrijfsprocessen bij GGD'en en GHOR-bureaus. Het creëren van deze applicaties moet maximaal geautomatiseerd gebeuren (genereren). Hiertoe moet het platform de instrumenten bieden voor het creëren en onderhouden van toepassingen ten behoeve van GGD'en en GHOR-bureaus, op basis van (aanpassingen op) het domeinmodel publieke gezondheid (OLTP);
- Op veilige, betrouwbare en wettige (compliant) manier gegevens kunnen worden aangeleverd ten behoeve van onderzoek en analyse (OLAP);
- Toepassingen voor de GGD'en en GHOR-bureaus, stabiel, performant en veilig kunnen worden uitgevoerd. Dit geldt zowel voor de op het platform ontwikkelde toepassingen als andere toepassingen. De infrastructuur hiervoor moet zeer snel kunnen opschalen om grote hoeveelheden gebruikers, gegevens en transacties te faciliteren.

Het platform wordt ingericht voor de ondersteuning van de Infectieziektebestrijding, maar zodanig generiek dat het ook voor andere werkvelden van de GGD'en en GHOR-bureaus ingezet kan worden, zoals JGZ en Maatschappelijke Zorg.

Hiervoor is een aantal diensten geformuleerd die door of vanaf het platform geleverd moeten worden. De aanduidingen PL1 – 8 zijn de codes zoals gehanteerd in de communicatie met het ministerie van VWS. Deze codes zijn in dit document gebruikt als indeling voor het conceptueel model:

- Digitale Identiteiten voor burgers en professionals (PL1);
- Cloud infrastructuur voor onderdelen die niet als SaaS worden afgenomen (PL2);
- End-to-End Security (PL3);
- Data services voor datacentrische inrichting van de omgeving (PL4);
- Koppelvlak t.b.v. Informatiedeling (PL5);
- Data Intelligence Platform voor analyse en research (PL6);
- Applicatie compositie (PL7);
- Veilige data- en applicatie-ontsluiting (veilige toegang) (PL8).

In onderstaand figuur zijn deze diensten aangegeven in relatie tot de mogelijke gebruikers.



In de volgende paragrafen worden deze eindproducten en -diensten in het kort functioneel beschreven.

3.2.1 (PL1) Digitale Identiteit Burgers en Professionals

Digitale Identiteit Burgers en Professionals is een voorziening voor digitale identiteit. Hiervan kunnen flexibel en schaalbaar (het vermogen van een IZB-systeem om snel te reageren op veranderende werklast) nieuwe organisaties, medewerkers, partners en machine identiteiten onderdeel worden. De voorziening draagt zorg voor een veilige en betrouwbare dienstverlening voor authenticatie en autorisatie doeleinden en zal intensief worden bewaakt door systeem en log monitoringsystemen.

De dienst Digitale Identiteit Burgers en Professionals voorziet onder andere in:

- Federatief identiteitenstelsel waarbij de digitale identiteit gecreëerd wordt bij de organisatie waar het personeel werkzaam is. Tijdens de warme fase kan het voorkomen dat er externe medewerkers van partijen toegang moeten krijgen tot de IZB applicaties/data die door GGD GHOR Nederland als dienst worden aangeboden. Denk hierbij aan de situatie waarin snel veel uitzendkrachten moeten worden ingehuurd om centraal afspraken te maken of calls te doen ten behoeve van bron- en contactonderzoek (BCO). Voor deze (tijdelijke) externe medewerkers zal op gecontroleerde wijze een zogenaamd IDU (in-dienst/doorstroom/uit-dienst) proces moeten zijn ingericht. Pas als het proces goed is doorlopen kan er een account (digitale identiteit) worden gecreëerd. Tevens zal er worden toegezien op het handhaven van de juiste rollen en dat accounts tijdig worden stopgezet;

- Decentraal belegd autorisatiebeheer op basis van toekenning van attributen of groepslidmaatschap aan digitale identiteiten in een federatief identiteitenstelsel;
- Ondersteuning van alle authenticatie- en autorisatiemechanismen die voor worden geschreven door (supra)nationale wet- en regelgeving (zowel vigerend als toekomstig, zoals: eIDAS).
- Toegang tot data wordt verleend vanuit (gedelegeerd) eigenaarschap op die data en geïmplementeerd door middel van een centrale voorziening met gesegmenteerde (regionale) inrichting;
- Voorzieningen voor het uitvragen van toestemming (consent) van burgers voor toegang tot hun data.

3.2.2 (PL2) Cloud

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: [Ref:IR008] Doelarchitectuur Informatievoorziening IZB.pptx

Met cloud-technologie kunnen processen snel, 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)) en kostenefficiënt worden opgeschaald om grotere volumes aan data en transacties te ondersteunen. Met cloud-technologie is het mogelijk maximale schaalbaarheid, (geo-) redundantie, flexibiliteit in onder andere de keuze voor opslagsystemen (flat file, relationeel, graph) en beschikbaarheid te realiseren.

Om te zorgen dat er geen afhankelijkheid ontstaat van één technologie (-leverancier) wordt de cloud-voorziening gerealiseerd met zoveel mogelijk standaardtechnieken die zorgen voor een flexibel en overdraagbaar platform, dat op elke willekeurige cloud-technologie kan worden gedraaid.

Een cloud-omgeving is de manier om efficiënt 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.

Inzet van cloud-technologie moet volledig conform het Rijksbreed cloudbeleid [REF:ER010] gebeuren.

3.2.3 (PL3) End-to-End Security

Het inrichten van monitoring en logging over de keten (RIVM, GGD GHOR Nederland en de 25 GGD'en) 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 betrokken organisaties, inclusief gebruikers.

De dienst End-to-End-Security-Monitoring moet voorzien in de juiste log-informatie voor het detecteren van aanvallen en het afhandelen van incidenten. Door ervoor te zorgen dat applicaties en systemen voldoende loginformatie genereren en door 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 wat daarbinnen allemaal gebeurt. Een Security

Operations Center (SOC) is een goed middel om zicht te houden op de beveiliging van bedrijfsinformatie en digitale dreigingen.

- 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 er afwijkende zaken plaatsvinden. 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 controlesystemen. 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 om hetgeen verplicht is, en hetgeen voor de organisaties (RIVM, GGD GHOR Nederland en de 25 GGD'en) van belang is.
- Een SOC speelt de centrale rol bij het afhandelen van security incidenten, het nemen van preventieve maatregelen en de secure onboarding van applicaties.
- Een hulpmiddel dat onlosmakelijk 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 het gebied van cyberaanvallen en andere beveiligingsincidenten. Het SOC kan gebruik maken van meerdere SIEM oplossingen en AI zodat detectie en response snel en effectief kan plaatsvinden.
- Bij alle applicaties en voorzieningen wordt gewerkt met SIEM by design. Hierbij wordt van begin af aan gewerkt aan het identificeren van de events die relevant zijn voor securitymonitoring en ervoor gezorgd 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.
- SOC en SIEM (Security Information and Event Management) zijn kostbare voorzieningen met veel schaarse expertise. Het gezamenlijk gebruik zorgt voor een beheersing van de kosten. Initieel is het monitoren van de gezamenlijke IV-voorzieningen die door de 25 GGD'en worden gebruikt in scope.

End-to-End security Services moeten gebruik maken van bestaande gecentraliseerde SOC-diensten en deze uitbreiden met monitoring, om inzicht te geven wie toegang heeft tot welke data en wanneer deze data is benaderd (Information Governance & Administration (IGA) en Data Access Governance (DAG)).

End-to-End Security betreft zowel reactieve als preventieve maatregelen, zoals Privacy Enhancing Technologies (PET) en eXtended Detection and Response (XDR), om te voorkomen dat problemen ontstaan en zodat direct mitigerende maatregelen (kunnen) worden genomen.

3.2.4 (PL4) Data Service

Met een datacentrische inrichting, die gegeven domeinmodellen gebruikt als structuur voor data, metadata en processen op die data, wordt eenduidigheid van de registratie van die data op het platform gewaarborgd. De gegevensstructuren zijn daarmee losgekoppeld van de applicaties, zodat de data eenmalig wordt vastgelegd en versnippering van informatie wordt voorkomen.

Kern van de Data Service is een aanpak waarbij domeinmodellen als invoer worden gebruikt voor het geautomatiseerd implementeren en uitbreiden van de structuren en technieken van opslag, netwerk en verwerking, waarmee de voorzieningen worden gerealiseerd voor de ondersteuning van zorgprocessen. In eerste instantie betreft het hier een domeinmodel voor IZB-data, maar de voorziening is ook beschikbaar voor domeinmodellen van andere werkvelden.

De Data Service levert ook de metadata ten behoeve van de (audit-)monitoring, de rapportage over het gebruik van gegevens en de rapportage over de wijzigingen op gegevens. Beide rapportages worden zowel inhoudelijk als structureel geleverd.

3.2.5 (PL5) Koppelvlak

Het Koppelvlak is een voorziening voor koppelingen met leden, (keten-) partners en andere partijen , d.w.z. de koppelingen tussen de verschillende componenten. Met deze voorziening kunnen snel informatie-uitwisselingen met nieuwe en bestaande partners zoals zorgverleners, logistieke dienstverleners, datastromen van apparaten, laboratoria en PGO-aanbieders worden opgezet en onderhouden.

De koppelvlakvoorziening is de enige toegangspoortpoort naar de data voor:

- alle niet-centrale, niet data-centrische applicaties die van de data gebruik maken;
- diensten van ketenpartners (onder andere Labs, VVT en huisartsen) waarmee data uitgewisseld wordt.

Het koppelvlak verzorgt tevens de translatie van de gegevens naar de verschillende (standaard-) formaten waarin afnemende applicaties deze kunnen gebruiken of gegevens kunnen worden uitgewisseld.

Via het koppelvlak wordt ook de metadata t.b.v. de (audit-)monitoring en rapportage vanuit de Data Service aangeleverd aan andere systemen.

3.2.6 (PL6) Data Intelligence Platform

Met het Data Intelligence Platform wordt het '*near real-time*' inzicht in de toestand van processen gefaciliteerd en worden dataproducten voor analyse en beleid geleverd. De datavoorziening wordt gebaseerd op internationale datastandaarden voor Infectieziekten. Het platform moet voorzien in het leveren van geanonimiseerde of gepseudonimiseerde data uit diverse (legacy-) bronnen en dataproducten ten behoeve van operationele activiteiten, analyses en onderzoeksactiviteiten. Dit geldt ook voor ketenpartners, zoals de LFI. Bijvoorbeeld, het beschikbaar stellen van sturings- en managementinformatie voor de uitvoering van medische-operationele processen.

Het platform levert daarbij ook mogelijkheden voor het creëren van dashboards en tooling voor het analyseren van de data uit de verschillende bronnen, die worden ontsloten op het platform (Selfservice BI).

3.2.7 (PL7) Applicatiebouwblokken compositie

De dienst PL7 Applicatiebouwblokken compositie voorziet in de integratie van applicatiebouwblokken tot een gebruikersapplicatie, inclusief de interfaces met gebruikers via diverse kanalen (multi-channel) die voldoen aan de WCAG2.1 richtlijn. Hiervoor worden kleine herbruikbare applicatie modules gemaakt en onderhouden die met behulp van orkestratie kunnen worden samengevoegd. Op deze wijze kunnen functionaliteiten snel worden toegevoegd of gewijzigd.

De dienst faciliteert digitale contacten en de afhandeling en vastlegging daarvan. Geregistreerde contacten met burgers worden vastgelegd en zijn voor analysedoeleinden te raadplegen.

3.2.8 (PL8) Veilige applicatie- en dataontsluiting

Met de dienst Veilige applicatie- en dataontsluiting worden de voorzieningen geleverd die nodig zijn om gegevens en applicaties op het te leveren platform op een veilige manier te benaderen.

De dienst bestaat uit voorzieningen voor Application Delivery en beveiliging van de communicatie (netwerk) tussen verschillende centrale en decentrale IV-componenten.

3.2.9 Leveren van diensten

Iedere basisvoorziening wordt geleverd als dienst. Onderstaande zijn aspecten van de implementatie van de diensten:

- 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 en kostenmodel voor het gebruik.
- Beveiligings- en privacykaders, inclusief periodieke audits en gateway reviews.

3.2.10 Verwerking Domeinmodel(len) publieke gezondheid

Het platform moet de executie van domeinmodellen faciliteren, zodat vanuit het informatie- en metadata-model en de bijbehorende bewerkingsregels uit het domeinmodel, specifieke toepassingen snel, veilig, schaalbaar en stabiel kunnen worden aangeboden.

Hiervoor biedt het platform alle generieke, technische voorzieningen die als nutsvoorzieningen steeds opnieuw nodig zijn voor gezamenlijke en specifieke applicaties en datasets. Het platform is hierdoor het fundament onder de gezamenlijke IV-diensten voor de publieke gezondheidszorg, de GGD'en en de GHOR-bureaus.

4 Niet-Functioneel perspectief

Voor het formuleren van niet-functionele eisen (NFR) wordt gebruik gemaakt van de ISO/IEC 25010-2011 standaard [REF:ER005].

De niet-functionele eisen zijn opgenomen in Bijlage 07 - Kaderdocument conceptueel model.

5 Conceptueel model

In de paragrafen van dit hoofdstuk worden de verschillende aspecten van het te realiseren generieke platform op conceptueel niveau beschreven, zoals afgestemd met verschillende expertteams en stakeholders, zoals vertegenwoordigers van de GGD'en.

De verschillende bouwblokken uit het conceptueel model worden gerealiseerd tot herbruikbare gezamenlijke voorzieningen.

5.1 Datacentrisch platform

Het platform wordt geïmplementeerd als een datacentrische informatievoorziening, waarbij de applicatie functionaliteit 'losjes' gekoppeld is aan één enkel, eenvoudig, uitbreidbaar, federeerbaar, universeel, gedeeld en direct implementeerbaar domeinmodel. Onderscheidende eigenschappen van deze informatievoorziening zijn:

- 'Losjes gekoppeld': de applicatie is niet door code gekoppeld aan het dataopslagsysteem, maar de dataopslag kan probleemloos vervangen worden door een ander dataopslagsysteem. Een 'loosely coupled system' is een systeem waarin elk van de componenten geen of weinig kennis heeft of gebruik maakt van de definities van andere componenten. Dit aspect is in het conceptueel model uitgewerkt in het meerlagen-model, waarbinnen de verschillende lagen (bouwblokken) onderling communiceren via API's in een zogenoemde *Decoupled Architectuur*;
- Niet één datamodel per applicatie, maar een gedeeld model, waarin verschillende disjuncte modellen met elkaar verenigd worden voor de hele organisatie. Als kern zal het platform gebruik maken van een gemeenschappelijk domeinmodel voor de publieke gezondheid;
- Eenvoudig: de applicatie modules leveren minimale functionaliteit en overlap wordt daarmee voorkomen. De organisatie wordt beschreven in een paar honderd elementen. Applicatie-functionaliteit wordt modulair geïmplementeerd, d.w.z. op basis van modules die elementaire functies uitvoeren en die communiceren via API's. Voor zover deze modules generieke functionaliteit bieden worden ze hergebruikt in de samenstelling van verschillende toepassingen;
- Uit te breiden: geen nieuwe applicatie maken voor een nieuwe taak maar het uitbreiden van een bestaande functionaliteit;
- Gedeeld: geen data kopiëren, maar data delen.
- Direct implementeerbaar: dat betekent dat het conceptuele domeinmodel zonder veel moeite omgezet kan worden naar een realisatie in informatietechnologie.

Bron: *Dave mcComb*, The Data-Centric Revolution

Het hart van het platform bestaat uit zogenaamde *Data Services*, waarmee de scheiding tussen gegevensverwerking en -opslag wordt verwezenlijkt. De communicatie tussen verschillende modules op het platform gebeurt door middel van API's.

Het platform biedt de mogelijkheid om vanuit een gegeven domeinmodel (voor publieke gezondheid) heel snel de applicatieve toepassingen te ontwikkelen (genereren) die voor de ondersteuning van zorgtaken nodig zijn ('*ontwikkel* modus'). Anderzijds moet het platform de applicaties als infrastructuur ondersteunen in reguliere én in pandemische situaties ('*run* modus').

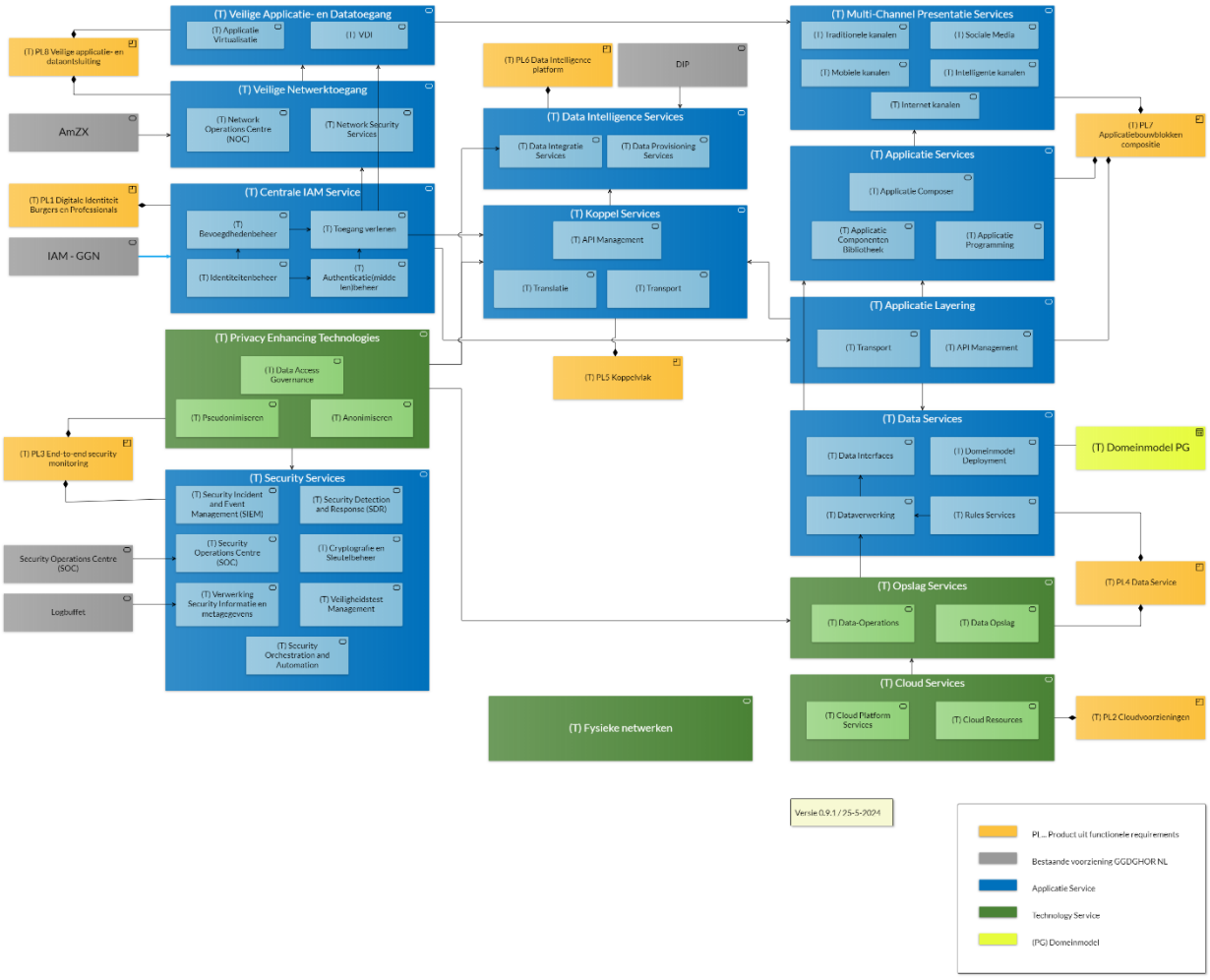
5.2 Opbouw van het platform in bouwblokken

In deze paragraaf en subparagrafen is beschreven welke conceptuele bouwbokken worden onderscheiden voor de realisatie van het generieke technologische platform. De indeling in de verschillende bouwblokken is een meerlagen-model en is gebaseerd op de volgende uitgangspunten:

- De bouwblokken voorzien elk in hun eigen duidelijk onderscheiden en samenhangende functionaliteiten;
- Omdat het platform wordt ingericht om datacentrische IV-oplossingen te ondersteunen, zijn de bouwblokken met betrekking tot de verwerking en activatie van domeinmodellen specifiek gemaakt (*Data Services*).
- De inrichting van het platform is modulair, waardoor in de architectuur 'logische' lagen onderscheiden kunnen worden die door middel van API's onderling communiceren ('decoupled' architectuur);
- Eén of meer – dat wil zeggen, een discreet aantal - bouwblokken voorzien in de realisatie van de te leveren diensten (aangeduid met PL-nummers) zoals beschreven in de doelarchitectuur IZB;

5.2.1 Overzicht Bouwblokken

In onderstaande figuur zijn de verschillende bouwblokken en hun onderlinge gebruiksrelatie weergegeven.



Op het overzichtsniveau worden de volgende bouwblokken onderkend:

- Centrale IAM Service (PL1)
  Dit virtuele bouwblok is de placeholder voor de technische componenten van de dienst *PL1 – Digitale Identiteit Burgers en Professionals*. Dit bouwblok zal gebruik maken van de bestaande en voorziene federatieve IAM (doel-) architectuur. De voorzieningen van *Centrale IAM Service* kunnen op alle lagen van het model worden ingezet.
  Het bouwblok *Centrale IAM Service* realiseert de technische invulling van de dienst *PL1 – Digitale identiteit Burgers en Professionals;*

- Cloud Services (PL2)
  Dit bouwblok voorziet in het leveren van de technische component voor de dienst *PL2 – Cloudvoorzieningen.* Dit is de landingsplaats voor de componenten van het platform die niet als SaaS-oplossing worden afgenomen.
  Het bouwblok *Cloud Services* realiseert de technische invulling van de dienst *PL2 – Cloud Voorzieningen;*

- Security Services (PL3a)
  Dit virtuele bouwblok is de placeholder voor ontwerp en omschrijving van alle technieken ten

behoeve van *Security by Design*. Deze technieken zullen op de verschillende lagen van het model worden ingezet.
Het bouwblok *Security Services* realiseert (in een deel-ontwerp) in combinatie met het bouwblok *Privacy Enhancing Technologies* de technische invulling van de dienst *PL3 – End-to-End Security Monitoring;*

- Privacy Enhancing Technologies (PL3b)
  Dit virtuele bouwblok is de placeholder voor ontwerp en omschrijving van alle technieken ten behoeve van Privacy by Design. Deze technieken zullen op de verschillende lagen van het model worden ingezet.
  Het bouwblok *Privacy Enhancing Technologies* realiseert (in een deel-ontwerp) in combinatie met het bouwblok Security & Privacy de technische invulling van de dienst PL3 – End-to-End Security Monitoring;

- Data Services (PL4a)
  Het bouwblok *Data Services* is het intelligente hart van het platform. Met de implementatie van dit bouwblok worden de volgende abstracties gerealiseerd:
    - De scheiding van data en opslag
    - Het loskoppelen van applicaties en de bewerkingsregels op gegevens
    - Het gebruik van metadata als data

  Data Services voorzien in data API's als interface tussen applicaties en elementaire informatie-objecten (bijv. een *afspraak*, een *dossier*), inclusief invoer-, verwerkings- en uitvoerregels, en de bijbehorende securitymaatregelen.

  Het bouwblok *Data Services* realiseert in combinatie met het bouwblok *Opslag Services* de technische invulling van de dienst *PL4 – Data Service*.

- Opslag Services (PL4b)
  Het bouwblok *Opslag Services* betreft de functionele inrichting van gevirtualiseerde (cloud-) opslagsystemen, gegevensstructuren (zoals DBMS) en de logistiek rondom gegevensopslag, zoals replicatie, archivering en back-up en restore (BuRst)
  Het bouwblok *Opslag Services* realiseert samen met het bouwblok *Data Services* de technische invulling van de dienst *PL4 – Data Service*.

- Koppel Services(PL5)
  Het bouwblok *Koppel Services* voorziet in alle functionaliteit die nodig is voor het beheren van koppelingen met interne- en externe systemen en het uitwisselen van gegevens met interne en externe (keten-) partners. Hiervoor zijn de volgende sub-functies onderscheiden:
    - *API-management* voor het centraal management van de API's in het landschap;
    - *Translatie* voor de vertaling van gegevens van en naar gestandaardiseerde en niet-gestandaardiseerde informatiestructuren voor de uitwisseling van gegevens;
    - *Integratie* voor de functies die nodig zijn voor het samenbrengen van gegevens buiten het domeinmodel, zoals legacy gegevens en gegevens uit externe databronnen, met gegevens binnen het domeinmodel;
    - *Transport* voor de technologische functies die het transport van data op een veilige, robuuste en performante manier verzorgen.

  Het bouwblok *Koppel Services* realiseert de technische invulling van de dienst *PL5 – Koppelvlak*.

- *Data Intelligence Services* (PL6)
  Het bouwblok *Data Intelligence Services* voorziet in alle functies die nodig zijn voor de aanlevering en analyse van gegevens van het platform, eventueel – via de *Koppel Services*- aangevuld met gegevens uit andere data- of applicatie-centrische omgevingen. Met de implementatie van dit bouwblok worden de technische componenten van de te leveren dienst *PL6 - Data Intelligence Platform* gerealiseerd.

- Multi-channel Presentatie Services (PL7a)
  Met het bouwblok *Multi-channel Presentatie Services* krijgen de technologische componenten ten behoeve van verschillende communicatiekanalen naar burgers en professionals hun plaats op het platform. Hiermee wordt presentatie van inhoud gescheiden en eenvoudige, snelle en flexibele distributie van informatie tussen gebruikers en het informatieplatform langs meerdere kanalen mogelijk gemaakt.
  Het bouwblok *Multi-channel Presentatie Services* realiseert in combinatie met de bouwblokken *Applicatie Services* en *Applicatie Layering* de technische invulling van de dienst *PL7 – Applicatie Bouwblokken Compositie*.

- Applicatie Services (PL7b)
  Met de functies van het bouwblok *Applicatie Services* worden data en bewerkingsregels die worden aangeboden vanuit de *Data Services* op basis van het domeinmodel samengevoegd tot uitvoerbare modules.
  De functies van het bouwblok zijn in drie groepen verdeeld:
  - *Applicatie programming*. Deze groep bevat het DevOps ontwikkelplatform en de functies voor het programmeren van specifieke en generieke programma-modules;
  - De modules die generiek kunnen worden toegepast worden als microservice met toegangs-API ontwikkeld. Deze generieke microservices worden opgenomen in een *Applicatie Componenten Bibliotheek* zodat ze hergebruikt kunnen worden;
  - *Applicatie Composer.* Met de functies in deze groep worden generieke modules gecombineerd en waar nodig aangevuld met specifieke modules, zodat een applicatie workflow ter ondersteuning van specifieke zorgprocessen wordt gerealiseerd.

  Het bouwblok *Applicatie Services* realiseert in combinatie met de bouwblokken *Multi-channel Presentatie Services* en *Applicatie Layering* de technische invulling van de dienst PL7 – *Applicatie Bouwblokken Compositie*.

- Applicatie Layering (PL7c)
  Het bouwblok *Applicatie Layering* voorziet in alle functionaliteit die nodig is voor beheren van de koppelingen (API's) tussen de bouwblokken (lagen) uit de primaire infrastructuur voor IZB-applicaties (Multi Channel Presentatie Services, Applicaties Services en Data Services).
  Het bouwblok *Applicatie Layering* realiseert samen met de bouwblokken *Applicatie Services* en *Multi Channel Presentatie Services* de technische invulling van de dienst PL7 – *Applicatie Bouwblokken Compositie*.

- Veilige Applicatie- en Datatoegang (PL8a)
  Het bouwblok *Veilige Applicatie- en Datatoegang* is de placeholder voor de technologische functies die maatregelen implementeren voor het op een snelle maar veilige manier toegankelijk maken van data en applicaties op het platform. Dit bouwblok is samen met het bouwblok PL8b *Veilige Netwerktoegang* de technische invulling van de te leveren dienst *PL8 Veilige applicatie- en dataontsluiting*.

- Veilige Netwerktoegang (PL8b)
  Het bouwblok Veilige Netwerktoegang is de placeholder voor de technologische functies voor een veilige connectiviteit van en naar (onderdelen van) het platform. Dit bouwblok is samen met het bouwblok PL8a *Veilige Applicatie- en Datatoegang* de technische invulling van de te leveren dienst *PL8 Veilige applicatie- en dataontsluiting*.

5.2.2 Eisen vanuit LFI - Algemeen

Bron: LFI BRQ				Implicatie alle bouwblokken
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.2.1	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Change- en incidentmanagementprocessen (gebaseerd op ITIL/BiSL methodieken) bij uitvoerders voorzien in het door de LFI aangestuurd landelijk change- en incidentmanagement tijdens pandemieën inclusief prioritering.	Het programma dient te voorzien in change & incident management over de gehele keten om de processen op de wens aan te passen. Onder wendbaar wordt verstaan: het vermogen van een IZB-systeem om snel gedrag aan te passen aan veranderende situaties.
5.1.6.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevensuitwisseling op niet-gedigitaliseerde/niet-geautomatiseerde wijzen (bijvoorbeeld telefoon, fax, dvd, etc.) worden niet ondersteund en worden actief voorkomen.	Beleid, training en naleving controleren t.a.v. actief voorkomen van gegevensuitwisseling op niet gedigitaliseerde/niet-geautomatiseerde wijze.
6.2.2.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	Betrokken IV/ICT-leveranciers kunnen voorzien in het substantieel (bijvoorbeeld een verdubbeling) opschalen van ontwikkel- en beheercapaciteit binnen een redelijke termijn (bv. Zes weken).	Onderdeel van contracten (SLA, DAP).
6.2.3.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	De ontwikkel- en beheerorganisatie is voorbereid op 24x7 dienstverlening tijdens pandemieën.	Deze zaken worden opgenomen in het PvE bij de opdrachtverstrekking en aanbestedingen.
7.1.1.	Relaties met leveranciers zijn volwassen en risico-gestuurd.	Organisatie en processen	Leveranciers hebben aantoonbare kennis en ervaring met het ontwerpen, bouwen en beheren van applicaties als onderdeel van een complex, dynamisch IV/ICT-landschap met een groot aantal gelijktijdige gebruikers en een hoog volume dagelijkse transacties, bij voorkeur in het zorgdomein	Deze zaken worden opgenomen in het PvE bij de opdrachtverstrekking en aanbestedingen.
7.1.2.	Relaties met leveranciers zijn volwassen en risico-gestuurd.	Organisatie en processen	Leveranciers en door leveranciers geleverde functionaliteiten worden periodiek geauditeerd op basis van de NEN-7512 norm.	Deze zaken worden opgenomen in het PvE bij de opdrachtverstrekking en aanbestedingen.
7.1.3.	Relaties met leveranciers zijn volwassen	Organisatie en processen	Leveranciers borgen en delen kennis en ervaring over IV/ICT-middelen en de inzet hiervan met de primaire uitvoerders en	Deze zaken worden opgenomen in het PvE bij de opdrachtverstrekking en aanbestedingen.

	en risico-gestuurd.		de LFI ten behoeve van paraatheid voor toekomstige, nieuwe (oplevingen van) pandemieën, onder andere door actief kennismanagement.	
7.1.4.	Relaties met leveranciers zijn volwassen en risico-gestuurd.	Organisatie en processen	Dienstverleningsovereenkomsten met leveranciers voorzien in: 1) in de op- en afschaling tijdens pandemieën. Leveranciers weten wat er van hen verwacht wordt tijdens een crisissituatie en daarbuiten. Specifieke en aanvullende afspraken worden gemaakt t.b.v. beschikbare capaciteiten voor ontwikkeling, beheer en incidentmanagement; 2) voorkomen een 'vendor lock-in' door o.a. duidelijke afspraken over dataportabiliteit - 3) bevatten duidelijke afspraken over de exit-strategie	Deze zaken worden opgenomen in het PvE bij de opdrachtverstrekking en aanbestedingen.
8.1.1.	Gegevensverwerking is aantoonbaar vertrouwelijk, transparant en risico-gestuurd (o.b.v. risicoanalyse met daaraan gekoppelde mitigerende maatregelen).	Organisatie en processen	Verwerking en uitwisseling van gegevens in het IV/ICT-landschap (een keten) zijn rechtmatig en voldoen aan de geldende wetgeving voor gegevensverwerking in de zorgsector.	Dit wordt vanuit uitgangspunten Privacy en Security by Design, meegenomen in de bouw van het platform.
8.1.2.	Gegevensverwerking is aantoonbaar vertrouwelijk, transparant en risico-gestuurd (o.b.v. risicoanalyse met daaraan gekoppelde mitigerende maatregelen).	Organisatie en processen	Het IV/ICT-landschap maakt het mogelijk te voldoen aan meerdere bij uitvoerders gangbare normkaders, waaronder ISO27001 (beschrijft hoe procesmatig met het beveiligen van informatie om te gaan met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen de organisatie zeker te stellen), NEN 7510 (beheersprocessen zorg) en BIO (Baseline Informatiebeveiliging Overheid), die voorzien in een risico-gestuurde aanpak van maatregelenselectie.	NEN7510 e.v. wordt als kader gehanteerd. Eis aan leveranciers om aan NEN7510 of vergelijkbaar te voldoen wordt in uitvraag gesteld.

5.2.3 Architectuurbesluiten - Algemeen

In onderstaande tabel zijn de architectuur-besluiten beschreven die voor het gehele platform van toepassing zijn.

ID	Architectuurbesluit	Rationale
PAB-0.01	Het IV-landschap wordt ingericht volgens een decoupled architectuur.	Een decoupled architectuur is er een waarin elk van de componenten weinig of geen kennis heeft van de definities van andere afzonderlijke componenten, of er gebruik van maakt.

		Deze methodiek verkleint het risico dat een wijziging in één component, zowel intern als extern, onverwachte veranderingen in andere delen veroorzaakt. Door de onderlinge verbindingen te beperken, kunnen problemen worden geïsoleerd.
PAB-0.02	Vanaf ontwerp t/m realisatie geldt voor alle producten, diensten en systemen het principe “security-by-design”.	Met 'security-by-design” worden alle componenten zo veilig mogelijk ontworpen en gerealiseerd en t.o.v. elkaar afgeschermd. Hierdoor wordt de impact van een eventuele inbreuk geminimaliseerd.
PAB-0.03	Alle componenten die ingezet worden voor het platform voldoen aan het principe “security-by-default”.	Out-of-the-box worden de meest veilige configuraties gebruikt. Verlichting van de veiligheidsmaatregelen gebeurt dan gecontroleerd en expliciet.
PAB-0.04	Asset- en configuratiemanagement zijn ingericht.	Zonder asset- en/of configuratiemanagement inrichting, kan beheer en monitoring op het platform niet juist worden uitgevoerd.
PAB-0.05	Alle componenten voldoen aan de richtlijnen, wetten, principes, normen, standaarden en eisen zoals geformuleerd in het kader document [REF:IR006].	Door te voldoen aan het gestelde in het kaderdocument wordt geborgd dat gebruikte componenten en oplossingen compliant en veilig zijn en de interoperabiliteit met (toekomstige) IV-ontwikkelingen mogelijk is.

5.3 Centrale IAM Service (PL1)

5.3.1 Definitie

Identiteits- en toegangsbeheer (Identity & Access Management: IAM) is een raamwerk van bedrijfsprocessen, beleid en technologieën dat het beheer van elektronische of digitale identiteiten vereenvoudigt. Met een IAM-oplossing kunnen verantwoordelijken op het gebied van informatietechnologie (IT) de toegang van gebruikers tot kritieke informatie binnen hun organisatie controleren.
IAM zal als basisvoorziening opgenomen worden binnen het platform en geeft invulling aan de gewenste dienst “*Digitale identiteit burgers en professionals*”.

De voorziening gaat uit van een datacentrische inrichting waarbij:

- Eén generieke voorziening de gebruikerstoegang voor de IV-voorzieningen van het platform regelt, waarbij GGD GHOR Nederland het bevoegdhedenbeheer uitvoert voor alle gebruikers (burgers, medewerkers GGD'en en ketenpartners, etc.) die toegang nodig hebben en daartoe gemachtigd zijn. Dit geldt ook voor bijzondere doelgroepen van de Publieke Gezondheid (bijvoorbeeld niet-ingezetenen (ander (EU) land, vreemdelingen (v-nummer), overige mensen zonder ID, militairen, anonieme registratie);
- Het beheer van identiteiten en authenticatie(middelen) wordt uitgevoerd door de aangesloten organisaties zelf. Deze worden door middel van een vertrouwensstelsel (federatie) of een elektronisch ID van de overheid (eID) verbonden;
- Eenvoudig gebruikers toegang ontnomen kan worden wanneer onterecht toegangsrechten bestaan (bijv. na uit-dienst gaan).

5.3.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Centrale IAM Service
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	

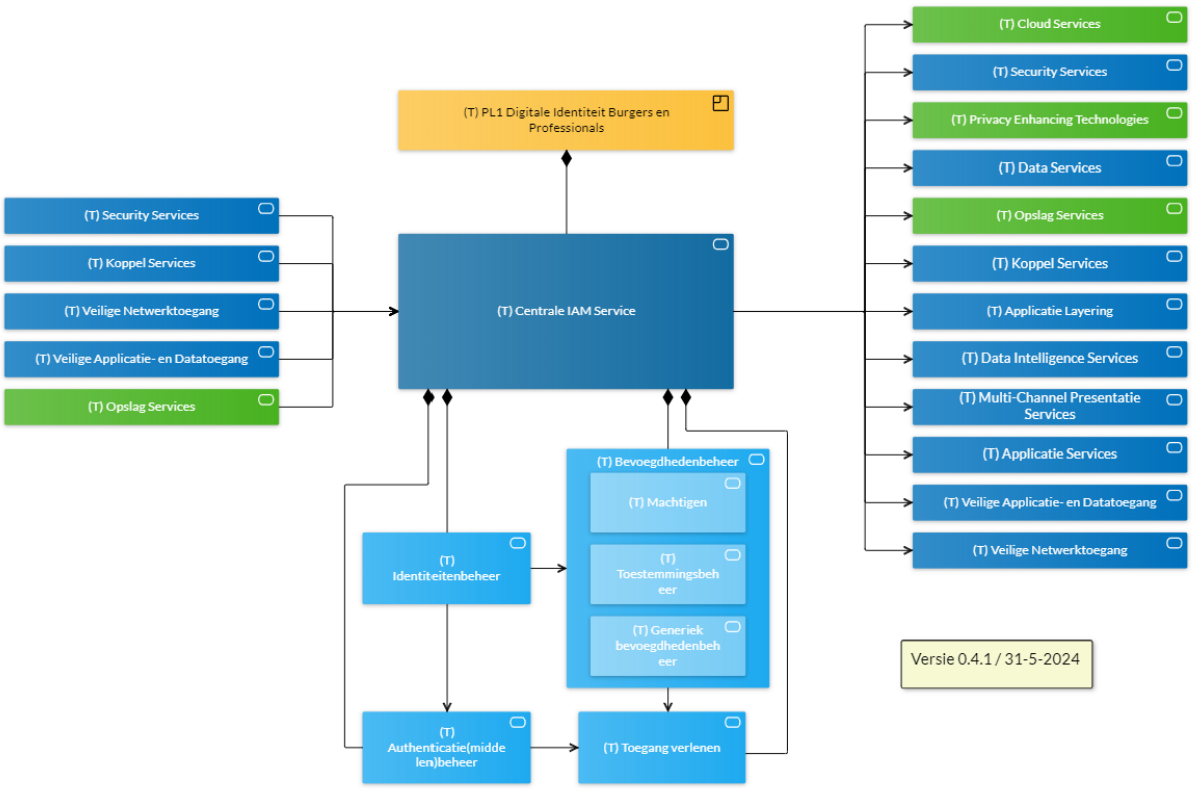
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	IAM-omgeving dient dermate schaalbaar te zijn dat 130.000 professionals gelijktijdig en 1.000.000 burgers per dag kunnen inloggen. De vereiste kengetallen zullen gehanteerd worden als een absoluut minimum. De IAM-voorziening is een federatief stelsel waarbij deelnemers zelf verantwoordelijk zijn voor de capaciteit en werking van zijn/haar onderdeel. De dienst zal, daar waar mogelijk, proactief rapporteren over capacitaire aandachtspunten bij deelnemers elders in de keten. Te denken valt hierbij aan congestieproblemen bij DigiD.
1.1.2.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap voorziet in het snel – bijvoorbeeld binnen enkele dagen – (landelijk) opschalen van professionals voor de uitvoering van medisch-operationele processen door hen te voorzien van een digitale identiteit, die inzetbaar is bij alle uitvoerders, met inachtneming van privacyaspecten.	Het platform gaat gebruik maken van een federatief identiteitenstelsel. Deelnemers kunnen, conform gangbare aansluit standaarden, snel onderdeel uitmaken van het stelsel. De governance in pandemische situatie zal nader uitgewerkt worden (het is niet de bedoeling om iedereen alle rechten te geven).
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Door middel van SLA afspraken en het realiseren van redundantie en geo spreiding wordt hier rekening mee gehouden. Het ontwerp van de oplossing houdt, waar mogelijk, rekening met meervoudige uitvoering op component niveau, om zo minimaal de gewenste 99.95% beschikbaarheid van de dienst te garanderen. Onderdeel van het ontwerp is tevens het uitwerken en realiseren van noodvoorzieningen waarbij professionals snel en effectief hun werkzaamheden weer kunnen uitvoeren indien delen van de dienst onverhoopt uitvallen.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers. Tevens zullen ontwikkelingen in de markt nauwgezet gevolgd en overwogen worden. Continue verbeteringen aan de dienstverlening zijn een integraal onderdeel van de dienstverlening.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen

	betrouwbaar.		(beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
3.1.2.	Het IV/ICT-landschap maakt digitale dienstverlening aan burgers mogelijk.	Techniek	Het IV/ICT-landschap ondersteunt de medisch-operationele processen zodanig dat het mogelijk is om, afhankelijk van de aard en ernst van de pandemie, bepaalde processtappen door burgers uit te laten voeren (bijvoorbeeld door een modulaire opzet).	Burgers kunnen d.m.v. DigiD authenticeren en via access management en -control toegang worden verleend tot bewerking van (eigen) gegevens. Hiervoor moet wel bijzondere autorisatie worden ingeregeld (want niet per rol, maar per persoon.
3.2.2.	Het IV/ICT-landschap maakt digitale dienstverlening aan burgers mogelijk.	Organisatie en processen	Digitale dienstverlening (ook in de opgeschaalde situatie) is het uitgangspunt en gaat uit van zelfredzaamheid van burgers, maar wel in combinatie met specifieke aandacht voor speciale doelgroepen waaronder de niet-digitaal vaardige burgers.	Toegang tot het dossier moet via gemachtigde kunnen worden ingesteld of via professionals worden aangepast. Bij de uitwerking van de oplossing maakt digitale inclusie een onderdeel uit van het ontwerp. Hiermee wordt geanticipeerd en geparticipeerd in het streven van de Nederlandse overheid ten aanzien van inclusieve digitale overheid.
4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	Alle componenten zijn volledig en snel schaalbaar.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Alle componenten zijn volledig en snel schaalbaar. Daarnaast zal de voorziening beschikken over geborgde mechanismen die het mogelijk maken om op een veilige en verantwoorde wijze grote volumes aan handelingen te automatiseren.

4.1.3.	Applicaties zijn gericht op het ondersteune n van hoog-volume processen.	Techniek	Het IV/ICT-landschap ondersteunt een geïntegreerde klantreis voor burgers, inclusief het principe eenmalige registratie, meervoudig gebruik (de verschillende uitvoerders in de keten hebben dus toegang tot dezelfde informatie). Gebruik van digitale middelen door burgers wordt gefaciliteerd op gangbare web- en mobiele technologieën.	Verder zal DigiD onderdeel zijn van het federatief identiteiten stelsel en er wordt rekening gehouden met het opnemen van de EUDI-wallet t.b.v. federatief identiteiten stelsel.
4.2.3.	Applicaties zijn gericht op het ondersteune n van hoog-volume processen.	Organisati e en processen	De regie- en beheerorganisatie van uitvoerders zijn voorbereidt op het leveren van functionele support aan eindgebruikers tijdens warme fase. *[met warme fase wordt de pandemische situatie bedoeld]*	Functioneel support dient ingericht te worden. Afstemming met uitvoerders van andere keten onderdelen maakt onderdeel uit van de governance van de totaaloplossing.
5.1.1.	Gegevensreg istratie en gegevensuit wisseling zijn digitaal, geautomatis eerd en gestandaardi seerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (welke gehost wordt op cloud services) dient dermate te zijn dat genoemde cijfers ondersteund worden. Aangezien de voorziening een onderdeel is van een keten van verschillende onderdelen zullen er op gezette tijden regressie testen op basis van dergelijke kenmerken gesimuleerd worden in een daarvoor ingerichte test- en acceptatieomgeving. Een dergelijke aanpak wordt nader uitgewerkt in samenwerking met andere belanghebbenden en verantwoordelijken van de andere onderdelen (uitvoerders) die deel uitmaken van de keten.
5.1.2.	Gegevensreg istratie en gegevensuit wisseling zijn digitaal, geautomatis eerd en gestandaardi seerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat in het kader van de Wpg en de Wet op het RIVM verplichte meldingen "onverwijld" aan het RIVM ter beschikking gesteld worden door digitale en geautomatiseerde informatie-uitwisseling en/of door verlening van toegang tot data.	Technische voorzieningen voor aanlevering data en/of overzicht zijn onderdeel van het platform. Waarbij gebruik wordt gemaakt van een federatief identiteiten stelsel.
6.1.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat door uitvoerders en/of LFI gecontracteerde partijen personeel toegang kunnen verschaffen tot IV-IZB op basis van door gecontracteerde partijen gegenereerde digitale identiteiten.	Het platform voorziet in een federatief identiteiten stelsel, waarbij de accounts moeten worden aangemaakt bij een federatief aangesloten organisatie.
6.1.2.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat identificatie- en authenticatieprocessen zodanig zijn ingericht dat op korte termijn (2 weken) de tot 130.000 (zorg)professionals voorzien zijn van juiste rollen en rechten.	Het platform voorziet in een federatief identiteiten stelsel, waarbij accounts worden aangemaakt bij een federatief aangesloten organisatie. De centrale voorziening voorziet in gedelegeerde functies voor de deelnemers zodat zij zelfstandig de rollen en rechten aan haar medewerkers kunnen toebedelen. Vanwege de

				omvang en snelheid van mutaties gedurende pandemische situaties, worden bulk invoer mechanismen beschikbaar gesteld om processen, mits geaccordeerd door verantwoordelijken, te versnellen.
6.1.3.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat identificatie- en authenticatieprocessen zodanig zijn ingericht dat rollen en rechten op grote schaal gemuteerd en/of beëindigd kunnen worden.	Het platform voorziet in een federatief identiteiten stelsel. Vanwege de omvang en snelheid van mutaties gedurende pandemische situaties, worden bulk invoer mechanismen beschikbaar gesteld om processen, mits geaccordeerd door verantwoordelijken, te versnellen.
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)securityprocessen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Schaalbaarheid van de oplossing en robuustheid tegen cyber bedreigingen zijn primaire uitgangspunten bij het ontwerp, de realisatie en de instandhouding van de oplossing. Waarbij rekening gehouden wordt met de genoemde schaalbaarheid en het dreigingsbeeld.

5.3.3 Inrichting



De Centrale IAM Service bestaat uit de volgende onderdelen:

- Identiteitenbeheer
- Authenticatie(middelen)beheer
- Bevoegdhedenbeheer
    - Generiek bevoegdhedenbeheer
    - Machtigen
    - Toestemmingsbeheer
- Toegang verlenen

5.3.4 Onderdelen van de Centrale IAM Service

De Centrale IAM Service wordt ontworpen en gebouwd op basis van de, door GGD GHOR Nederland opgestelde, doelarchitectuur "Identity and Access Management" [REF:IR004]

Voor de voorziening in zijn geheel zijn verschillende aanvullende vereisten gesteld:

- Eén generieke voorziening die de gebruikerstoegang voor de IV-voorzieningen van het platform regelt, waarbij GGD GHOR Nederland het bevoegdhedenbeheer uitvoert voor alle gebruikers (burgers, medewerkers GGD'en en ketenpartners, etc.) die toegang nodig hebben en daartoe gemachtigd zijn. Dit geldt ook voor bijzondere doelgroepen van de publieke gezondheid (bijvoorbeeld niet-ingezetenen (ander (EU) land, vreemdelingen (V-nummer), overige mensen zonder ID, militairen, anonieme registratie) [bron Doelarchitectuur IZB];
- Opschalen: in een pandemische situatie dient het platform de mogelijkheid te bieden om snel - bijvoorbeeld binnen enkele dagen – de (landelijke) opschaling van professionals voor de uitvoering van medisch-operationele processen te realiseren, door hen te voorzien van een digitale identiteit. [bron LFI eis 1.1.2.];
- Het platform moet, zodra specificaties bekend zijn, worden toegerust voor aansluiting/gebruik van de EUDI-Wallet;
- De voorziening is inclusief van aard en volgt de richtlijnen van de Nederlandse (digitale) overheid voor doelgroepen die een digitale achterstand hebben.

De voorziening is opgebouwd uit verschillende onderdelen welke in de volgende paragrafen behandeld worden.

Identiteitenbeheer

Identiteitenbeheer (Identity Management) is het proces van het toekennen, bewaken en muteren van digitale identiteiten die gekoppeld zijn aan entiteiten zoals natuurlijke personen. Binnen de Centrale IAM Service faciliteert de voorziening digitale identiteitenbeheer dit proces.

Identiteitenbeheer zal vanuit de dienst primair federatief zijn.

Onder federatief identiteitenbeheer worden alle processen, standaarden en technologie verstaan welke het mogelijk maken om op een gecontroleerde manier identiteitsgegevens uit te wisselen over organisatiegrenzen heen. Hierbij blijven aangesloten partijen verantwoordelijk voor het opvoeren, muteren en verwijderen van digitale identiteiten van gebruikers. Deze decentrale voorziening voor het beheren van digitale identiteiten wordt een Identity Provider (IdP) genoemd. Zoals eerder benoemd is de voorziening primair federatief voor wat betreft identiteitenbeheer. Identiteitenbeheer biedt tevens de voorzieningen om centraal een generieke identiteiten database te onderhouden die zal fungeren als IdP. De centrale IdP functie maakt een integraal onderdeel uit van het identiteitenbeheer.

Aanvullende eis die vanuit het platform aan identiteitenbeheer gesteld wordt:

- De dienst moet rekening houden met koppelingen naar een grote verscheidenheid aan digitale identiteitsvoorzieningen (IdP's);

Authenticatie(middelen)beheer

Authenticatie(middelen)beheer omvat het proces waarbij gecontroleerd wordt dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft. Authenticatie noemt men ook wel verificatie van de identiteit.

Binnen de Centrale IAM Service faciliteert de voorziening Authenticatie(middelen)beheer dit proces.

Aanvullende eisen die vanuit het platform aan authenticatie(middelen)beheer gesteld worden zijn:

- Het platform moet, zodra specificaties bekend zijn, worden toegerust voor aansluiting/gebruik van de EUDI Wallet. Als *Relaying Party* is het verplicht om het gebruik van *EUDI wallets* te accepteren t.b.v. gebruikersauthenticatie.

Bevoegdhedenbeheer

Bevoegdhedenbeheer betreft de "levenscyclus" van bevoegdheden die bestaat uit het identificeren, vastleggen, wijzigen en eventueel verwijderen van bevoegdheden, en het toekennen of afnemen ervan aan digitale identiteiten.

Doorgaans wordt dit ook wel Autorisatie beheer of Access management genoemd. (NORA definitie) Generiek bevoegdhedenbeheer
Bevoegdhedenbeheer is de centrale bouwsteen binnen de Centrale IAM Service en draagt zorg voor:

- Het periodiek herbevestigen van toewijzingen (attestation, review and certification);
- Het periodiek controleren of de vastgelegde bevoegdheden overeenkomen met de werkelijkheid (reconsiliation);
- Het distribueren (provisioning) van toewijzingen naar doel applicaties;
- Bevoegdheden toewijzingen en afnemen.

Het toewijzen van bevoegdheden kan op individu plaatsvinden maar wenselijker is het om bevoegdheden te clusteren tot rollen (RBAC) en deze automatisch te koppelen aan personen of aan (contextuele) kenmerken/attributen van deze personen (ABAC).

De Centrale IAM Service binnen het platform zal zich met name richten op het hergebruik van bestaande registers, om deze kenmerken te kunnen gebruiken tijdens het toewijzingsproces. Deze registers, ook wel Attribute Service Providers (ASP) genoemd, dienen gezaghebbend te zijn en worden aan dwingende eisen onderworpen. Deze methode past volledig in een datacentrisch streefbeeld.

Machtigen

Een bijzondere vorm van bevoegdhedenbeheer is machtigen.

Personen moeten in staat worden gesteld om elkaar over en weer te kunnen machtigen en vertegenwoordigen, in ieder geval in hun relatie met de overheid. Personen betreffen zowel Natuurlijke als Niet-Natuurlijke personen.

De service faciliteert machtigen vanuit twee perspectieven:

- Vanuit een burgerperspectief zal de voorziening aansluiten bij initiatieven, nationaal en mogelijk ook Europees, die ontwikkeld zijn en worden op het vlak van machtigen, zoals DigiD Machtigingen. Het merendeel van de activiteiten zal buiten de dienstverlening om ingeregeld worden. Met deze voorziening *Machtigingen* wordt invulling gegeven aan de Algemene wet bestuursrecht, waarin is vastgelegd dat een burger zich mag laten vertegenwoordigen. Naar verwachting zal dit niet alleen een nationaal karakter hebben maar moet ook rekening gehouden worden met Europese initiatieven op dit vlak. De service dient waar mogelijk bij deze initiatieven aan te sluiten
- Voor professionals zal de dienstverlening services opnemen en aanbieden waarbij het mogelijk wordt om taken en bevoegdheden, al dan niet tijdelijk, over te dragen aan andere professionals.

Toestemmingsbeheer

Enigszins gerelateerd aan machtigingen is het proces van toestemming (consent). Dit aspect speelt wanneer toestemming van burgers nodig is voor gegevensuitwisseling met derden. Voor de gezondheidszorg is Mitz een belangrijke veilige online-toestemmingsvoorziening (register) waarmee een burger zelf zijn toestemmingskeuzes kan beheren en vastleggen, o.a. voor gegevensuitwisseling via het Landelijk Schakelpunt (LSP). Mitz is opgenomen als bouwsteen in het Informatiestelsel Zorg. De Centrale IAM Service zal deze dienst incorporeren binnen haar dienstverlening.

Waar Mitz niet gebruikt kan worden, moet het platform voorzien in de middelen waarmee burgers toestemming tot het gebruik en/of het delen van data kunnen verlenen, of deze kunnen weigeren of intrekken. Indien de overheid andere gezaghebbende toestemmingsregisters aanwijst, worden deze opgenomen in het stelsel.

Verlenen van toegang

Verlenen van toegang, ook wel Toegangsbeheer of Access control genoemd, is het proces om te beslissen of een persoon of systeem op grond van een authenticatiemiddel, identiteitsverklaring, of een machtiging toegang krijgt tot applicaties of gegevens. De beslissing wordt mede gebaseerd op bij de applicatie of gegevens behorende autorisatieregels en omgevingsfactoren.

5.3.5 Overige aspecten Centrale IAM Service

Beheerderstoegang

Met betrekking tot toegangsbeheer zijn beheerders een speciale groep omdat zij vaak verhoogde graad van bevoegdheden op de omgeving hebben. Onder beheerders worden zowel functionele als technische beheerders bedoeld welke toegang moeten krijgen tot (delen van) het systeem. Voor deze groep moeten daarom bijzondere toegangsmaatregelen worden ingericht, het Priviliged Access Management (PAM). PAM-oplossingen identificeren de mensen, processen en technologie die uitgebreide toegang nodig hebben en specificeert de beleidsregels die daarop van toepassing zijn. PAM is onderdeel van de Doelarchitectuur Identity and Access Management [REF:IR004].

5.3.6 Koppelvlakken

Naast de interne relaties tussen de diverse onderdelen van de Centrale IAM Service heeft de service ook relaties/koppelvlakken met andere bouwblokken van het platform. De service kan, ook gelijktijdig, aanbieder dan wel afnemer zijn naar andere bouwblokken.

Centrale IAM Service maakt gebruik van:

- Security Services
  Alle systeemlogging en audit trails van de *Centrale IAM Service* worden beschikbaar gesteld aan de SOC-voorziening. Op basis van vooraf gedefinieerde "use cases" zal deze data verwerkt worden.
- Koppel Services
  De voorziening maakt gebruik van het bouwblok "*Koppel Services*" voor het veilig kunnen koppelen met zowel bron- (registers) als afhankelijke systemen waarmee de voorziening communiceert.
- Veilige Applicatie- en Datatoegang
  De voorziening maakt gebruik van het bouwblok *Veilige Applicatie- en Datatoegang* voor de ontsluiting van deze omgeving voor beheerders.
- Veilige Netwerktoegang
  De voorziening maakt gebruik van het bouwblok *Veilige Netwerktoegang* voor de ontsluiting van deze omgeving voor beheerders.
- Opslag Services
  De voorziening maakt gebruik van het bouwblok *Opslag Services* voor het veilig en betrouwbaar opslaan van data, welke onderdeel uitmaakt van de centrale bouwblokken van de dienst. Denk hierbij aan de identiteiten- en bevoegdheden registers en de middelen die de interactie met (andere) bron- en doelsystemen ondersteunen.

Centrale IAM Service wordt gebruikt door alle bouwblokken/onderdelen binnen het platform ten behoeve van toegangsbeheer.

5.3.7 Architectuurbesluiten

In onderstaande tabel zijn de architectuur-besluiten beschreven die m.b.t. het bouwblok zijn geformuleerd

ID	Architectuurbesluit	Rationale
PAB-1.01	Voor Identity Management wordt de Doelarchitectuur Identity and Access Management [REF:IR004] gevolgd	De doelarchitectuur is vastgesteld en betreft de generieke, federatieve voorzieningen t.b.v. GGD'en, GHOR en GGD GHOR Nederland.
PAB-1.02	Het platform moet, zodra specificaties bekend zijn, worden toegerust voor aansluiting/gebruik van de EUDI Wallet.	Aansluiten bij Europese normen en wetgeving.
PAB-1.03	Access Management moet de mogelijkheid hebben om op basis van dataverwerkingsrollen en dataverwerkingsregels, welke zijn gespecificeerd in het domeinmodel, (geautomatiseerd) autorisaties toe te kennen.	In een datacentrisch landschap zijn dataverwerkingsrollen en -regels onderdeel van het domeinmodel.
PAB-1.04	Consent registratie vindt bij voorkeur plaats d.m.v. Mitz	Nationale visie gezondheidsinformatiestelsel.

5.4 Cloud Services (PL2)

5.4.1 Definitie

Doel van het bouwblok *Cloud Services* is het leveren van een veilige en hoog beschikbare infrastructuur gebaseerd op Cloud technologie die geautomatiseerd geschaald kan worden, als onderdeel van de dienst *PL2 - Cloudvoorzieningen*.

De Cloud Services dienen als infrastructuurcomponent voor de inrichting van die bouwblokken waarvoor geen SaaS-oplossing wordt afgenomen (SaaS voorziet immers zelf in de virtuele infrastructuur voor de te

leveren dienst). Daarnaast worden de Cloud Services aangeboden als basisvoorziening voor de leden van GGD GHOR Nederland, de GGD'en.

Er is gekozen voor cloud infrastructuur omdat deze ten opzichte van traditionele on-premises infrastructuren veel flexibiliteit biedt in schaalbaarheid, met een zeer korte *time to market* (TTM). Deze eigenschap is cruciaal voor een oplossing die ten tijde van een pandemie in zeer korte tijd moet kunnen opschalen.

Op basis van de huidige formulering van het Rijksbreed cloudbeleid [REF:ER009] kunnen de Cloud Services voor bijzondere persoonsgegevens niet worden afgenomen als publieke cloud, tenzij aan een aantal voorwaarden wordt voldaan. Alle opslag en verwerking van persoonsgegevens moet plaatsvinden conform geldende privacy-vereisten uit de AVG. Eén van de onderdelen van de AVG is het voldoen aan vereisten inzake doorgiften van persoonsgegevens (hoofdstuk V van de AVG), waarbij wordt voldaan aan één van de onderstaande eisen:

- opslag en verwerking binnen de Europese Economische Ruimte (EER), of
- in landen waarvoor een adequaatheidsbesluit bestaat, of
- op basis van een passend doorgiftemechanisme dat voldoet aan de vereisten (van art. 46, hoofdstuk V) van de AVG, zoals een modelcontract (standaard contractbepalingen of 'standard contractual clauses')

GGD GHOR Nederland heeft een cloud-strategie opgesteld [REF:IR015]. De belangrijkste richtlijnen van de cloud-strategie zijn:

- In navolging van de NORA geldt: SaaS boven PaaS boven IaaS, m.u.v. de realisatie van de data services en onderliggende opslag services (één van de basisvoorzieningen van het toekomstige IV-landschap), daar geldt PaaS of IaaS op eigen cloud services;
- Implementatiemodel is hybrid cloud; regulier zal sprake zijn van alleen private cloud. Indien bij een pandemie niet tijdig opgeschaald kan worden, zal voor de verwerking public cloud resources worden ingezet. Voor dataopslag geldt dat dit alleen op de private cloud mag;
- Voor de opschaling tijdens een pandemie geldt dat dit gerealiseerd wordt in de private cloud. Indien dit niet tijdig kan dient outscaling voor de applicaties op het platform en platformonderdelen (dus niet dataopslag) naar public cloud van dezelfde EER-organisatie welke de private cloud levert mogelijk te zijn. Indien dat niet tijdig kan dient outscaling naar de public cloud van de Big Tech (Microsoft/Amazon/Google) mogelijk te zijn;
- De public cloud van de Big Tech wordt eveneens geleverd door dezelfde EER-organisatie welke de private cloud levert. Uitgangspunt van de strategie is dat de volledige hybride cloudoplossing ingericht wordt door 1 combinatie van Big Tech oplossingen (d.w.z. Amazon Web Services + AWS Outpost óf Microsoft Azure + Azure Stack óf Google Cloud Platform + Google Anthos).

5.4.2 Eisen vanuit LFI

In onderstaande tabellen zijn de eisen vanuit LFI weergegeven die specifiek van toepassing zijn op het bouwblok.

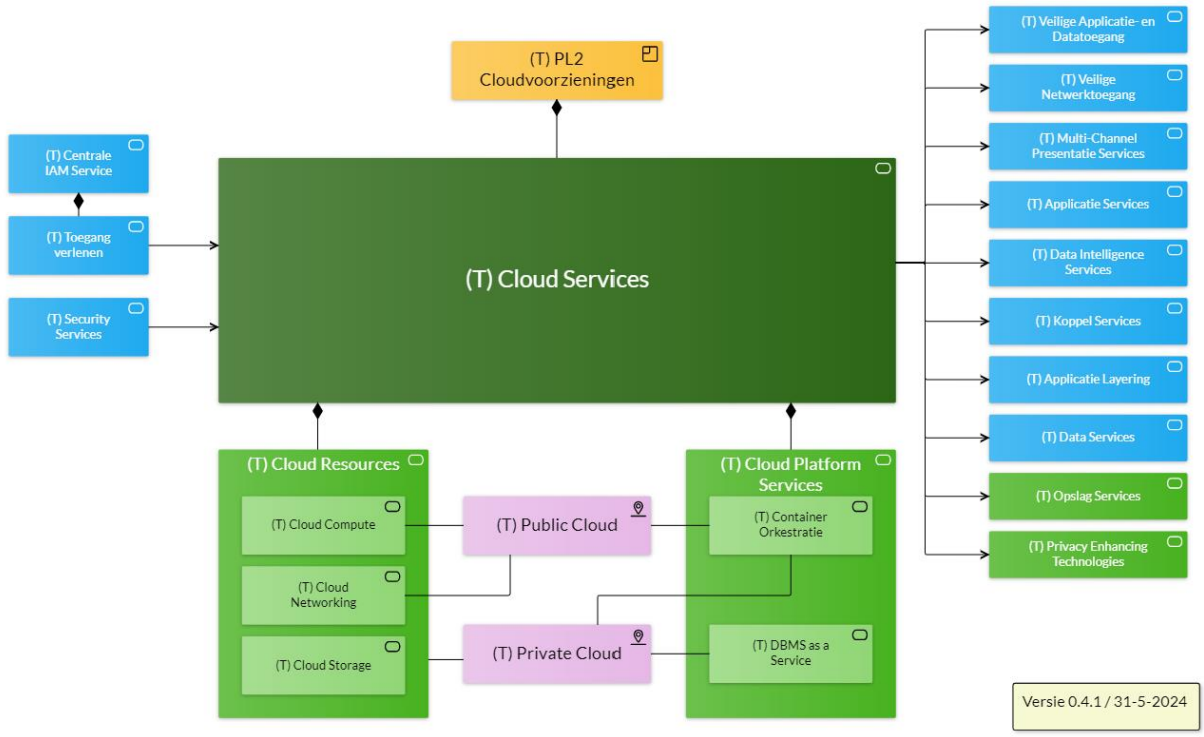
Bron: LFI BRQ				Implicatie Cloud Services
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Schaling van onderliggende infrastructuur (Private Cloud t.b.v. data hosting) zal plaatsvinden o.b.v. genoemde cijfers en zal zo de daadwerkelijke inrichting specificeren.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA afspraken en het realiseren van redundantie en site failover met geo-spreiding wordt hier rekening mee gehouden.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers. Dit geldt zowel voor de ontwikkel- als de run-modus componenten.
1.1.6.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	• Flexibiliteit om nieuwe oplossingen snel van de benodigde infrastructuur te voorzien door middel van IaC; • CI/CD-tools beschikbaar stellen voor ontwikkelpartijen zodat zij snel (binnen overeengekomen termijnen) wijzigingen en/of nieuwe oplossingen kunnen implementeren zonder handmatige interventie van cloudbeheer.
1.1.7.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het opschalen en doorvoeren van wijzigingen ten behoeve van de landelijke bestrijding van een A-infectieziekte vormt geen belemmering in de ondersteuning van de bestrijding van overige infectieziekten waarvan de bestrijding door het IV/ICT-landschap wordt ondersteund.	Isolatie van impact door: • Inzetten afzonderlijke resourcepools; • Voorzien van tooling om applicaties geïsoleerd van elkaar te draaien (zoals containerisatie); • Inrichting infrastructurele OTAP.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van

	betrouwbaar.		(informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	De onderliggende platform infrastructuur is een schaalbare (private) cloud t.b.v. hosting van data (datacentrisch). Applicaties kunnen (gedeeltelijk) gehost worden op de private cloud omgeving. De applicaties dienen een cloud agnostisch scale out te kunnen doen naar public cloud.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	De onderliggende platform infrastructuur is een schaalbare (private) cloud t.b.v. hosting van data (datacentrisch). Applicaties kunnen (gedeeltelijk) gehost worden op de private cloud omgeving. De applicaties dienen een cloud agnostisch scale out te kunnen doen naar public cloud.
4.1.6.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorkomt een te grote afhankelijkheid van een of meerdere leveranciers (vendor lock-in). Applicaties moeten door nieuwe leveranciers overgenomen kunnen worden op basis van een vooraf overeengekomen Escrow overeenkomst.	• Containerisatie is een aansluitvoorwaarde. Dit zorgt ervoor dat applicaties portable zijn en dus makkelijker van de ene cloud provider naar de andere kunnen worden verplaatst; • Gebruik van cloud-agnostische containerorkestratie-tools; • Gebruik van cloud-agnostische IaC-tools.

5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	De dataopslag vindt plaats in de private cloud en dus moet voor dataleveringen de private cloud voldoende geschaald zijn.

5.4.3 Inrichting

De Cloud Services omvatten de faciliteiten van de infrastructuur die nodig zijn voor het leveren van diensten aan GGD'en en GHOR-bureaus die niet als SaaS worden afgenomen.



5.4.4 Onderdelen van de Cloud Services

Cloud Resources

De componenten van de Cloud infrastructuur leveren de resources voor verwerking (compute), netwerk en opslag (storage) voor implementaties die niet worden afgenomen als SaaS.

Dankzij de cloud-technologie en de virtualisatie-technieken zijn deze cloud-oplossingen zeer schaalbaar. Flexibiliteit en wendbaarheid worden gerealiseerd door het automatiseren van creatie en de allocatie van resources (IaC, Infrastructure as Code).

Compute

De verwerkingscapaciteit van de cloud-infrastructuur wordt potentieel door verschillende bouwblokken gebruikt wanneer deze niet als SaaS worden afgenomen. Voor de extreme schaalbaarheid, zoals die verlangd wordt in een pandemische situatie is de mogelijkheid van verticale schaalbaarheid (uitbreiding

computer resources) en horizontale schaalbaarheid (het parallel uitvoeren van meerdere instanties van codes) zeer belangrijk, bijvoorbeeld door het gebruik van microservices en containerorkestratie. De inzet van container-technologie heeft als bijkomend voordeel dat de portabiliteit over verschillende providers wordt verhoogd.

Networking

Het (gevirtualiseerde) netwerk van de cloudoplossing moet aansluiten op de inrichting van Zero Trust Network Access (ZTNA). ZTNA is onderdeel van het bouwblok Veilige Netwerktoegang (par.5.15).

Storage

De (Cloud-)opslagvoorzieningen kunnen in het platform op twee manieren worden ingezet:

1. Als onderdeel van de opslagvoorziening voor de (datacentrische) *Data Services* (par. 5.7) en dan met name de verschillende manieren van opslag (*Opslag Services*, par:5.8). Afhankelijk van te maken keuzes in die bouwblokken, kan de cloudopslag bestaan uit een variatie van PaaS voor bijvoorbeeld databasemanagement diensten (zie volgende paragraaf), IaaS zoals voor archiverings- of bestandsopslag, of CSV-bestanden voor bestandsuitwisseling.
2. Als afzonderlijke voorziening voor (tijdelijke) opslag ten behoeve van de leden van GGD GHOR Nederland, de GGD'en en GHOR-bureaus.

De opslag-voorzieningen worden door externe applicaties of gebruikers alleen benaderd via de Koppel Services.

Cloud Platform Services

Cloudproviders bieden naast rauwe resources (IaaS) ook mogelijkheden om specifieke technologische services af te nemen.

Twee van deze diensten worden in ieder geval als onderdelen van het platform ingezet:

1. Database Management as a Service (DBaaS)
   Met name voor de opslag van OLTP gegevens in de Data Services zullen verschillende vormen van Database Management Systemen worden gebruikt, zoals relationele DBMS-en, Graph DB's en Document- en Column Stores, zowel *highly consistent* (ACID) als *highly available* (BASE). Daarnaast moeten ook andere vormen van opslag (BLOB storage) gebruikt kunnen worden.
   Ten behoeve van het platform worden deze als dienst afgenomen.
2. Container Orkestratie
   Applicaties en applicatiemodules (zoals micro-services) zullen in containers worden uitgevoerd. Met behulp van een container-orkestratie systeem (zoals Kubernetes) worden het leveren (provisioning), de uitrol (deployment) en het beheer (management) van de containers uitgevoerd.

5.4.5 Overige aspecten Cloud Services

Vormen van cloud implementatie: *Private, public en hybrid cloud*

Het datacentrische platform moet zeer flexibel zijn en de mogelijkheid hebben aan toekomstige eisen te voldoen, bijvoorbeeld vanuit een mogelijk vernieuwd Rijksbreed cloudbeleid met betrekking tot dataverwerking en –opslag. Ten aanzien van Cloud Services betekent dit onder andere dat hybride vormen van cloud ondersteunt moeten worden, dat wil zeggen: combinaties van private en public clouds.
De combinatie van beide moet zich transparant gedragen als één omgeving, zodat vanuit de private cloud-omgeving, bijvoorbeeld in het geval van extreme expansie bij een pandemie, ook opgeschaald kan worden naar de public cloud voorziening.

Automatische op- en afschaling

De Cloud Services moeten - waar mogelijk automatisch – kunnen (op-)schalen, zowel verticaal als horizontaal, wanneer het gebruik van een bepaalde resource (CPU-belasting, IO rate, netwerk throughput) daar om vraagt.

Verticaal schalen

Verticale schaalbaarheid betreft het toevoegen van bronnen zoals extra CPU's of geheugen aan een enkel knooppunt in een systeem.

Horizontaal schalen

Horizontale schaalbaarheid wordt bereikt door het uitvoeren van meerdere exemplaren (instances) van services naast elkaar. Dit geeft het cloudplatform de mogelijkheid om de serviceslaag automatisch te schalen. Hiertoe wordt container technologie ingezet (zie 5.4.4).

Bewaking van componenten

Het is belangrijk elk onderdeel van de omgeving te monitoren en te onderkennen wanneer bepaalde grenzen in het systeem bereikt worden. Het systeem moet in staat zijn om automatisch en op het juiste moment de bandbreedte te vergroten om de diensten die gerealiseerd zijn op het cloudplatform draaiende te houden. Monitoring kan extern zijn of door een applicatie worden geïnitieerd, maar in beide gevallen is het uiteindelijke doel om het systeem automatisch te laten schalen op basis van de belasting.

Segmentatie

Op het platform moet het mogelijk zijn langs verschillende dimensies (GGD-regio, Infectieziekte) bewerking en opslag van data te scheiden en de segmenten die zo worden gevormd te voorzien van eigen meta-gegevens zoals beveiligings-attributen voor toegangscontrole (access control). Dit betekent dat ook op de onderliggende voorzieningen (compute, netwerk, storage) van de cloud services deze afscheidingen moeten kunnen worden geïmplementeerd.

5.4.6 Koppelvlakken

De Cloud Services maken gebruik van de volgende bouwblokken:

- Access Control (Centrale IAM Service)
  Met Access Control wordt toegang tot de resources van de cloud omgeving verleend of ontkend op basis van profielen van diensten, gebruikers en context.
- Security Services
  Alle activiteit op de cloud-omgeving dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok *Security Services*.

De Cloud Services kunnen worden gebruikt door de volgende bouwblokken:

- Veilige Applicatie- en Datatoegang
- Veilige Netwerktoegang
- Multi-channel presentatie
- Applicatie Services (Container technology)
- Data Intelligence Services
- Koppel Services (Container technology)
- Applicatie Layering (Container technology)
- Data Service (Container technology)
- Opslag Services

- Privacy Enhancing Technology

5.4.7 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die m.b.t. het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-2.01	Alle cloud voorzieningen voor dataverwerking en -opslag worden afgenomen van datacenters gesitueerd in de Europese Economische Ruimte (EER)	Met deze eis wordt voldaan aan de voorwaarden aan het gebruik van public cloud voor medische gegevens zoals gesteld in het Rijksbreed cloudbeleid.
PAB-2.02	Implementatiemodel is hybrid cloud	• Private cloud ten behoeve van hosting van data (data soevereiniteit). • Public Cloud voor out-scale mogelijkheden. Voor applicaties waarbij niet de maximale resources gereserveerd hoeven te worden.
PAB-2.03	Alle cloud-resources worden geautomatiseerd beheerd met Infrastructure as Code (IaC)	Door infrastructuur inrichting te automatiseren wordt: • de kans op (configuratie-)fouten verkleind; • het on-demand klaarzetten van OTAP-omgevingen versimpeld.
PAB-2.04	Applicaties (modules) op de cloudomgeving worden aangeboden via container technologie	Container technologie: • verhoogt de portabiliteit; • vereenvoudigt het beheer van micro-services; • faciliteert segmentatie (vermindering impact bij wijzigingen en incidenten).
PAB-2.05	Alle containers op de cloud infrastructuur worden beheerd met container-orkestratietechnologie	Het gebruik van container-orkestratietechnologie in de cloud zorgt voor een efficiënt beheer, schaalbaarheid en automatisering van container-gebaseerde applicaties.
PAB-2.06	Hosting redundant en geografisch gespreid	Beschikbaarheid en continuïteit met minimale uitvaltijd.
PAB-2.07	Op- en afschalen van de cloudomgeving moet automatisch gebeuren op basis van de verbruikte resources	Op- en afschaling moet eenduidig, snel en foutloos gebeuren.

5.5 Security Services (PL3a)

5.5.1 Definitie

De IV-beveiliging heeft betrekking op oplossingen en maatregelen voor de processen in de organisatie, de technologie en het gedrag van mensen. Dit betreft ook de sturing daaromtrent en het delen van de benodigde kennis tussen verschillende leveranciers, professionals, GGD'en en zorg- en ketenpartners.

Doel van het bouwblok Security Services is te voorzien in de technologische maatregelen ten behoeve van cyber security op en rondom het platform.

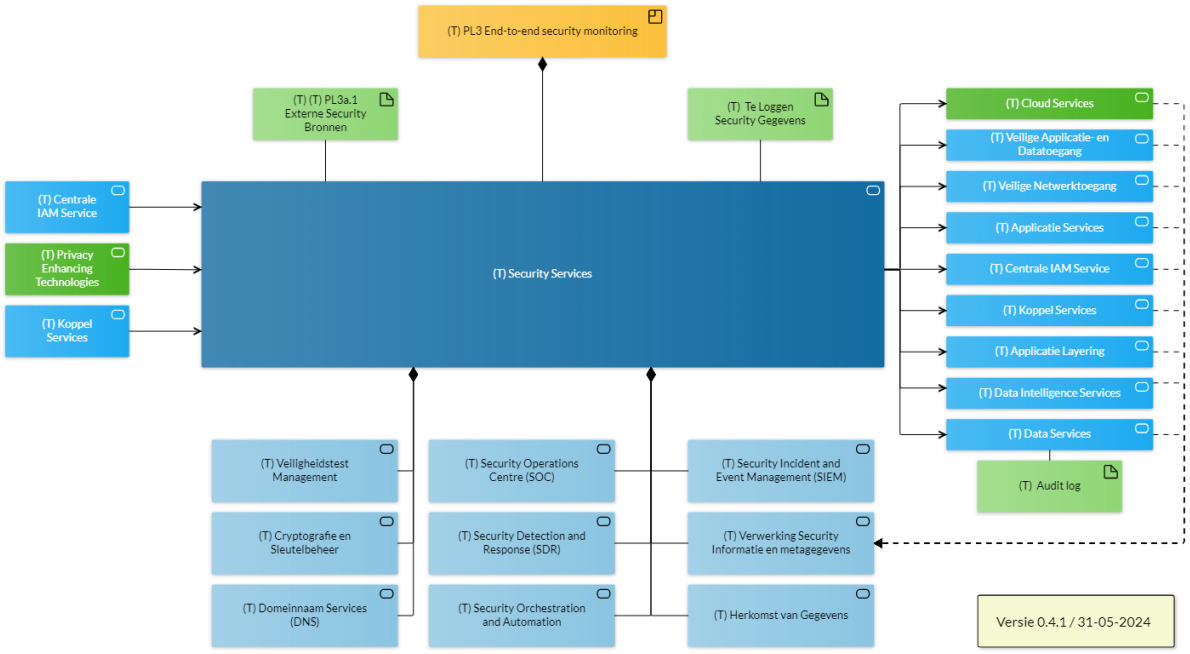
Dit betreft de voorzieningen die nodig zijn om schade te voorkomen door storing, uitval of misbruik van informatiesystemen (zoals het ten onrechte openbaar worden van privacygevoelige (bijzondere) persoonsgegevens, geblokkeerde toegang tot computersystemen of ongewenste verandering van gegevens, bewust of onbewust) en de voorzieningen om schade te beperken en/of te herstellen mocht die onverhoopt toch ontstaan.

5.5.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Security Monitoring
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	De logging infrastructuur dient dermate schaalbaar te zijn dat benodigde log-data gebaseerd op genoemde cijfers gedaan kan worden.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA afspraken en het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van

				de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
3.1.3.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	In het IV/ICT-landschap wordt ten behoeve van het bewaken van de datakwaliteit en -betrouwbaarheid de herkomst van gegevens geregistreerd, zodanig dat onderscheid mogelijk is tussen data welke geregistreerd zijn door bijvoorbeeld burgers of GGD-medewerkers.	Logging wordt geregeld conform NEN 7510, zodat te auditen is wie, wat, waar, wanneer, waarvandaan gedaan heeft. Hierbij wordt de meta data en audittrail altijd meegenomen en vastgelegd in: 1. Log retention omgeving; 2. SIEM.
5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (welke gehost wordt op cloud services) dient dermate te zijn dat genoemde cijfers ondersteund worden.
5.2.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Organisatie en processen	Data governance op de voor de landelijke bestrijding benodigde data is ingericht.	In het conceptmodel zijn SIEM en Log Retention opgenomen.
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)securityprocessen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Er wordt rekening gehouden met de genoemde schaalbaarheid.

5.5.3 Inrichting



5.5.4 Onderdelen van Security Services

Security Services bestaat uit de volgende diensten en voorzieningen:

- PL3a.1 - Verwerking Security Informatie en metagegevens
- PL3a.2 - Security Operations Centre (SOC)
- PL3a.3 - Security Incident and Event Management (SIEM)
- PL3a.4 - Veiligheidstest Management
- PL3a.5 - Security Orchestration and Automation
- PL3a.6 - Security Detection and Response
- PL3a.7 - Cryptografie en Sleutelbeheer
- PL3a.8 - Domeinnaam Services (DNS)
- PL3a.9 - Herkomst van Gegevens

PL3a.1 - Verwerking Security Informatie en metagegevens

Dagelijks worden in de publieke gezondheid aanzienlijke hoeveelheden security- informatie en metagegevens geproduceerd door de aangesloten gebruikersorganisaties en leveranciers. Deze data bevatten security-informatie over activiteiten die plaatsvinden op netwerken, applicaties en computers.

Voor het tijdig en adequaat acteren op signalen van vermoedelijk afwijkend gedrag is het essentieel dat deze gegevens zo snel mogelijk geschikt worden gemaakt voor verdere verwerking binnen Security Services en de aangesloten oplossingen. Gezien de zeer grote hoeveelheden data en de diversiteit van dataformaten, moeten de voorzieningen hiertoe maximaal schaalbaar en wendbaar zijn.

PL3a.2 - Security Operations Centre (SOC)

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 netwerken, systemen en hard- en software functioneren in de organisatie.

PI3a.3 - Security Incident and Event Management (SIEM)

SIEM gebruikt gegevens uit alle aangesloten informatievoorzieningen. SIEM voorziet in het continu, (near-) realtime monitoren van beveiligingsmaatregelen en afwijkend gedrag in applicaties, data en infrastructuren. Het voorziet in inzicht van verzamelde gegevens op lange termijn, maar ook in historische analyses en trendanalyses van die gegevens. SIEM biedt naast monitoring en triage ook ondersteunende functies voor threat hunting en forensisch ICT-onderzoek.

PL3a.4 - Veiligheidstest management

Veiligheidstest-management is het uitvoeren en managen van testen rondom een applicatie- en infrastructuursysteem ten behoeve van het verbeteren van de veiligheid. Specifiek rondom het continu, automatisch en niet automatisch, creëren van:

- inzicht in kwetsbaarheden en daarbij behorende risico's;
- voorstellen van te implementeren maatregelen om kwetsbaarheden te mitigeren en daarmee risico's te verlagen.

Veiligheidstest-management richt zich op de integrale veiligheid van een applicatie- en/of infrastructuursysteem vanaf de buitenkant en de binnenkant van een systeem. Dit verbetert de integrale veiligheid van het betreffende systeem, onder meer door *vulnerability* management (het verbeteren van de veiligheid van een applicatie systeem vanuit de binnenkant, zoals *hardening* en *patching*).

PL3a.5 - Security Orchestration and Automation

Security Orchestration, Automation and Response (SOAR), is een oplossing die SIEM-platforms aanvult en ondersteunt. SOAR is erop gericht om over verschillende organisaties en securityleveranciers (de ketens) heen gebeurtenisgegevens te verrijken, het identificeren van kritieke incidenten te vereenvoudigen en reacties op specifieke gebeurtenissen of triggers te automatiseren. Het werkt met een zeer hoge automatiseringsgraad, die pas menselijke interventie nodig heeft als er echt een probleem is dat aandacht vereist.

PL3a.6 - Security Detection and Response

Security Detection and Response is een oplossing die detectie, en de reactie op deze detectie, volledig automatisch tracht af te handelen met diensten en oplossingen die voorzien in:

- Managed Detection & Response (MDR), die technologieën (zoals SIEM, EDR, NDR en XDR) en menselijke expertise combineert om de organisatie beter te beschermen tegen cyberdreigingen;
- Endpoint Detection & Response (EDR), waarbij tools continu alle endpoints in het netwerk monitoren;
- Network Detection & Response (NDR), voor een 360-graden kijk op netwerkverkeer;
- Extended Detection and Response (XDR), wat een proactieve oplossing biedt voor ingewikkelde beveiligingsuitdagingen bij het werken in hybride omgevingen, met meerdere Clouds en meerdere leveranciers in een veranderend bedreigingslandschap.

PL3a.7 - Cryptografie en Sleutelbeheer

Cryptografie en Sleutelbeheer verzorgt gecentraliseerde cryptografische voorzieningen en het beheer van digitale sleutels voor GGD'en en zorg- en ketenpartners. Door de omgevingen die gebruik maken van cryptografie en sleutelbeheer continu te blijven managen, ontwikkelen en te verbeteren, wordt de mate van veiligheid van medische en (bijzondere) persoonsgegevens verhoogd.

Vanwege de eisen van vertrouwelijkheid en integriteit wordt (waar mogelijk) gebruik gemaakt van 'peer-reviewed' goedgekeurde cryptografische methoden en sleutelbeheer. Alle onderliggende mechanismen, protocollen, en data(opslag)-technieken die in de omgevingen van GGD'en en zorg- en ketenpartners gebruikt worden, hanteren de voorgeschreven methoden.

PL3a.8 - Domeinnaam Services (DNS)

Domeinnaam Services (DNS) verzorgen de automatische vindbaarheid van applicatie-, data-, infrastructuur- en securityservices op interne en externe netwerken. Daarnaast verzorgen de services de administratie van de registratie en de beheerconfiguratie van DNS domeinen in een centrale omgeving. Domeinnaam Services (DNS) richten zich op DNS registraties en DNS server- en configuratiemanagement voor GGD GHOR Nederland, GGD'en, zorg- en ketenpartners.

PL3a.9 – Registratie Herkomst van Gegevens

Registratie Herkomst van Gegevens betreft het leveren en managen van de automatische herleidbaarheid van gegevens, met name (bijzondere) persoonsgegevens.

Registratie Herkomst van Gegevens verzorgt de administratie, begeleiding en afhandeling van uitwisselingsovereenkomsten tussen aanbieders en gebruikers van gegevens.

5.5.5 Koppelvlakken

Alle bouwblokken, maken gebruik van *Security Services* voor de verwerking van audit-, systeem- en applicatieloggegevens. Daarnaast maken alle bouwblokken - daar waar toepasbaar - gebruik van de overige diensten van *Security Services*.

Het bouwblok *Security Services* levert (geautomatiseerd) beveiligingsonderzoek en beveiligingsinformatie af aan de leveranciersomgevingen van de andere bouwblokken ten behoeve van het verbeteren van beveiliging van de voorzieningen in het betreffende bouwblok.

De volgende bouwblokken uit dit conceptuele model worden gebruikt door bouwblok PL3a *Security Services*:

- Centrale IAM Service - voor de authenticatie van gebruikers en services op *Security Services* diensten;
- Koppel Services – voor de samenwerking van diensten ten behoeve van de uitwisseling van gegevens;
- Privacy Enhancing Technologies – voor het management van diensten die tokenisation verzorgen.

Verder maakt het bouwblok *Security Services* gebruik van Externe Security Bronnen:

- Threat Intelligence – voor het aanleveren van indicators of compromise, open en closed source intelligence;
- Log(filter)regels – voor het kunnen filteren op gebeurtenissen die in logbestanden worden vastgelegd door bronsystemen;
- Common Vulnerability Scoring System (CVSS) – Voor het inzicht in vulnerabilities van gebruikte software en hardware;
- Materiaal lijst (BOM's) bronnen – voor het overzicht van asset gegevens

De dienst *Verwerking van Security en Metagegevens* fungeert als de centrale in- en uitgang voor alle koppelvlakken die gegevensuitwisselingen met *Security Services* hebben.

5.5.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die met betrekking tot het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-3a.01	Het platform maakt gebruik van de bestaande SOC/SIEM voorzieningen.	Er is een bestaande SOC/SIEM oplossing waarvoor een roadmap bestaat.
PAB-3a.02	Alle IV-voorzieningen worden aangesloten op de Security Services voor de betreffende IV-voorziening voordat ze in productie gaan.	Het onder controle krijgen van de juiste security baseline voor IV-voorzieningen is een continu proces. Het aangesloten zijn van alle IV-voorzieningen op Security Services draagt bij aan een betere en snellere bescherming tegen aanvallen en kwetsbaarheden.
PAB-3a.03	Alle gegevensuitwisseling tussen de componenten van Security Services en met andere bouwblokken gebeurt (exclusief) via het component Verwerken Security Informatie en Metagegevens.	Hiermee wordt maximale controle bereikt voor de correcte, en tijdige verwerking van Security Gegevens.
PAB-3a.04	De IV-voorzieningen van leveranciers, zorg- en ketenpartners en GGD GHOR Nederland die data bewerken of uitwisselen met het datacentrische platform, leveren altijd beveiligingsgegevens aan op de centrale Security Services.	Alle verwerking en opslag van gegevens die eigendom zijn van de GGD'en wordt gecontroleerd en gemonitord.
PAB-3a.05	Alle IV-voorzieningen van zowel leveranciers als zorg- en ketenpartners en GGD GHOR Nederland die onderdeel uitmaken van het datacentrische platform, wisselen de beveiligingsgegevens met Security Services uitsluitend uit via de centrale Verwerken Security Informatie en Metagegevens voorziening.	Verspreiding van securitygegevens over verschillende systemen is ongewenst omdat daardoor onvoldoende controle op gebruik en misbruik van deze gegevens kan worden uitgevoerd.
PAB-3a.06	De situationele informatie (context) die nodig is voor de interpretatie van securitygegevens moeten bij de securitygegevens worden bewaard.	Alle benodigde metagegevens, zoals onder andere beschreven in NEN7513, en overige asset en configuratie managementinformatie, worden meegestuurd naar de Security Services gegevens voorzieningen. Daarmee kan Security Services de opgevangen securitygegevens verrijken met situationele informatie om securitygegevens te kunnen interpreteren.
PAB-3a.07	Voor het vergroten van de volwassenheid volgens het SOC Capability Maturity Model (SOC-CMM) worden de producten gebruikt die vanuit SOC-CMM beschikbaar worden gesteld (op dit moment zijn dat xlsx bestanden).	Eenheid van taal en standaardisatie. SOC-CMM is in Nederland de de-facto standaard welke ook gebruikt wordt door Z-CERT.
PAB-3a.08	Asset en configuratie management informatie-uitwisseling gebruiken OWASP Bill-of-Materialen (BOM's) CycloneDX gegevens formaat	OWASP heeft een open dataformaat ontwikkeld samen met leveranciers van hardware en software. Dit formaat moet binnen de asset en configuratie managementprocessen gebruikt worden voor het uitwisselen van BOM's. Deze geeft daarmee altijd een up-to-date inzicht in de geleverde goederen binnen de diensten en oplossingen.
PAB-3a.09	Voor het bouwblok Security Services wordt het woordenboek gebruikt zoals dat is opgesteld en wordt onderhouden door Cyberveilig Nederland. bron: https://cyberveilignederland.nl/woordenboek	Het gebruik van dit externe woordenboek bevordert de communicatie met leveranciers en professionals.

PAB-3a.10	De verwerking van securitygegevens, zoals beschreven in de dienst "Verwerken Security Informatie en Metagegevens" wordt uitgevoerd in een andere oplossing dan een SIEM oplossing.	Op deze manier is het mogelijk om meerdere SOC en SIEM oplossingen tegelijk gebruik te laten maken van de centrale functies voor de verwerking van securitygegevens en is het relatief eenvoudig om een gebruikte SOC en SIEM oplossing te vervangen.
PAB-3a.11	Security gegevensverwerking en opslag draaien op zeer schaalbare oplossingen	De Security Services voor de verwerking en opslag van securitygegevens moeten ten minste zo schaalbaar zijn als de voorzieningen die zij monitoren.
PAB-3a.13	Alle Security Services voorzieningen maken, voor de verwerking en opslag van securitygegevens, gebruik van de functie Opslaan Securityinformatie en Metagegevens.	Op deze manier wordt voldaan aan de eis vanuit de afdeling Compliance om invulling te geven aan de uitvoering van NEN-7513 door security-informatie en gebeurtenissen gescheiden op te slaan.

5.6 Privacy Enhancing Technologies (PL3b)

5.6.1 Definitie

Het virtuele bouwblok Privacy Enhancing Technologies (PET) omvat de diverse technieken en diensten die ingezet kunnen worden voor verregaande bescherming van privacygevoelige gegevens (*in rest*, *in use* en *in transport*) en inzicht in het gebruik van deze gegevens.
PET's implementeren maatregelen ten behoeve van de fundamentele beginselen inzake gegevensbescherming, zoals:

- Wettigheid
- Eerlijkheid en transparantie
- Doelbinding
- Dataminimalisatie
- Nauwkeurigheid
- Opslagbeperking
- Integriteit en vertrouwelijkheid
- Verantwoordelijkheid

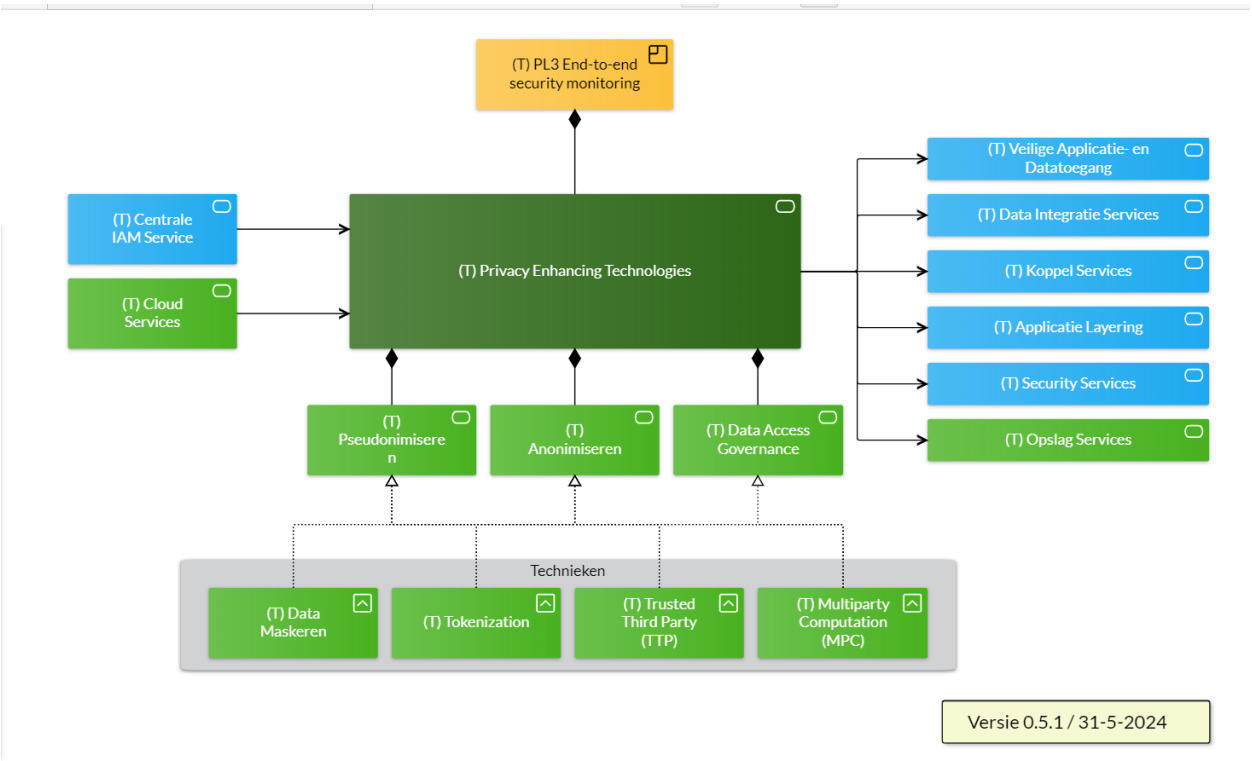
5.6.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Privacy Enhancing Technologies
Nr	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	De PET infrastructuur dient dermate schaalbaar te zijn dat privacy technologieën de workload gebaseerd op genoemde cijfers aankunnen.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur	Middels SLA afspraken en het realiseren van redundantie en geo spreiding wordt hier rekening mee gehouden.

			(RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Alle componenten volledig en snel schaalbaar
5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen	Inrichting (schaalbaarheid) van de services (welke gehost wordt op cloud services) dient dermate te zijn dat genoemde cijfers ondersteund worden.

			deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	
5.2.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Organisatie en processen	Data governance op de voor de landelijke bestrijding benodigde data is ingericht.	In het conceptmodel is Data Access Governance opgenomen
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)securityprocessen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Rekening houdend met genoemde schaalbaarheid

5.6.3 Inrichting



Privacy Enhancing Technologies bestaan o.a. uit:

- Vormen van pseudonimiseren
- Vormen van anonimiseren
- Data Access Governance

Technieken die hiervoor gebruikt worden zijn o.a.:

- Data Maskeren
- Tokenization
- Data TTP (Trusted Third Party)
- Multiparty Computation (MPC)

5.6.4 Onderdelen van Privacy Enhancing Technologies

Pseudonimiseren is een beveiligingsmaatregel. Door persoonsgegevens te pseudonimiseren wordt het moeilijker gemaakt om deze gegevens te herleiden naar personen. En dat maakt bijvoorbeeld de impact kleiner bij een datalek. Een methode om persoonsgegevens te pseudonimiseren is hashing.
Bij gepseudonimiseerde gegevens is weliswaar niet direct duidelijk over welke personen de gegevens gaan, maar de gegevens kunnen alsnog herleidbaar zijn tot specifieke personen door aanvullende gegevens te gebruiken.

Anonimiseren

Anonimiseren, ook wel datamasking genoemd, is een methode waarbij persoonsgegevens zodanig worden bewerkt dat deze niet meer gebruikt kunnen worden om een persoon te identificeren. Deze bewerking is onomkeerbaar.

Data Access Governance

Data Access Governance (DAG) biedt de mogelijkheid om te identificeren welke ongestructureerde gegevens worden opgeslagen, wie er toegang toe heeft en wat de relevantie van de gegevens is. Data Access Governance kan ook actieve bescherming bieden voor repositories die gevoelige en waardevolle gegevens opslaan, en aan de hand van toegangsbeoordelingen (formeel) bevestigen dat alleen geautoriseerde gebruikers toegang hebben tot deze gegevens.

Technieken

Data Maskeren

Data Maskeren is een oplossing die ervoor zorgt dat er buiten de productieomgeving gewerkt kan worden met representatieve data. Bijvoorbeeld om software te testen of analyses te maken.

Tokenization

Tokenization is de bescherming van gegevenselementen op een omkeerbare en formaat-besparende manier. Tokenization technieken maken niet alleen het behoud van het onderliggende gegevensformaat mogelijk, maar ook het "voorschrijven" van het uiterlijk van het beschermde element. Dit omvat bijvoorbeeld het behoud van de lengte van de onderliggende gegevens of het opvullen tot een gewenste lengte. Andere opties zijn onder andere om binnen hetzelfde alfabet te blijven of de gegevens naar een ander alfabet te transformeren.

Data TTP (Trusted Third Party)

Een TTP wordt voornamelijk ingezet voor het op persoonsniveau samenvoegen, koppelen of verrijken van gegevens van verschillende bronbestanden of verstrekkers, op zo'n manier dat afnemers alleen gepseudonimiseerde gegevens ontvangen. Het kan daarbij zowel gaan om onomkeerbare (eenweg-) als om omkeerbare (tweeweg-) pseudonimisering. Bij onomkeerbare pseudonimisering kunnen de gepseudonimiseerde gegevens niet op persoonsniveau worden teruggekoppeld tot de bron, bij omkeerbare pseudonimisatie kan dat (met behulp van de TTP) wel.

De diverse bronbestanden kunnen bestanden zijn van verschillende GGD'en. Indien gegevens bij verschillende GGD'en bovenregionaal gecorreleerd dienen te worden, kan dit met behulp van een TTP gerealiseerd worden. Dit is nodig als er bijvoorbeeld geen toestemming van de burger is, of een wettelijke grondslag.

Een 'eigen' TTP, waarbij bijvoorbeeld GGD GHOR Nederland als TTP optreedt voor de verschillende GGD'en, vergt een juridische basis voor GGD GHOR Nederland. Het meest zuiver is een wettelijke grondslag. Een TTP kan ook worden afgenomen, zoals ZorgTTP.

Multiparty Computation (MPC)

MPC is een cryptografische techniek die meerdere partijen in staat stelt om bewerkingen uit te voeren op gegevens. Deze bewerkingen worden zo uitgevoerd dat geen enkele partij iets leert dat verder gaat dan zijn eigen invoer en uitvoer. Met andere woorden, de gegevensinvoer door de ene partij blijft verborgen voor de andere partijen. De deelnemende partijen bepalen wie de uitkomst van de berekening mag inzien.

Secure Multiparty Computation (MPC) is een techniek om een TTP te vervangen door een beveiligd protocol waarbij dezelfde partijen betrokken zijn, maar geen TTP.

5.6.5 Koppelvlakken

Privacy Enhancing Technologies maakt gebruik van:

- Cloud Services
- Security Services: alle activiteit op de *Privacy Enhancing Technologies* dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok *Security Services*

Privacy Enhancing Technologies wordt gebruikt door:

- Opslag Services
- Security Services
- Data Integratie Services (onderdeel *Data Intelligence Services*)
- Koppel Services
- Applicatie Layering

5.6.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die met betrekking tot het bouwblok zijn geformuleerd

ID	Architectuurbesluit	Rationale
PAB-3b.01	Voor de bescherming van privacygevoelige gegevens wordt gebruik gemaakt van Privacy Enhancing Technologies (PET).	PET bieden een hoge mate van bescherming.

5.7 Data Services (PL4a)

5.7.1 Definitie

De dienst *Data Service* (PL4) bestaat uit twee technische bouwblokken: het bouwblok Data Services en het bouwblok Opslag Services. De functie van het bouwblok Data Services is het afhandelen van data-verwerkingsverzoeken. Data-verwerkingsverzoeken kunnen zijn: het bewaren en verstrekken van data, maar

ook het bewerken van data. Data-verwerkingsverzoeken worden door de System-API's van het bouwblok Data Services ontvangen.

- De API-specificaties zijn gebaseerd op een domeinmodel. Wijzigingen in het domeinmodel worden zo veel mogelijk geautomatiseerd doorgevoerd in de dataopslagstructuren, databewerkingsmechanismes en de API-deployments.
- De verzoeken om dataverwerking komen via het bouwblok Applicatie *Layering* aan bij de System-API's van het bouwblok Data Services. De verzoeken om data te bewaren worden vervolgens vertaald naar een verzoek om de data op te slaan, dat wordt uitgevoerd door het bouwblok Data Opslag Services. De verzoeken om data te verstrekken worden vertaald naar een verzoek om de data op te halen, dat ook wordt uitgevoerd door het bouwblok Data Opslag Services.

5.7.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Data Services
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (run-modus) dient dermate te zijn dat genoemde cijfers ondersteund worden.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA afspraken en het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.
1.1.4.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om vastgestelde beleidswijzigingen en/of vastgestelde wijzigingen in LCI-richtlijnen die leiden tot wijzigingen in bestaande werkinstructies/werkprocessen, middels aangepaste configuratie binnen 24 uur uniform door te voeren bij alle uitvoerders.	Met configuratie wijzigingen worden hier met name veranderingen in selectievragen bedoeld. Deze content- en workflow-aanpassingen moeten snel, eenvoudig en uniform aangebracht kunnen worden. Aanpassingen binnen het domein model (t.b.v. content) dienen binnen 24 uur over de gehele keten (incl. RIVM) actief te zijn. Hiervoor moeten werkprocessen worden ingericht.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar,	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen,	De LCM en Update policy worden contractueel vastgelegd met de leveranciers. Dit

	robuust en betrouwbaar.		infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	geldt zowel voor de ontwikkel- als de run-modus componenten.
1.1.6.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	Hierbij wordt gebruik gemaakt van een aanpasbaar domein model inclusief procesafspraken om gezamenlijk snel tot uitbreidingen te kunnen komen.
1.1.7.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het opschalen en doorvoeren van wijzigingen ten behoeve van de landelijke bestrijding van een A-infectieziekten vormt geen belemmering in de ondersteuning van de bestrijding van overige infectieziekten waarvan de bestrijding door het IV/ICT-landschap wordt ondersteund.	Data API's moeten horizontaal schaalbaar zijn. (meerdere instances)
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend

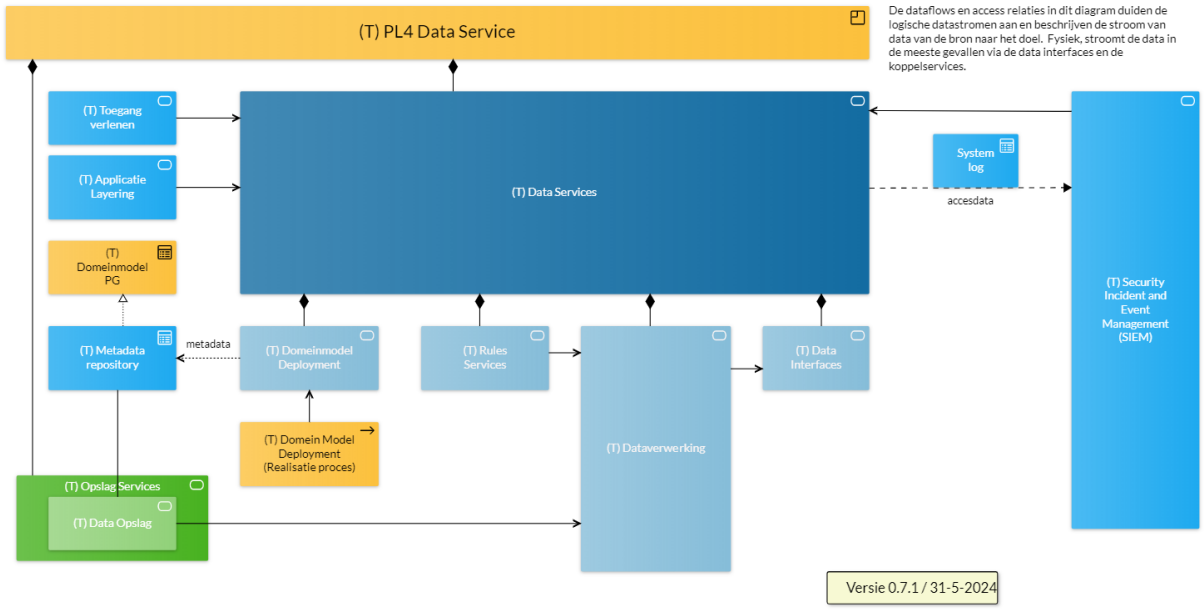
				geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.3	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Organisatie en beheer- en ontwikkelprocessen maken het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	Aanpasbaar domeinmodel, welke snel te (indien mogelijk geautomatiseerd) executeren is.
2.1.1.	Processen voor de landelijke bestrijding van A-infectieziekten zijn uniform.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat professionals van uitvoerders (tijdens pandemieën, in de warme fase) door de LFI vastgestelde blauwdruk-inrichting(en) van processen en applicaties gebruiken. Deze blauwdrukken zijn te allen tijde eenvoudig, online te raadplegen voor betrokkenen.	Data Services worden zo ingericht dat aanpassingen op het domeinmodel snel actief gerealiseerd kunnen worden inde IV-stack.
2.1.3.	Processen voor de landelijke bestrijding van A-infectieziekten zijn uniform.	Techniek	Noodzakelijke aanvullingen op de blauwdruk voor een individuele uitvoerder vormen geen belemmering voor de werking van het IV/ICT-landschap, uniforme werkprocessen en ondersteuning ten behoeve van de bestrijding van landelijke uitbraken van A-infectieziekten.	Via een aanpasbaar domeinmodel incl. procesafspraken is het mogelijk snel tot (gezamenlijke) uitbreidingen te komen.
2.1.4.	Processen voor de landelijke bestrijding van A-infectieziekten zijn uniform.	Techniek	Het IV/ICT-landschap voorziet in het faciliteren, afhandelen en vastleggen van digitale contacten (online en telefonisch) met burgers door (landelijke) klantcontactcentra. Geregistreerde contacten met burgers zijn voor analysedoeleinden raadpleegbaar.	IV-ondersteuning van processen is onderdeel van een gemeenschappelijk domeinmodel, hetgeen helpt tot uniformering
3.1.3.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	In het IV/ICT-landschap wordt ten behoeve van het bewaken van de datakwaliteit en -betrouwbaarheid de herkomst van gegevens geregistreerd, zodanig dat onderscheid mogelijk is tussen data welke geregistreerd zijn door bijvoorbeeld burgers of GGD-medewerkers.	Metadata m.b.t bron ook opslaan, ook i.v.m. doelbinding.
3.2.1.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Organisatie en processen	Medische-operationele processen hebben waar mogelijk een digitale variant, die op gelijkwaardige wijze de analoge dienstverlening digitaal aanbiedt aan burgers, met inachtneming van de AVG en met aandacht voor burgers die terughoudend zijn in het delen van hun gegevens.	Inrichting van domeinmodel bevat ook procesinformatie voor verwerking m.b.t. IV-middelen.

4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	Alle componenten volledig en snel schaalbaar.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Alle componenten volledig en snel schaalbaar.
4.1.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap ondersteunt een geïntegreerde klantreis voor burgers, inclusief het principe eenmalige registratie, meervoudig gebruik (de verschillende uitvoerders in de keten hebben dus toegang tot dezelfde informatie). Gebruik van digitale middelen door burgers wordt gefaciliteerd op gangbare web- en mobiele technologieën.	Brondata eenmalig opslaan, meervoudig gebruik.
4.1.5.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap faciliteert correcte en complete invoer in de bron (door burgers en door uitvoerders) en voorkomt foutieve invoer (of omissies) zoveel als mogelijk en proactief.	Het platform gaat uit van een uitbreidbaar data-centrische inrichting inclusief invoer bewerkingsregels die foutieve invoer voorkomen.
4.1.6.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorkomt een te grote afhankelijkheid van een of meerdere leveranciers (vendor lock-in). Applicaties moeten door nieuwe leveranciers overgenomen kunnen worden op basis van een vooraf overeengekomen Escrow overeenkomst.	Het (data-centrisch gebaseerde) platform zal voorzien (via modulaire ontwikkeling) in een ontkoppeling tussen de presentatie-, applicatie- en data lagen.
4.2.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	(Administratieve) handelingen die gedigitaliseerd kunnen worden, worden zoveel als mogelijk gedigitaliseerd.	Het domeinmodel moet rekening houden met digitalisering (administratieve) handelingen.
4.2.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	De regie- en beheerorganisatie van uitvoerders zijn voorbereidt op het leveren van functionele support aan eindgebruikers tijdens warme fase. *[met warme fase wordt pandemische situatie bedoeld]*	Functioneel support dient ingericht te worden.
5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (welke gehost wordt op Cloud Services) dient dermate te zijn dat genoemde cijfers ondersteund worden. Data Services en Opslag Services worden bij elkaar gehost.

5.1.2.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat in het kader van de Wpg en de Wet op het RIVM verplichte meldingen "onverwijld" aan het RIVM ter beschikking gesteld worden door digitale en geautomatiseerde informatie-uitwisseling en/of door verlening van toegang tot data.	Door gemeenschappelijk domeinmodel RIVM en GGD kan informatie eenvoudig en eenduidig gedeeld worden. Technische voorzieningen voor aanlevering data en/of overzicht zijn onderdeel van het platform, er is beschikking over juiste data API's.
5.1.3.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat voor sturing op medische-operationele processen benodigde stuur- en managementinformatie beschikbaar is voor de LFI.	Door gemeenschappelijk domeinmodel LFI, RIVM en GGD kan informatie eenvoudig en eenduidig gedeeld worden. Technische voorzieningen voor aanlevering data en/of overzicht zijn onderdeel van het platform, er is beschikking over juiste data API's.
5.1.4.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk om de te verzamelen meldingsinformatie binnen 24 uur landelijk aan te passen.	Snel aanpasbaar domeinmodel inclusief proces om dit ook daadwerkelijk snel (binnen 24 uur) over de hele IV-stack actief te maken.
5.1.5.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevensuitwisseling is gebaseerd op gangbare informatiestandaarden zoals HL7.	Bij de definitie van de data in het semantisch datamodel zal rekening moeten worden gehouden met formaat waardes en welke velden verplicht zijn in bepaalde data relaties.
5.1.7.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevenskwaliteit wordt continue en geautomatiseerd bewaakt. En er wordt proactief op gerapporteerd. Applicaties waarin bronregistraties worden ingevoerd voorkomen actief registratiefouten, signaleren actief registratiefouten en bieden sturingsinformatie op datakwaliteit.	Bij de definitie van de data in het semantisch datamodel zal rekening moeten worden gehouden met formaat waardes en welke velden verplicht zijn in bepaalde data relaties.
5.2.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Organisatie en processen	Data governance op de voor de landelijke bestrijding benodigde data is ingericht.	Er dient met name een proces te zijn om domein model aan te passen.
5.2.2.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Organisatie en processen	Datamanagement, waaronder processen voor monitoring van datakwaliteit en de verbetering daarvan en voor metadata-management, is ingericht.	Data- en informatiemanagement zijn de hoekstenen van de data-centrische oplossing van het platform.

5.2.3.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Organisatie en processen	Gegevensregistratie en datakwaliteit zijn vast onderdeel in de reguliere sturingsoverleggen.	In te richten regulier sturingsoverleg.
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)securityprocessen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Rekening houdend met genoemde schaalbaarheid.

5.7.3 Inrichting



Data Services scheiden de Data Opslag van de applicatiefunctionaliteit.
De Data Services zijn verantwoordelijk voor de verwerking van de data die aangeboden of opgevraagd kan worden via de Data Interfaces. Er zijn drie soorten verzoeken die gedaan kunnen worden aan de Data Services om data te verwerken:

- Het opslaan van aangeboden data;
- Het afleiden van data uit de aangeboden en al opgeslagen data;
- Het teruggeven van opgeslagen of afgeleide data.

De Data Services slaan zelf geen data op. Deze verantwoordelijkheid ligt bij de Opslag Services. De Data Services maken wel gebruik van de Opslag Services.

- De Data Services bieden data aan de Opslag Services aan voor permanente opslag;
- De Data Services vragen data op uit de Opslag Services.

De Data Services voorzien in de mogelijkheid om *event based*, (near-)realtime afgeleide data (bijvoorbeeld geaggregeerde gegevens) te actualiseren.

De Data Services bewaken de datakwaliteit. Dat kan op het moment van invoer maar ook daarna. De resultaten van de datakwaliteitscontrole worden gelogd als zogenaamde metadata (data over data). Deze

metadata wordt opgeslagen op een wijze die toegankelijk en bruikbaar is voor audit trails en datamanagementrapportages. De kwaliteitscontrole wordt gedaan op basis van validatieregels. Een validatieregel kan bijvoorbeeld een bepaalde geldige range bevatten, maar ook logica om te controleren of een bepaalde waarde, zoals een DigiD, klopt.

Zie o.a. overheidsstandaard Stelselcatalogus en Linked Data omtrent Metadata: Vocabularium | Stelselcatalogus - linked data

5.7.4 Onderdelen van de Data Services

De Data Services bestaan uit verschillende services:

- De Data Interfaces: de expeditieafdeling van de Data Services. Deze bestaat uit API's waaraan een verzoek kan worden aangeboden om data te verwerken.
- Dataverwerking: dit is de werkplaats van de Data Services. Hier worden de verzoeken om dataverwerking afgehandeld. De data worden verwerkt in overeenstemming met de geldende eisen voor databeheer zoals bewaartermijnen, vertrouwelijkheid en beschikbaarheid.
- Rules Services: deze bevat de functionaliteit om gegevens correct te kunnen verwerken, in overeenstemming met de geldende semantische dataverwerkingsregels.
- Domeinmodel Deployment: dit bevat de functionaliteit om het domeinmodel te kunnen onderhouden.
- Domeinmodel Deployment: Bevat functionaliteit om het domeinmodel om te zetten naar werkende IV-componenten, zoals API's, semantische dataverwerkingsregels en databeheer regels.

Data Interfaces

De Data Interfaces bestaan uit System-API's en dienen gebaseerd te zijn op de definities in het Domeinmodel. Het uitgangspunt hierbij is een direct implementeerbaar model.
Systeem-API's kunnen met elkaar gecombineerd worden om complexere, zogenaamde process-API's te kunnen vormen. Deze process-API's maken geen onderdeel uit van de Data Services.
De Data Interfaces worden via de Koppel Services aangeboden aan de buitenwereld.

Dataverwerking

De Dataverwerking is onderdeel van de Data Services. De Dataverwerking zorgt voor de verwerking van de dataverwerkingsverzoeken die via de Data Interfaces worden gedaan. De Dataverwerking gebruikt de Rules Services (zie onderstaand) om de data correct te kunnen verwerken in overeenstemming met de geldende semantische dataverwerkingsregels uit het actuele domeinmodel. De Dataverwerking gebruikt Data Opslag om data op te kunnen slaan of data op te halen. De Dataverwerking vult de auditlog en maakt deze beschikbaar voor het SOC/SIEM.

Rules Services

De Rules Services zijn een apart onderdeel van de Data Services. De Rules Services worden door de Dataverwerking gebruikt om data te verwerken in overeenstemming met de geldende regels uit het actuele domeinmodel. Deze regels zijn de uitvoerbare implementatie van de bedrijfsregel zoals gedefinieerd in het domeinmodel.
Er zijn verschillende soorten regels:

- Input regels:
    - Voeren controles uit op de invoer van data. Bijvoorbeeld: er mogen geen rookwaren verkocht worden aan minderjarigen.

    - Voeren controles uit op de volgorde van de data invoer. Bijvoorbeeld: een bestelling mag niet verzonden worden voordat deze ingepakt is.
- Output regels:
    - Voeren berekeningen uit om gevraagde of benodigde data te kunnen leveren. Bijvoorbeeld: bepalen minderjarigheid: iemand is minderjarig als het verschil tussen de geboortedatum en de huidige datum minder is dan 18 jaar.

Domeinmodel deployment

Domeinmodel deployment zorgt ervoor dat wijzigingen in het domeinmodel (de kern van het domeinmodel en de implementatiedetails) correct omgezet worden in IV-componenten zoals datastructuren, dataverwerkingsmechanismes en API-deployments.

Domeinmodel deployment dient domeinmodellen te kunnen verwerken waarbij er sprake is van hiërarchie in de modellen (class model/overerving) en hergebruik van structuurdefinities van de verschillende modellen.

Logging

De Data Services leveren een systeemlog aan de SOC/SIEM.

De Dataverwerking verzorgt de auditlog. Dit is de log van de toegang (lezen, schrijven) tot de data en de mutaties van de data of de metadata. Ook de herkomst van de data wordt gelogd.

Domeinmodel en data access

In het domeinmodel worden de dataverwerkingsrollen gespecificeerd. Een dataverwerkingsrol koppelt een processtap aan de dataverwerkingsverzoeken en processtatusinformatie die nodig zijn om deze processtap correct uit te voeren. Voor elke rol wordt gedefinieerd welke dataverwerkingsverzoeken deze rol moet kunnen doen (zoals bewaren, bewerken en verstrekken) en op welke gegevens. Ook is er gedefinieerd welke processtatusinformatie deze rol nodig heeft om de processtap te kunnen uitvoeren.

Voorbeelden van dataverwerkingsrollen:

- afhandelen van het verzoek (beslissen om gehoor te geven aan het verzoek of deze te weigeren);
- het uitvoeren van de verkoop zelf;
- opleveren verkoop aan de verzoeker (beslissen om de verkoop op te leveren of niet);
- deze drie rollen kunnen gecombineerd worden tot de rol “uitvoerder verkoop”

Een voorbeeld van dataverwerkingsrechten:

- De rol “afhandelen van verkoopverzoek” mag dataobjecten ten aanzien van de verkoop aanmaken.

De dataverwerkingsrollen moeten aan organisatierollen toegekend worden. Deze organisatierollen moeten aan digitale identiteiten toegekend worden.

5.7.5 Koppelvlakken

De *Data Services* maakt gebruik van Access Control.

Dataverwerking maakt gebruik van Data Opslag om data op te halen en weg te schrijven in bijvoorbeeld een database.

De *Data Services* maken gebruik van de *Applicatie Layering,* bijvoorbeeld wanneer een systeemcomponent een data-API aanroept. De aanroep wordt dan bemiddeld door de *Koppel Services*.

Security Services ontvangt auditlog data van Data Verwerking, bijvoorbeeld over welke wijzigingen er zijn gemaakt op de data of metadata en over wie, wanneer data of metadata heeft bekeken of aangepast.

5.7.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die met betrekking tot het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-4a.01	Aanmaken van auditlog records gebeurt in de Data Services. Andere services, zoals Applicatie- en Koppel Services, leveren hiervoor de metadata.	Het werkelijk verlenen of weigeren van toegang (acces control) op basis van (input-)regels gebeurt in Data Services.
PAB-4a.02	Data Services en Opslag Services worden bij elkaar gehost	Performance van de data toegang moet ook voor de grote aantallen transacties tijdens pandemieën gegarandeerd zijn.

5.8 Opslag Services (PL4b)

5.8.1 Definitie

Het bouwblok *Opslag Services* voorziet in de technische functies voor de opslag van data en de logistiek daaromheen.

In combinatie met het bouwblok *Data Services* zijn *Opslag Services* de technische invulling van de dienst *Data Service* (PL4).

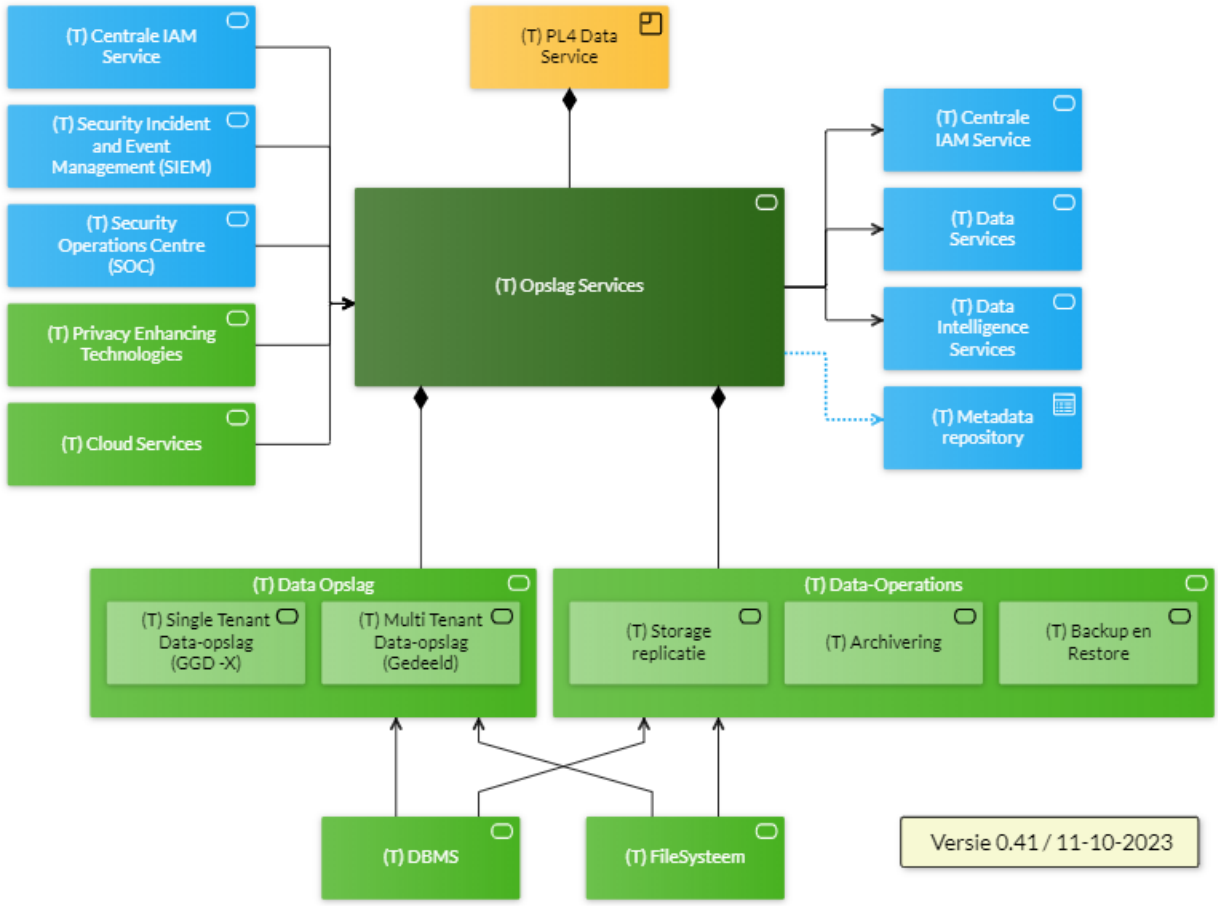
5.8.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Opslag Services
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (run-modus) dient dermate te zijn dat genoemde cijfers ondersteund worden.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,9%. Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA-afspraken, het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers. Dit geldt zowel voor de ontwikkel- als de run-modus componenten.

1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	Alle componenten zijn volledig en snel schaalbaar.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Alle componenten zijn volledig en snel schaalbaar.

5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (welke gehost wordt op cloud services) dient dermate te zijn dat genoemde cijfers ondersteund worden.
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)securityprocessen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Er wordt rekening gehouden met de genoemde schaalbaarheid.

5.8.3 Inrichting



5.8.4 Onderdelen van de Opslag Services

De *Opslag Services* bestaan uit de volgende onderdelen:

Data Opslag

De component Data Opslag omvat de (cloud-)technologieën voor het – fysiek – opslaan van data. Deze gegevensopslag wordt aangeboden ten behoeve van de generieke voorzieningen, dat wil zeggen, voor meerdere GGD'en (Multi tenant data-opslag). Ook wordt gegevensopslag aangeboden als basisvoorziening aan afzonderlijke GGD'en GHOR-bureaus (Single Tenant data-opslag).

Voor de opslag van gegevens ondersteunen de *Opslag Services* verschillende typen Database Management Systemen (Poly-Glot persistence), zoals relationele DBMS-en, Graph DB's, en Document- en Column Stores, zowel *highly consistent* (ACID) als *highly available* (BASE). Daarnaast moeten ook andere vormen van opslag (BLOB, Flat Files) gebruikt kunnen worden.
De inrichting van database omgevingen, en dan met name de inrichting van beschikbaarheidsmaatregelen als clustering en mirroring, wordt in hoge mate bepaald door meta-informatie over de data, zoals BIV-classificaties, RTO- en RPO-eisen.

Data Operations

Data Operations zijn alle geautomatiseerde logistieke functies rondom data, zoals replicatie, back-up en archivering. Ook voor de inrichting van deze functies wordt gebruik gemaakt van meta-informatie rondom data, zoals die vanuit het domein model zijn vastgelegd. Voorbeelden van parameters voor de logistiek die gebaseerd zijn op metadata uit het domeinmodel zijn bewaartermijnen, back-up cycli en archiveringsacties vanuit (wettelijke) kaders zoals de archiefwet.
Het vertalen van metadata naar parameters voor de logistieke functies moet waar mogelijk geautomatiseerd gebeuren.

5.8.5 Koppelvlakken

Opslag Services maken gebruik van:

- Cloud Services
  De Data Opslag component maakt gebruik van cloud-storage. Dit kan zowel in de vorm zijn van IaaS (Disk-, Blob-storage etc.) als van PaaS/DBaaS (NoSQL, RDBMS etc.);
- Security Services & Privacy Enhancing Technologies
  Opslag van gegevens gebeurt altijd versleuteld. Afhankelijk van het type en de classificatie van de data (zoals vastgelegd in de meta-informatie van het domeinmodel) worden gegevens versleuteld op record- of bestands-niveau, bijvoorbeeld door middel van encryptie of tokenization. Deze technieken zijn onderdeel van het bouwblok Security Services & Privacy Enhancing Technologies;
- Security Services
  Alle activiteit op de Data opslag dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok Security Services;

Opslag Services worden gebruikt door:

- Data Services
  Het lezen en bewerken van gegevens wordt in het datacentrische landschap aangestuurd door de Data Services;
- *Data Intelligence Services* ten behoeve van het lezen en schrijven van afgeleide gegevens voor analyse (datawarehouse) of dataset-provisioning (bijvoorbeeld als CSV) maken gebruik van de Opslag Services. Dit betreft datasets die niet onder controle staan van de Data Services.

5.8.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die met betrekking tot het bouwblok zijn geformuleerd

ID	Architectuurbesluit	Rationale
PAB-4b.01	Primaire (OLTP) data van het platform wordt alleen via de API's van de Data Services benaderd.	(Fysieke) opslag is transparant om modulariteit ten behoeve van flexibiliteit te borgen.

5.9 Koppel Services (PL5)

5.9.1 Definitie

Doel van het bouwblok *Koppel Services* is het leveren van de toegangsweg naar interne en externe gegevens, zowel voor interne gebruikers, externe gebruikers, (keten)partners als systemen. De *Koppel services* vervullen ook de vertaalfunctie van en naar verschillende uitwisselingsprotocollen (SFTP, SOAP, REST, etc.) en (zorg-) informatiestandaarden (Zibs, FHIR, IPS, Nederlandse Labcode Set, CDA, SNOMED, LOINC, DICOM, IHE, etc.).

Ook het gecentraliseerd management van API's die binnen het landschap in de *span of control* van het platform leven is onderdeel van de *Koppel Services*. Uitzondering hierop zijn de API's tussen de lagen (bouwblokken: Multichannel Presentatie-, Applicatie- en Data Services) van gerealiseerde IZB-applicaties (zie par 5.13 - PL7c).

Hiermee is het bouwblok de technische invulling van de dienst *PL5 – Koppelvlak.*
De Koppel Services zorgen ervoor dat:

- Veilige en betrouwbare data-uitwisseling mogelijk is met GGD'en, GHOR-bureaus, leveranciers en ketenpartners;
- Verschillende transport- en informatieprotocollen worden ondersteund. Koppelvlakken worden bij voorkeur geïmplementeerd op basis van API's en message-services. Omdat niet alle ketenpartners al kunnen koppelen met deze moderne koppelvlakken moet de oplossing ook de mogelijkheid bieden om via 'traditionele' kanalen - zoals SFTP - gegevens op een veilige en gecontroleerde manier uit te wisselen;
- De hoeveelheid koppelingen met systemen van derden (voor de regio's) minimaal is;
- Gebruik gemaakt wordt van gangbare of overeengekomen en vastgestelde uitwisselingsstandaarden.

5.9.2 Eisen vanuit LFI

In onderstaande tabellen zijn de eisen vanuit de LFI weergegeven die specifiek van toepassing zijn op het bouwblok *Koppel Services.*

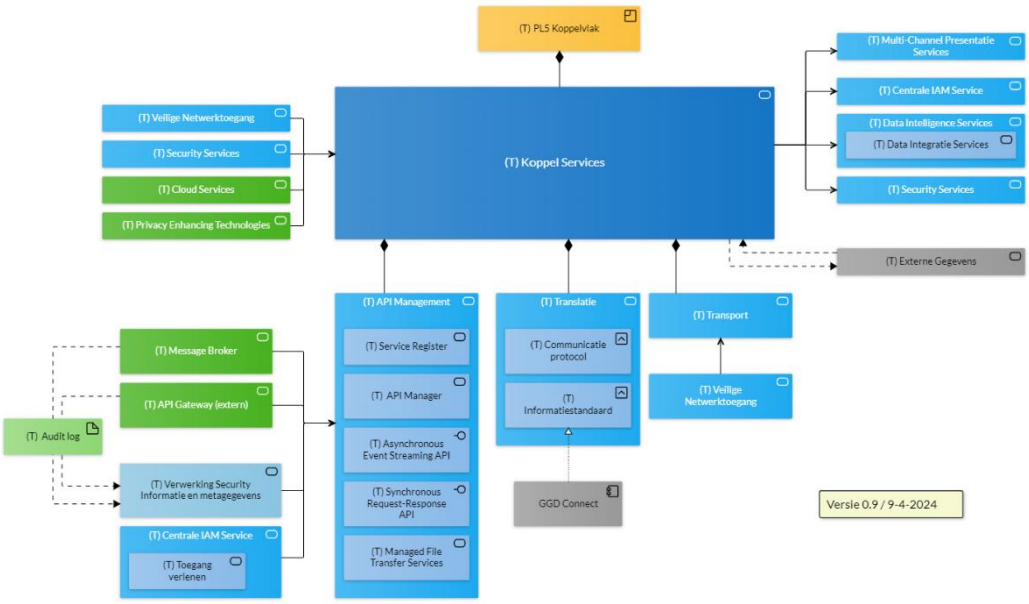
Bron: LFI BRQ				Implicatie Koppel Services
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (run-modus) dient dermate te zijn dat genoemde cijfers ondersteund worden.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,9%. Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA-afspraken, het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.

1.1.4.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om vastgestelde beleidswijzigingen en/of vastgestelde wijzigingen in LCI-richtlijnen die leiden tot wijzigingen in bestaande werkinstructies/werkprocessen, middels aangepaste configuratie binnen 24 uur uniform door te voeren bij alle uitvoerders.	Aanpassingen binnen het domeinmodel dienen binnen 24 uur over de gehele stack (o.a. API-register bijwerken) actief te zijn.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers.
1.1.6.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	Inrichten van paradoxale Koppel Services, standaardiseren waar mogelijk, maar voorbereid zijn om alle mogelijke koppelingen te realiseren. Dit zijn voorwaarden om snel te kunnen implementeren.
1.1.7.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het opschalen en doorvoeren van wijzigingen ten behoeve van de landelijke bestrijding van een A-infectieziekten vormt geen belemmering in de ondersteuning van de bestrijding van overige infectieziekten waarvan de bestrijding door het IV/ICT-landschap wordt ondersteund.	Voor Koppel Services is de mogelijkheid tot schaling van belang, bijvoorbeeld met betrekking tot API's, API-gateway en -management, dus ook hier moet rekening gehouden worden met de genoemde cijfers.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security.

				Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.3	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Organisatie en beheer- en ontwikkelprocessen maken het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	Paradoxale voorbereiding, dus veel verschillende Koppel Services voorbereiden.
3.1.2.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	Het IV/ICT-landschap ondersteunt de medisch-operationele processen zodanig dat het mogelijk is om, afhankelijk van de aard en ernst van de pandemie, bepaalde processtappen door burgers uit te laten voeren (bijvoorbeeld door een modulaire opzet).	PGO-systeemkoppeling met data API's.
4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	Alle componenten zijn volledig en snel schaalbaar.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Alle componenten zijn volledig en snel schaalbaar.
4.1.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap ondersteunt een geïntegreerde klantreis voor burgers, inclusief het principe eenmalige registratie, meervoudig gebruik (de verschillende uitvoerders in de keten hebben dus toegang tot dezelfde informatie). Gebruik van digitale middelen door burgers wordt gefaciliteerd op gangbare web- en mobiele technologieën.	Brondata moet ontsloten kunnen worden via Koppel Services.
4.2.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	De regie- en beheerorganisatie van uitvoerders zijn voorbereid op het leveren van functionele support aan eindgebruikers tijdens warme fase. *[met warme fase wordt pandemische situatie bedoeld]*	Functioneel support dient ingericht te worden.
5.1.1.	Gegevensregistratie en	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de	Inrichting (schaalbaarheid) van de services (welke

	gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.		ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	gehost wordt op Cloud Services) dient dermate te zijn dat genoemde cijfers ondersteund worden.
5.1.2.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat in het kader van de Wpg en de Wet op het RIVM verplichte meldingen "onverwijld" aan het RIVM ter beschikking gesteld worden door digitale en geautomatiseerde informatie-uitwisseling en/of door verlening van toegang tot data.	Door een gemeenschappelijk domeinmodel van de LFI, het RIVM en de GGD'en kan informatie eenvoudig en eenduidig gedeeld worden. Technische voorzieningen voor de aanlevering van data en/of overzicht zijn onderdeel van het platform. Ook is er beschikking over juiste data-API's.
5.1.3.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat voor sturing op medische-operationele processen benodigde stuur- en managementinformatie beschikbaar is voor de LFI.	Door een gemeenschappelijk domeinmodel van de LFI, het RIVM en de GGD'en kan informatie eenvoudig en eenduidig gedeeld worden. Technische voorzieningen voor de aanlevering van data en/of overzicht zijn onderdeel van het platform. Ook is er beschikking over juiste data-API's.
5.1.5.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevensuitwisseling is gebaseerd op gangbare informatiestandaarden zoals HL7.	De vertaling van en naar standaarden, zoals HL7 ten behoeve van gegevensuitwisseling, gebeurt in de Koppel Services. Gegevens zijn via API's te versturen/benaderen.
5.1.7.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevenskwaliteit wordt continue en geautomatiseerd bewaakt. En er wordt proactief op gerapporteerd. Applicaties waarin bronregistraties worden ingevoerd voorkomen actief registratiefouten, signaleren actief registratiefouten en bieden sturingsinformatie op datakwaliteit.	Op het platform zullen de applicaties de data middels data-API's benaderen.
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)securityprocessen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Er dient rekening gehouden te worden met de genoemde schaalbaarheid.

5.9.3 Inrichting



Uitgangspunten voor de implementatie van het bouwblok *Koppel Services* zijn:

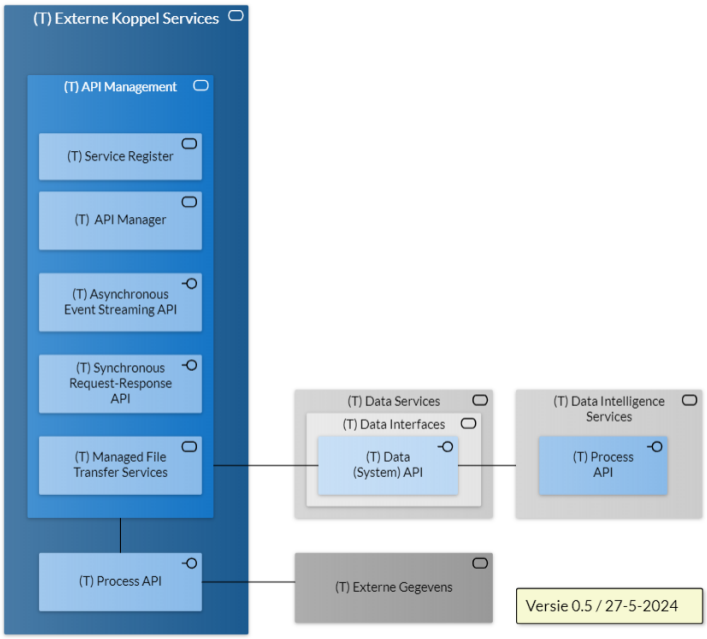
1. Koppelingen worden bij voorkeur gerealiseerd met behulp van API's en micro-services ten behoeve van horizontale schaalbaarheid;
2. Er moet snelle adaptie kunnen zijn van nieuwe of vernieuwde communicatie- en/of informatiestandaarden en -protocollen (flexibiliteit en aanpasbaarheid);
3. Veilige voorzieningen voor 'traditionele' vormen van gegevensuitwisseling (niet alle ketenpartners kunnen al koppelen met moderne koppelvlakken);
4. Beheersbaarheid en governance op gegevensuitwisseling (auditeerbaar en traceerbaar);
5. De componenten van de *Koppel Services* worden op verschillende plaatsen en manieren ingezet:
6. Horizontaal (intern): koppelingen tussen componenten binnen het bouwblok (modulair);
7. Horizontaal (extern): koppelingen ten behoeve van data-provisioning;
8. Gebruik van API's moet uitgaan van de API-strategie van Nictiz (REF: ER012 API-strategie voor de zorg);
9. De Koppel Services voorzien in koppelingen met regionale- en landelijke community-netwerken, zoals LSP en AmZX.

5.9.4 Onderdelen van de Koppel Services

API Management

De *Koppel Services* verzorgen het beheer en de beveiliging (API Management) van de Application Programming Interfaces (API) die in het landschap zijn geïmplementeerd en die binnen de *span of control* van het platform vallen. Dit geldt zowel voor synchrone als asynchrone gegevensoverdracht.

Ook verzorgt het bouwblok de adresseerbaarheid van deze API's door middel van een Service Register.



In bovenstaande figuur zijn de bouwblokken aangegeven waarin communicatie via API's gebeurt. De verschillende API's zijn ingedeeld volgens de typologie zoals die gehanteerd wordt door Nictiz:

- System API's
  Data/System API's zijn de koppelvlakken die de directe toegang van en naar gegevens in de data services en data opslag verzorgen. Deze API's zijn onderdeel van de *Data Services*;
- Process API's
  Met process API's kunnen data worden gecombineerd en kan de samenvoeging van meerdere data API's georkestreerd worden ten behoeve van specifieke informatiebehoeften. Process API's zijn onderdeel van *Applicatie Services*, *Data Intelligence Services* en *Koppel Services*.
- De process API's zorgen zowel voor de gegevenstoegang tussen de verschillende bouwblokken (verticaal) als tussen de elementen zoals microservices onderling binnen een bouwblok (horizontaal). Ook de toegang van en naar de gegevens in externe bronnen (via de *Koppel Services*) wordt via process-API's ingeregeld;
- Experience/Convenience API's
  De experience API's leveren data in de combinaties die nodig zijn voor verschillende kanalen, zoals mobiele apps, webformulieren en dergelijke. Deze API's worden gebruikt door de *Multi-Channel Presentatie Services*.

Translatie

De translatie component van de *Koppel Services* zorgt voor alle vertalingen en mappings van en naar gegevensuitwisselings-standaarden en -protocollen. Dit geldt zowel voor informatie- als communicatiestandaarden en -protocollen.

In het bijzonder zal de – atomaire - informatie van de data (system) API's van de *Data Services* vertaald worden van en naar de technische- en informationele structuren voor gegevensuitwisseling met derden.

Transport

De Transport-functies van de *Koppel Services* zijn belast met alle aspecten van het transport van gegevens tussen verschillende omgevingen. Dit kan zowel het transport zijn tussen de verschillende bouwblokken van

het platform (bijvoorbeeld wanneer deze zich bij verschillende leveranciers en/of op verschillende locaties bevinden), als het transport tussen het platform en andere omgevingen bij GGD'en, GHOR-bureaus, ketenpartners of anderen.

Transport is nauw gerelateerd aan het *bouwblok PL8b Veilige Netwerktoegang*. *Transport* is de placeholder voor alle zaken met betrekking tot performance (bandbreedtes, throttling, Quality of Service etc.) en beveiliging (zoals encryptie) van gegevensuitwisselingen zowel in reguliere als pandemische situaties (schaalbaarheid).

5.9.5 Koppelvlakken

Koppel Services maken gebruik van:

- Data Services: Koppel Services leveren voor alle gegevensmanipulaties (inclusief leesopdrachten ten behoeve van externe partijen) de audit-gegevens aan de *Data Services* (data-verwerking) ten behoeve van doelbinding. Hiervandaan worden de audit-gegevens doorgegeven aan de SOC/SIEM oplossing (PL3.2);
- Veilige Netwerktoegang voor het beveiligd en gecontroleerd transport van data;
- Security Services: alle activiteit op de Multi-Channel Presentatie Services dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok Security Services;
- Cloud Services (indien PaaS of IaaS) - container technologie;
- Privacy Enhancing Technologies (PET) om privacygevoelige gegevens te beschermen.
-

Koppel Services worden gebruikt door:

- Veilige Applicatie- en Datatoegang;
- Centrale IAM Services;
- Data Intelligence Services;
- Security Incident and Event Management (SIEM);
- Externe bronnen.

5.9.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die met betrekking tot het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-5.01	Koppelingen worden bij voorkeur gerealiseerd met behulp van API's en micro-services.	Ten behoeve van (horizontale) schaalbaarheid en omdat dit de standaard en bewezen technologie is.
PAB-5.02	De *Koppel Services* verzorgen het API Management van alle API's die in het landschap zijn geïmplementeerd, met uitzondering van de API's voor het decoupled IZB Applicatie stack	Centraal beheer en governance bevorderen eenduidigheid en verminderen daarmee de kans op fouten.
PAB-5.03	De *Koppel Services* verzorgen ook veilige voorzieningen voor 'traditionele' vormen van gegevensuitwisseling.	Niet alle ketenpartners kunnen al koppelen met moderne koppelvlakken zoals Rest-API's.
PAB-5.04	Gebruik van API's moet uitgaan van de API-strategie van Nictiz (REF: ER012 API-strategie voor de zorg).	Standaardisatie en interoperabiliteit.
PAB-5.05	API Management moet cloud-agnostisch geleverd worden	Standaardisatie en portabiliteit

5.10 Data Intelligence Services (PL6)

5.10.1 Definitie

Doel van het bouwblok *Data Intelligence Services* is het leveren van een omgeving voor analytische gegevensbewerking (OLAP) met data uit diverse (legacy) bronnen.
Hiermee is het bouwblok de technische invulling van de dienst *PL6 – Data Intelligence Platform.*

5.10.2 Eisen vanuit LFI

In onderstaande tabel zijn de eisen vanuit de LFI weergegeven die specifiek van toepassing zijn op het bouwblok *Data Intelligence Services.*

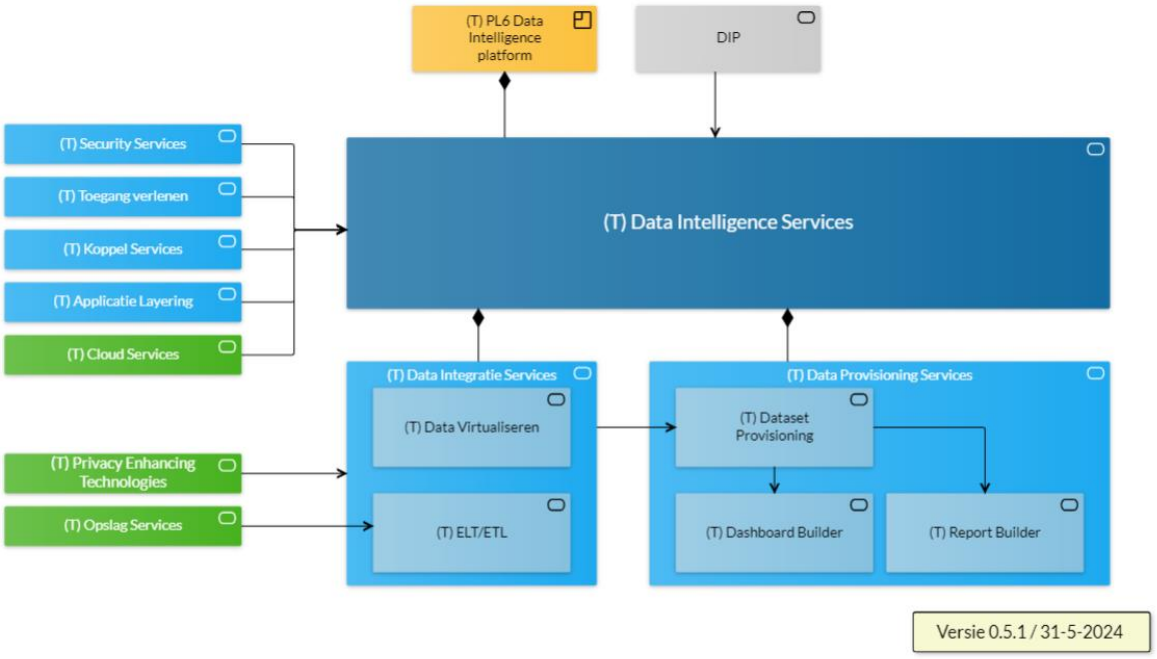
Bron: LFI BRQ				Implicatie *Data Intelligence Services*
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (welke gehost wordt op cloud services) dient dermate te zijn dat genoemde cijfers ondersteund worden. Deze genoemde aantallen lijken zich niet te richten op Data Intelligence Services, waarbij uiteindelijk analytische datasets en dashboards benaderd worden. Schaalbaarheid moet mogelijk zijn, maar in welke mate dient nader gespecificeerd te worden door het LFI. Schaalbaarheid van de services is met name van belang om een toename van gegenereerde data uit de medisch-operationele processen (bv. meer afspraken, meer vaccinaties, meer testuitslagen) als gevolg van een toename van het aantal gebruikers en van het gebruik op zich, te kunnen verwerken. Afspraken hierover worden opgenomen in de SLA's.
1.1.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap voorziet in het snel – bijvoorbeeld binnen enkele dagen – (landelijk) opschalen van professionals voor de uitvoering van medisch-operationele processen door hen te voorzien van een digitale identiteit, die inzetbaar is bij alle uitvoerders, met inachtneming van privacy aspecten	De services zijn beschikbaar voor geautoriseerde professionals via de digitale identiteit en moeten dus mee kunnen gaan in deze opschaling. Afspraken hierover worden opgenomen in de SLA's.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een	Middels SLA afspraken en het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden. In nadere uitwerking dient het LFI aan te geven in hoeverre alle componenten van het platform moeten voldoen aan deze beschikbaarheidscijfers.

			maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	
1.1.4	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om vastgestelde beleidswijzigingen en/of vastgestelde wijzigingen in LCI-richtlijnen die leiden tot wijzigingen in bestaande werkinstructies/werkprocessen, middels aangepaste configuratie binnen 24 uur uniform door te voeren bij alle uitvoerders.	Dit geldt ook voor de services wanneer de wijzigingen impact hebben op de gegenereerde data en op de gerelateerde dataleveringen en informatieproducten vanuit de services. Afspraken hierover worden opgenomen in de SLA's.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers.
1.1.6	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	Dit geldt ook voor de services wanneer de wijzigingen of vernieuwingen impact hebben op de gegenereerde data en op de gerelateerde dataleveringen en informatieproducten vanuit de services, of als er nieuwe dataleveringen en/of informatieproducten nodig zijn. Afspraken hierover worden opgenomen in de SLA's.
1.1.7	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het opschalen en doorvoeren van wijzigingen ten behoeve van de landelijke bestrijding van een A-infectieziekten vormt geen belemmering in de ondersteuning van de bestrijding van overige infectieziekten waarvan de bestrijding door het IV/ICT-landschap wordt ondersteund.	Dit geldt ook de dataleveringen en informatieproducten voor de verschillende infectieziekten (en voor overige taken van de GGD'en) vanuit de services. Afspraken hierover worden opgenomen in de SLA's.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het GGD GHOR Nederland IV-beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.

1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het GGD GHOR Nederland IV-beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
2.1.4.	Processen voor de landelijke bestrijding van A-infectieziekten zijn uniform.	Techniek	Het IV/ICT-landschap voorziet in het faciliteren, afhandelen en vastleggen van digitale contacten (online en telefonisch) met burgers door (landelijke) klantcontactcentra. Geregistreerde contacten met burgers zijn voor analysedoeleinden raadpleegbaar.	Geregistreerde contacten met burgers zijn voor analysedoeleinden raadpleegbaar en worden dus ontsloten t.b.v. de services. Zoals voor alle data die gedeeld wordt, dient privacy gewaarborgd te zijn. Indien geen rechten op persoonsgegevens worden de gegevens geanonimiseerd / gepseudonimiseerd.
4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	Alle componenten volledig en snel schaalbaar.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Alle componenten volledig en snel schaalbaar.
4.1.6.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorkomt een te grote afhankelijkheid van een of meerdere leveranciers (vendor lock-in). Applicaties moeten door nieuwe leveranciers overgenomen kunnen worden op basis van een vooraf overeengekomen Escrow overeenkomst.	Dit geldt ook voor de applicaties gerelateerd aan de services.
5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag	Afspraken hierover worden opgenomen in de SLA's.

			persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	
5.1.2.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat in het kader van de Wpg en de Wet op het RIVM verplichte meldingen "onverwijld" aan het RIVM ter beschikking gesteld worden door digitale en geautomatiseerde informatie-uitwisseling en/of door verlening van toegang tot data.	De services ondersteunen de benodigde uitwisseling van data en informatie met het RIVM.
5.1.3.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat voor sturing op medische-operationele processen benodigde stuur- en managementinformatie beschikbaar is voor de LFI.	Technische voorzieningen voor aanlevering data en/of overzicht zijn onderdeel van het platform. Hier wordt dus uitgegaan dat het platform deze informatie oplevert aan het LFI. De technische voorziening dient dermate generiek te zijn dat ook andere informatie (zodra aanwezig), zoals wetenschappelijke informatie, kan worden verstrekt.
5.1.4.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk om de te verzamelen meldingsinformatie binnen 24 uur landelijk aan te passen.	Deze aanpassingen worden ook doorgevoerd in de ontsluiting van de data zodat deze ook binnen de 24 uur beschikbaar komen voor de services.
5.1.5.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevensuitwisseling is gebaseerd op gangbare informatiestandaarden zoals HL7.	De services volgen hier ook de relevante specificaties uit de domeinarchitectuur en het domeinmodel PP IV.
5.1.7.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevenskwaliteit wordt continue en geautomatiseerd bewaakt. En er wordt proactief op gerapporteerd. Applicaties waarin bronregistraties worden ingevoerd voorkomen actief registratiefouten, signaleren actief registratiefouten en bieden sturingsinformatie op datakwaliteit.	De services bieden de mogelijkheid om de datakwaliteit in de keten te monitoren en te analyseren, en erop te rapporteren t.b.v. landelijk data management/governance. Dit betreft zowel de kwaliteit van de registratie als de kwaliteit van de (geautomatiseerde) verwerking en levering van de data.
6.1.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat door uitvoerders en/of LFI gecontracteerde partijen personeel toegang kunnen verschaffen tot IV-IZB op basis van door gecontracteerde partijen gegenereerde digitale identiteiten.	De services dienen aangesloten te zijn op en gebruik te maken van de centrale IAM Services, inclusief inrichting van rollen en rechten.

5.10.3 Inrichting



5.10.4 Onderdelen van de Data Intelligence Services

Data Integratie Services

Data Integratie Services zorgen ervoor dat uit verschillende bronnen (de *Data Services*, maar ook andere (externe) bronnen) gegevens worden gecombineerd en daar een resultaat van wordt gemaakt. Dit kan gerealiseerd worden door:

- Data Virtualisatie
- ELT/ETL (Extract, Load en Transform)

De bronnen worden benaderd via *Applicatie Layering* (Data Services) en de *Koppel Services* (externe bronnen).

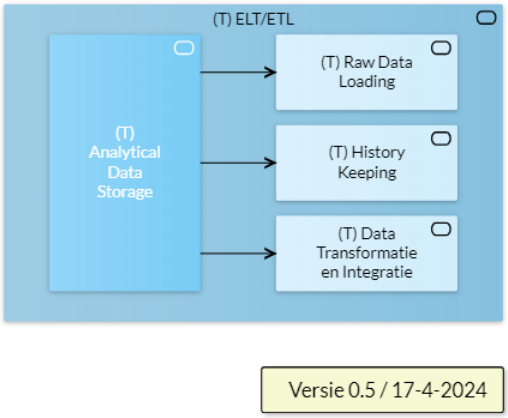
Data Virtualiseren

Datavirtualisatie, of gegevens-virtualisatie, is het virtueel samenbrengen van gegevens vanuit meerdere databronnen, zodat het voor de gebruiker van de data lijkt alsof er maar één databron wordt aangesproken. De virtualisatie van de data is een proces waarbij de onderliggende informatiebronnen via webservices, XML en andere methoden worden gekoppeld en er dus geen gegevens worden gekopieerd.

Ten behoeve van performance zal voor datavirtualisatie mogelijk caching (in zowel opslag als geheugen) plaatsvinden. Deze opslag heeft niets te maken met de eerdergenoemde *Opslag Services*, maar kan daarvan wel dezelfde onderliggende infrastructuur gebruiken.

ELT/ETL

ELT staat voor Extract, Load en Transform. De letters in ETL hebben dezelfde betekenis, alleen is er dan een andere volgorde van toepassing.



Deze functionaliteit levert de mogelijkheid voor het extraheren van data uit een bron, het laden in de eigen omgeving (*Raw Data Loading*) en het transformeren en integreren ervan tot een formaat waarmee je kunt werken (*Data Transformatie en Integratie*). Daarbij dienen alle veranderingen te worden bijgehouden ten behoeve van historische overzichten om bijvoorbeeld trendanalyses te kunnen doen (*History Keeping*).

Raw Data Loading, History Keeping en Data Transformatie en Integratie gebruiken als opslag *Analytical Data Storage*, welke gebruik maakt van dezelfde technieken die benoemd zijn in *Opslag Services* (welke een onderdeel is van *PL4 Data Service)*.

Bij ELT/ETL wordt data dus gekopieerd uit één of meerdere bronnen. Dit moet zoveel mogelijk voorkomen worden, zie de NORA implicatie 'Verwijs naar de bron. Dit kan in sommige gevallen echter nodig zijn, zoals bij pseudonimiseren of in verband met performance redenen. De voorkeur heeft dan ook data virtualisatie.

Data Provisioning Services

Data wordt beschikbaar gesteld via datasets en dashboards, daarom dienen in ieder geval de volgende services gerealiseerd te worden:

- Dataset Provisioning
- Dashboard Builder
- Report Builder

Het platform moet daarbij generiek zijn, zodat ook kan worden voorzien in andere informatiebehoeftes, die bijvoorbeeld gerealiseerd moeten worden door data science en process mining.

Dataset Provisioning

De (onderzoeks-)dataproducten die door de *Data Intelligence Services* als dataset worden geleverd (provisioning) zijn veelal resultaten van de *Data Integratie Services*. Met Dataset Provisioning wordt hier bedoeld dat het product ook daadwerkelijk beschikbaar wordt gesteld. De ontsluiting van een dataset geschiedt via de *Koppel Services*. Deze ontsluiting gebeurt bij voorkeur door het gebruik van API's.

Dashboard Builder

Gezondheidsdata wordt onder andere door GGD-professionals gebruikt voor gezondheidsadvisering en beleidsadvisering naar gemeenten. Dit is onderdeel van één van hun wettelijke taken. De datarapportage vindt vaak plaats in dashboards. Voor de GGD'en is toegang tot data noodzakelijk om inzicht in de (regionale/lokale) gezondheidssituatie te krijgen zodat zij rapportages en advisering naar gemeentes kunnen uitvoeren. Een dashboard, schaalbaar naar de regionale situatie, is daarbij helpend. De basis van het dashboard is daarbij 25x hetzelfde, dus één (1) inrichting is kostenbesparend.
Gegevens (sturings-, management- en medisch-wetenschappelijke gegevens) omtrent medisch-operationele processen moeten beschikbaar gesteld worden aan onder meer het RIVM, de LFI, de IZB-professionals en de afdelingen Epidemiologie van de 25 GGD'en en GGD GHOR Nederland. Deze gegevens moeten verrijkt worden met fixed varabelen en data vanuit selfservice, om hen in staat te stellen hun adviesfunctie binnen een breder, regionaal relevant gezondheidsperspectief te plaatsen.

Een data dashboard is de visualisatie vanuit *Data Integratie Services* (ontsloten via de *Koppel Services*) die ervoor zorgt dat benodigde indicatoren visueel gevolgd, geanalyseerd en weergegeven worden. Dit betreft bijvoorbeeld KPI's om procesevaluaties uit te voeren, medische gestandaardiseerde data die voldoet aan informatiestandaarden (van bijvoorbeeld NICTIZ) en metrics en key data points. Nadat duiding is toegevoegd ontstaat inzicht in bedrijfsprocessen, de gezondheidssituatie van de bevolking en de performance van een afdeling of een specifiek proces. Deze duiding bevat altijd een lokale context.

Met de Dashboard Builder kunnen in eerste instantie centraal dashboards gemaakt worden die vaste gegevens bevatten (fixed). In de verdere ontwikkeling van de Data Intelligence Services wordt voorzien dat de Dashboard Builder ook de mogelijkheid biedt om dashboards (selfservice) aan te passen aan specifieke behoeften, mogelijk in een aparte Selfservice BI-omgeving voor geautoriseerde medewerkers van GGD GHOR Nederland, GGD'en en ketenpartners. De data kunnen worden weergegeven in de vorm van tabellen, lijndiagrammen, staafdiagrammen en metrics.

De mogelijkheid van selfservice is essentieel voor de bredere verwerking van gezondheidsdata en voor de uitvoer van wettelijke taken van de GGD'en en GGD GHOR Nederland.

Report Builder

Behalve in de vorm van dashboards, worden datasets in voorkomende gevallen ook gepresenteerd in de vorm van online of geprinte rapporten. Hiervoor dient het onderdeel Report Builder.

5.10.5 Koppelvlakken

Data Intelligence Services maken gebruik van

1. Security Services: *Data Intelligence Services* leveren voor alle raadplegingen op de producten van de *Data Intelligence Services* de audit-loggegevens aan de *Security Services*. Systeemlogging van het onderliggende besturingssysteem (event log / system log) wordt aangeboden aan het logsysteem ten behoeve van logarchivering;
2. Access Control: voor de producten die met *Data Provisioning Services* worden aangeboden wordt de toegang geregeld vanuit Access Control;
3. Koppel Services: *Data Integratie Services* benadert (of kopieert indien nodig) de externe bronnen via de *Koppel Services*. Datasets worden door *Data Provisioning Services* met behulp van de *Koppel Services* ontsloten (bij voorkeur met API's, maar andere bestandsformaten zijn eveneens mogelijk). De Dashboard Builder maakt dashboards die de externe bron(nen) benadert via de *Koppel Services* en ontsluit het dashboard daarna via de *Koppel Services*;

4. Applicatie Layering: *Data Integratie Services* benadert (of kopieert indien nodig) de interne bronnen via de *Applicatie Layering*. De Dashboard Builder maakt dashboards die de interne bron(nen) benadert via de *Applicatie Layering*;
5. Cloud Services: hierop worden de *Data Intelligence Services* gerealiseerd, indien mogelijk als IaaS of PaaS;
6. Opslag Services: worden gebruikt indien data moet worden opgeslagen in een *Analytical Data Storage*;
7. Privacy Enhancing Technologies: worden gebruikt om gegevens waar nodig te pseudonimiseren, anonimiseren en te maskeren.

   Een Trusted Third Party (TTP) wordt voornamelijk ingezet voor het op persoonsniveau samenvoegen, koppelen of verrijken van gegevens van verschillende bronbestanden of verstrekkers, op zo'n manier dat afnemers alleen gepseudonimiseerde gegevens ontvangen. De *Data-TTP* is vanwege het *pseudonimiseren* gepositioneerd onder *Privacy Enhancing Technologies*. Indien GGD GHOR Nederland zelf een TTP wordt zal deze, ook vanwege de integratie in het conceptueel model, onder *Data Integratie Services* kunnen worden geplaatst.

5.10.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die met betrekking tot het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-6.01	Data virtualisatie heeft voorkeur boven ETL/ELT.	NORA implicatie 'Verwijs naar de bron'. Verwijzen naar de bron heeft voorkeur boven een kopie uit die bron.
PAB-6.02	Dataleveringen aan afnemers verlopen altijd via het DIP, dus niet direct vanuit de (interne) Data Services.	Op deze wijze is er een centraal punt in het landschap waarlangs data uit de applicaties naar "buiten" gaat en is het beheer van de dataleveringen minder complex.
PAB-6.03	Voor toegang voor eindgebruikers tot dataproducten, met name dashboards, rapporten en bestanden wordt gebruik gemaakt van de IAM Services.	Gecentraliseerd beheer van gebruikerstoegang.
PAB-6.04	Uitwisseling van data via API services heeft de voorkeur boven andere technieken.	Ten behoeve van schaalbaarheid en omdat dit de standaard is.

5.11 Multi-Channel Presentatie Services (PL7a)

5.11.1 Definitie

Het bouwblok *Multi-Channel Presentatie Services* voorziet in de technologie(en) die het mogelijk maakt om geautomatiseerde interactie met gebruikers via verschillende digitale kanalen te presenteren. Door de vormen van presentatie te scheiden van data en processen wordt de digitale communicatie met gebruikers eenduidiger en flexibeler.

5.11.2 Eisen vanuit LFI

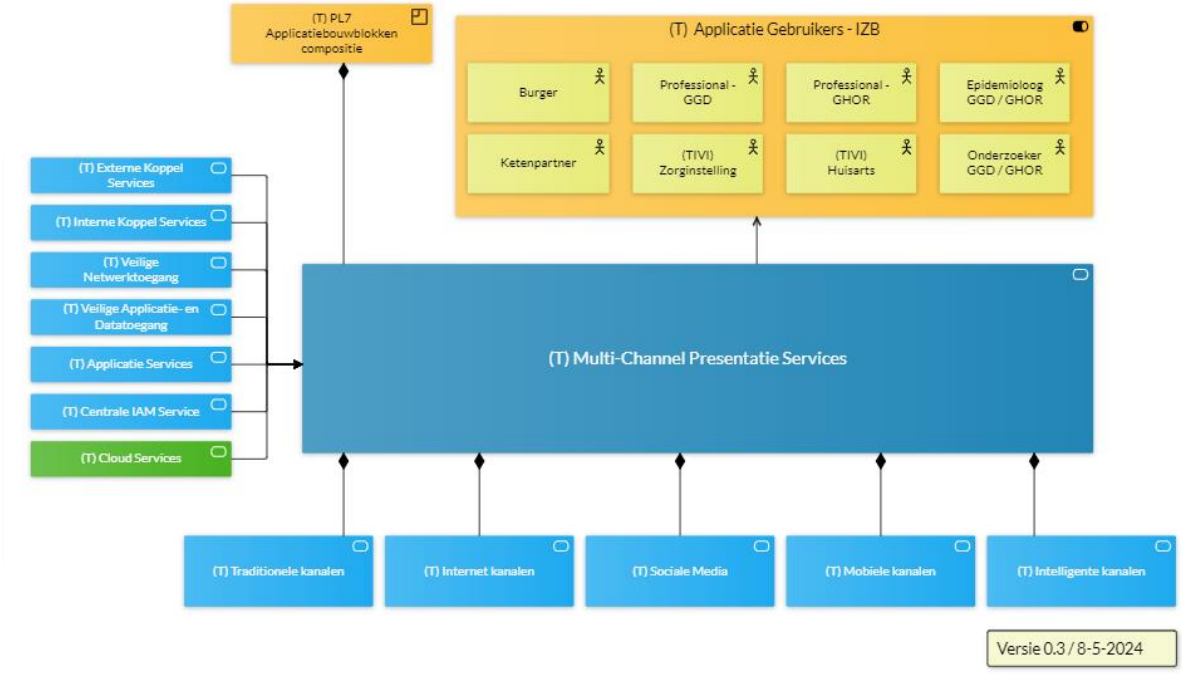
Bron: LFI BRQ				Implicatie *Multi-Channel Presentatie Services*
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000	Inrichting (schaalbaarheid) van de services (run-modus) dient dermate te zijn dat genoemde cijfers ondersteund worden, bijv. voor webservices.

			burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,9%. Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA-afspraken, het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers. Dit geldt zowel voor de ontwikkel- als de run-modus componenten.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	Het IV-beleid van GGD GHOR Nederland, wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2, is als uitgangspunt/kader opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving wordt tijdens de levensloop van de dienstverlening blijvend geanticipeerd op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Organisatie en beheer- en ontwikkelprocessen maken het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag-	Nieuwe processen worden aangeboden via de Applicatie Services en dienen dankzij de decoupled architectuur eenvoudig en snel door de Presentatie Services aangeboden te worden

			of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	aan de verschillende kanalen. In de SLA met (bestaande) leveranciers wordt hiertoe een inspanningsverplichting opgenomen.
2.1.1.	Processen voor de landelijke bestrijding van A-infectieziekten zijn uniform.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat professionals van uitvoerders (tijdens pandemieën, in de warme fase) door de LFI vastgestelde blauwdruk-inrichting(en) van processen en applicaties gebruiken. Deze blauwdrukken zijn te allen tijde eenvoudig, online te raadplegen voor betrokkenen.	Nieuwe processen worden aangeboden via de Applicatie Services en dienen dankzij de decoupled architectuur eenvoudig en snel door de Presentatie Services aangeboden te worden aan de verschillende kanalen. In de SLA met (bestaande) leveranciers wordt hiertoe een inspanningsverplichting opgenomen.
3.1.1.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	Het IV/ICT-landschap voldoet aan de WCAG2.1 richtlijn, niveau A en AA is leidend.	Applicatie UX-design dient te voldoen aan de laatste goedgekeurde versie van de WCAG2.1 richtlijn.
4.1.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap ondersteunt een geïntegreerde klantreis voor burgers, inclusief het principe eenmalige registratie, meervoudig gebruik (de verschillende uitvoerders in de keten hebben dus toegang tot dezelfde informatie). Gebruik van digitale middelen door burgers wordt gefaciliteerd op gangbare web- en mobiele technologieën.	UX-design (de input voor de ontwikkel-modus van Multi-Channel Presentatie Services) moet ingericht zijn op gebruik in hoge aantallen. Op run-modus bieden de services deze aan op de gangbare kanalen.
4.1.4.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Applicaties zijn eenvoudig in gebruik en snel – bijvoorbeeld binnen één dag – aan te leren; handleidingen (ook in-applicatie voor directe ondersteuning bij gebruik) en scholing zijn up-to-date en beschikbaar. Wijzigingen in bijvoorbeeld handleidingen en trainingen zijn tijdig (binnen 24 uur) centraal te distribueren.	Het wordt mogelijk om Applicaties en UX in een presentatie-/portalisatielaag via de Agile methode te (laten) ontwikkelen, waarbij representanten van gebruikersgroepen nauw betrokken zijn. Belangrijk is een uniforme look & feel in de presentatielaag.
4.1.5.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap faciliteert correcte en complete invoer in de bron (door burgers en door uitvoerders) en voorkomt foutieve invoer (of omissies) zoveel als mogelijk en proactief.	Generieke controle op invoerformaten (zoals datum en postcode) is hier (in de run-modus) mogelijk.
4.2.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	Implementatie van gewijzigde en door IV/ICT ondersteunde processen wordt ondersteund met landelijke instructie/training aan professionals en met digitale leeromgevingen.	Multi-Channel Presentatie Services kunnen ook aangesloten worden op andere content leverende systemen dan het datacentrische landschap, zoals een digitale leeromgeving.

5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (welke gehost wordt op cloud services) dient dermate te zijn dat genoemde cijfers ondersteund worden.

5.11.3 Inrichting



Uitgangspunten voor de implementatie van het bouwblok zijn:

1. Multi-Channel: De mogelijkheid interactieve inhoud te publiceren naar meerdere kanalen: website, mobiel, telefoon, mail e.d.;
2. Multi-Device: De mogelijkheid interactieve inhoud te publiceren naar meerdere typen apparaten: mobiel, tablet, computer e.d.;
3. Intuïtieve en eenvoudige *user interfaces*: de toegang tot de voorzieningen moet inclusief zijn, rekening met de verschillen in digitale mogelijkheden en vaardigheden van gebruikers (burgers en zorg-professionals).

Eisen die aan het bouwblok worden gesteld zijn onder meer:

- Goede applicatieve ondersteuning van de processen bij GGD en GHOR, betere toegankelijkheid en eenvormigheid van presentatie;

- Flexibel uit te breiden en aan te passen;
- Nieuwe en meerdere distributiekanalen;
- Korte Time To Market van nieuwe en aan te passen eisen en wensen.

Personae

Verschillende soorten eindgebruikers zullen gebruik maken van het platform.

1. M.n. IV-professionals als informatie-managers en functioneel beheerders zullen gebruik maken van het platform als motor (ontwikkel-modus) voor het (geautomatiseerd) realiseren van applicatieve voorzieningen vanuit een gegeven domeinmodel (data-centrische ontwikkeling). De toegang tot de omgeving voor deze gebruikers wordt verzorgd via de services van het bouwblok *Veilige Applicatie- en Datatoegang*;
2. Het platform als generieke infrastructuur voor het bedienen van toepassingen (run-modus) voor de ondersteuning van IZB- en andere processen zal gebruikt worden door burgers en professionals, zoals GGD zorg-professionals, professionals van GHOR, keten-partners, aangesloten zorginstellingen en huisartsen;
3. GGD, GHOR en GGD GHOR Nederland epidemiologen en onderzoekers zullen van het platform gebruik maken ten behoeve van hun onderzoekstaken.

De *Multi-Channel Presentatie Services* ondersteunen een Omni-Channel strategie, waarbij gebruikers en dan met name burgers via meerdere kanalen op een herkenbare, intuïtieve en uniforme manier worden benaderd. De inrichting en het beheer van de presentatie-aspecten, zoals stijl en interactie, moet over de verschillende kanalen eenvoudig en eenduidig zijn en via één interface te onderhouden zijn.

Kanalen

De *Multi-Channel Presentatie Services* leveren de IV-functionaliteit die nodig is om via verschillende kanalen met (eind-) gebruikers te kunnen communiceren. In de loop der tijd zijn deze IV-voorzieningen doorontwikkeld in de mate waarin ze bijdragen aan de interactie. Op dit moment moeten in ieder geval onderstaande kanalen worden ondersteund en de voorzieningen moeten adaptief zijn ingericht zodat toekomstige ontwikkelingen snel en eenvoudig zijn te implementeren:

- Traditionele kanalen, zoals SMS en het automatisch versturen en verwerken van briefpost;
- Internetkanalen. Dit zijn kanalen als websites, webformulieren, en e-mail;
- Sociale Media als Facebook, Twitter, WhatsApp e.d.;
- Mobiele kanalen. De inzet van Apps voor mobiele telefoons en tablets;

In een later stadium zullen ook Intelligente kanalen, zoals Chatbot, Virtual- en Augmented reality ondersteund moeten worden.

Datakwaliteit

De Multi-Channel Presentatie Services kunnen de gebruikers ondersteunen bij de correcte invoer van gegevens om zo de datakwaliteit te verbeteren. Deze invoercontroles dienen herleidbaar te zijn tot het domeinmodel. Dit om te voorkomen dat bij wijzigingen in het domeinmodel de bijbehorende controles in de userinterface worden vergeten.

5.11.4 Koppelvlakken

De *Multi-Channel Presentatie Services* maken gebruik van de volgende bouwblokken:

- Access Control (Centrale IAM Service) t.b.v. de toegangscontrole van applicaties. *Multi-Channel Presentatie Services* leveren de inlogschermen;

- Security Services: Alle activiteit op de *Multi-Channel Presentatie Services* dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok *Security Services*;
- Applicatie Services verzorgen de workflow en het ophalen en aanleveren van gegevens van en naar de data-services via de *Koppel Services*. De *Multi-Channel Presentatie Services* voorzien uitsluitend in het omzetten van deze informatie van en naar de juiste kanalen via Experience API's.
- Applicatie Layering t.b.v. interne Experience API's.
- Koppel Services t.b.v. externe Experience API's.

5.11.5 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die m.b.t. het bouwblok zijn geformuleerd

ID	Architectuurbesluit	Rationale
PAB-7a.01	Multi-Channel Presentatie Services voorzien uitsluitend in het omzetten van informatie tussen de verschillende kanalen en de applicatie services.	Door de *decoupled* architectuur worden presentatie (look & feel) en verwerking gescheiden en kunnen ze onafhankelijk van elkaar worden aangepast/vervangen.
PAB-7a.02	De inrichting en het beheer van de presentatieaspecten, zoals stijl en interactie, moet over de verschillende kanalen eenvoudig en eenduidig zijn en via één interface mogelijk zijn.	Op deze manier wordt eenvormigheid en eenduidigheid afgedwongen en het beheersgemak vergroot.
PAB-7a.03	De voorziening is inclusief.	Digitale inclusie gaat over meedoen op digitaal gebied voor iedere burger. Niet iedereen kan digitale diensten even makkelijk gebruiken. De overheid wil dit op verschillende manieren verbeteren. Het ontwerp houdt, daar waar mogelijk, rekening met deze groep van eindgebruikers.
PAB-7a.04	Channel Presentatie Services kunnen ook aangesloten worden op andere content leverende systemen dan het datacentrische landschap, zoals een digitale leer omgeving	Optimalisatie gebruik van de presentatie-voorzieningen

5.12 Applicatie Services (PL7b)

5.12.1 Definitie

Het bouwblok *Applicatie Services* voorziet in de technische functies voor het coderen van applicatie modules, het herbruikbaar maken daarvan via een code-bibliotheek, het combineren van de modules tot applicatieve toepassingen en de technologieën om deze applicaties via verschillende media (kanalen) aan te bieden aan gebruikers. Het bouwblok voorziet daarmee in de technische voorzieningen ten behoeve van de dienst *Applicatiebouwblokken compositie* (PL7).

5.12.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Applicatie Services
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken	Inrichting (schaalbaarheid) van de services (run-modus) dient dermate te zijn dat genoemde cijfers ondersteund worden.

			plannen (cijfers o.b.v. ervaringen in de coronacrisis).	
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA afspraken en het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden. Aangevuld met vastgestelde noodprocedures.
1.1.4.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om vastgestelde beleidswijzigingen en/of vastgestelde wijzigingen in LCI-richtlijnen die leiden tot wijzigingen in bestaande werkinstructies/werkprocessen, middels aangepaste configuratie binnen 24 uur uniform door te voeren bij alle uitvoerders.	Met configuratie wijzigingen worden hier met name veranderingen in selectievragen bedoeld. Deze content- en workflow-aanpassingen moeten snel, eenvoudig en uniform aangebracht kunnen worden. Aanpassingen binnen het domein model dienen binnen 24 uur over de gehele stack (t.b.v. workflow) actief te zijn. Hiervoor moeten werkprocessen worden ingericht.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers. Dit geldt zowel voor de ontwikkel- als de run-modus componenten.
1.1.6.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	Het modulair applicatielandschap voorzien van functionaliteiten die hergebruikt kunnen worden. Afspraken met bestaande leveranciers en nieuwe leveranciers (ontwikkelpartijen) inventariseren en up-to-date houden om snel te kiezen.

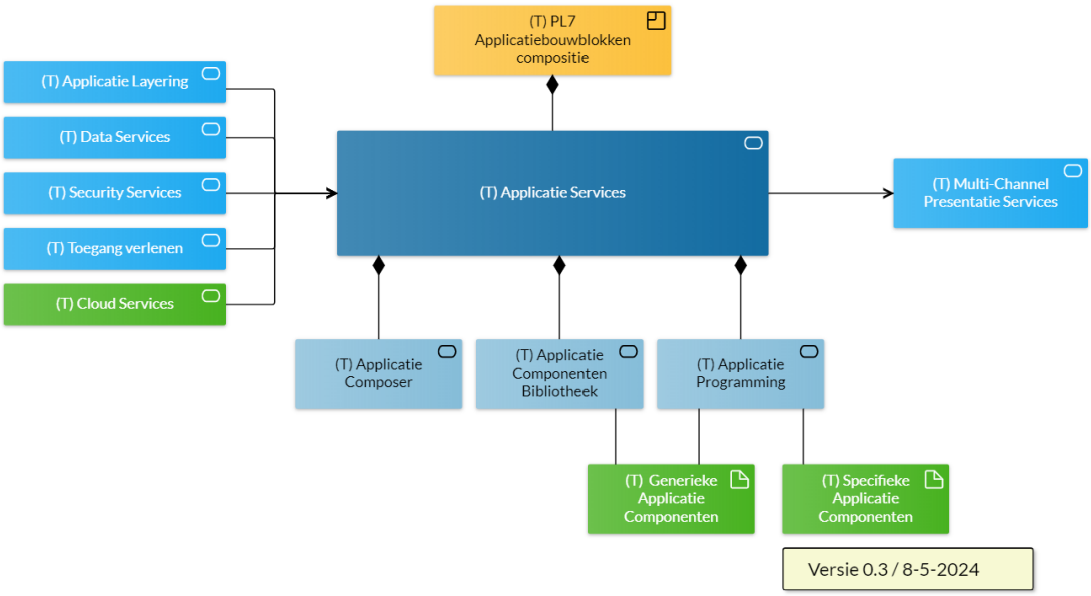
1.1.7.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het opschalen en doorvoeren van wijzigingen ten behoeve van de landelijke bestrijding van een A-infectieziekten vormt geen belemmering in de ondersteuning van de bestrijding van overige infectieziekten waarvan de bestrijding door het IV/ICT-landschap wordt ondersteund.	Behalve modulaire opbouw verticaal, ook segmentering tussen afzonderlijke IZB-composities. Het beste patroon t.b.v. multi-tenant cloud software aanbieden moet gekozen worden.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.

1.2.3	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Organisatie en beheer- en ontwikkelprocessen maken het mogelijk om in de context van het doorlopend en op korte termijn naar voren komen van (ver)nieuwe(nde) inzichten in de bestrijding van de infectieziekten, soms op dag- of weekbasis, functionaliteit van het IV/ICT-landschap snel – bijvoorbeeld binnen enkele weken – te wijzigingen en/of nieuwe oplossingen toe te voegen van zowel bestaande als nieuwe leveranciers.	Nieuwe processen worden aangeboden vanuit de Data Services en kunnen binnen de Applicatie Services dankzij de modulaire opbouw eenvoudig en snel worden samengevoegd in workflow en user-experience. Inspanningsverplichting hiertoe wordt opgenomen in de SLA met (bestaande) leveranciers.
2.1.1.	Processen voor de landelijke bestrijding van A-infectieziekten zijn uniform.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat professionals van uitvoerders (tijdens pandemieën, in de warme fase) door de LFI vastgestelde blauwdruk-inrichting(en) van processen en applicaties gebruiken. Deze blauwdrukken zijn te allen tijde eenvoudig, online te raadplegen voor betrokkenen.	Nieuwe processen worden aangeboden vanuit de Data Services en kunnen binnen de Applicatie Services dankzij de modulaire opbouw eenvoudig en snel worden samengevoegd in workflow en user-experience. Inspanningsverplichting hiertoe wordt opgenomen in de SLA met (bestaande) leveranciers.
3.1.1.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	Het IV/ICT-landschap voldoet aan de WCAG2.1 richtlijn, niveau A en AA is leidend.	Applicatie UX-design dient te voldoen aan laatste goedgekeurde versie van WCAG2.1 richtlijn.
3.1.2.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	Het IV/ICT-landschap ondersteunt de medisch-operationele processen zodanig dat het mogelijk is om, afhankelijk van de aard en ernst van de pandemie, bepaalde processtappen door burgers uit te laten voeren (bijvoorbeeld door een modulaire opzet).	Dankzij het modulaire applicatielandschap (en semantisch datamodel incl. procesafspraken) zijn ook nieuwe functionaliteiten snel te ontwikkelen.
4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	De UX en workflow zullen gebaseerd moeten zijn op (werk) processen. De modulaire en gelaagde opbouw zal dit flexibel faciliteren.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Betreft applicatie design.

4.1.4.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Applicaties zijn eenvoudig in gebruik en snel – bijvoorbeeld binnen één dag – aan te leren; handleidingen (ook in-applicatie voor directe ondersteuning bij gebruik) en scholing zijn up-to-date en beschikbaar. Wijzigingen in bijvoorbeeld handleidingen en trainingen zijn tijdig (binnen 24 uur) centraal te distribueren.	Er zal rekening gehouden worden in het applicatie UX-design, waarbij via DevOps/Agile inrichting de applicaties via pipelines snel van updates te voorzien zijn.
4.1.6.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorkomt een te grote afhankelijkheid van een of meerdere leveranciers (vendor lock-in). Applicaties moeten door nieuwe leveranciers overgenomen kunnen worden op basis van een vooraf overeengekomen Escrow overeenkomst.	Daarbij is het mogelijk dat applicaties de data benaderen middels data-API's. Het applicatielandschap wordt van functionaliteiten voorzien die hergebruikt kunnen worden.
4.2.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	Implementatie van gewijzigde en door IV/ICT ondersteunde processen wordt ondersteund met landelijke instructie/training aan professionals en met digitale leeromgevingen.	Digitale leeromgeving dient aangeboden te worden.
5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (welke gehost wordt op cloud services) dient dermate te zijn dat genoemde cijfers ondersteund worden.
5.1.3.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk dat voor sturing op medische-operationele processen benodigde stuur- en managementinformatie beschikbaar is voor de LFI.	Op het platform zullen de applicaties de data middels data-API's benaderen.
5.1.4.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap maakt het mogelijk om de te verzamelen meldingsinformatie binnen 24 uur landelijk aan te passen.	Het modulair applicatielandschap bezit functionaliteiten die hergebruikt kunnen worden en zijn nieuwe functionaliteiten snel te ontwikkelen.
5.1.5.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevensuitwisseling is gebaseerd op gangbare informatiestandaarden zoals HL7.	Op het platform zullen de applicaties de data middels data-API's benaderen.

5.1.7.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevenskwaliteit wordt continue en geautomatiseerd bewaakt. En er wordt proactief op gerapporteerd. Applicaties waarin bronregistraties worden ingevoerd voorkomen actief registratiefouten, signaleren actief registratiefouten en bieden sturingsinformatie op datakwaliteit.	Op het platform zullen de applicaties de data middels data-API's benaderen.
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)security processen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Rekening houdend met genoemde schaalbaarheid

5.12.3 Inrichting



In bovenstaande figuur is het bouwblok Applicatie Services weergegeven met zijn onderdelen en de bouwblokken die gebruik maken van of gebruikt worden door *Applicatie Services*.

De onderdelen van de Applicatie Services zijn:

- Applicatie Programming
- Applicatie Componenten bibliotheek
- Applicatie Composer

5.12.4 Onderdelen van de Applicatie Services

Applicatie Programming

Voor het ontwikkelen van applicatie-modules en bijbehorende API's voorziet het platform in programmeer faciliteiten. Deze faciliteiten worden gebruikt voor ontwikkeling en onderhoud van zowel generieke als specifieke applicatie-componenten;

Applicatie Componenten bibliotheek

Generieke applicatie-componenten (microservices) worden opgenomen in een componenten bibliotheek zodat ze hergebruikt kunnen worden voor de compositie van applicaties;

Applicatie Composer

Met de applicatie-compositie functie kunnen generieke (uit de bibliotheek) en specifieke applicatiemodules worden samengevoegd tot applicaties.

5.12.5 Koppelvlakken

1. Applicatie Services maken gebruik van de cloud inrichting, zowel ten behoeve van het ontwikkelplatform (indien niet ingericht als SaaS) als voor het werkelijk uitvoeren van applicaties;
2. De applicatiemodules (microservices) worden in run-modus als een container aangeboden aan de Cloud Services;
3. Applicatie Services leveren voor alle gegevensmanipulaties de audit-gegevens aan de Data Services (dataverwerking) t.b.v. doelbinding. Daarvandaan worden de audit gegevens doorgegeven aan de Security Services;
4. Applicatie logging wordt geïntegreerd met de systeem-logging van het onderliggende besturingssysteem (eventlog/systemlog) en als onderdeel daarvan aangeboden aan het logsysteem ten behoeve van log archivering;
5. Uitwisseling van data van, naar en tussen applicaties gebeurt via API's die worden aangeboden en beheerd via de Applicatie Layering;
6. Gebruik van applicatiemodules (microservices) in de compositie laag gebeurt via API's. Deze worden aangeboden via en beheerd in de Koppel Services.

5.12.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die m.b.t. het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-7b.01	Voor de implementatie van (generieke) applicatie componenten wordt gebruik gemaakt van micro-services.	Micro-services vergroten de schaalbaarheid, portabiliteit en herbruikbaarheid van applicatiefuncties.
PAB-7b.02	Communicatie tussen applicatie onderdelen gebeurt via API's.	Decoupled architectuur maakt vervanging van verschillende bouwblokken mogelijk met minimale impact voor overige bouwblokken.
PAB-7b.03	Presentatie (UX) voorzieningen worden niet door Applicatie Services, maar door Multi-Channel Presentatie bouwblok uitgevoerd.	Decoupled architectuur maakt vervanging van verschillende bouwblokken mogelijk met minimale impact voor overige bouwblokken.
PAB-7b.04	Aanmaken van Audit-log records gebeurt in de Data Services. Applicatie services leveren hier voor de metadata.	Het werkelijk verlenen of weigeren van toegang (acces control) op basis van (input-) regels gebeurt in Data Services.

5.13 Applicatie Layering (PL7c)

5.13.1 Definitie

Doel van het bouwblok *Applicatie Layering* is het faciliteren en managen van de communicatie tussen de verschillende lagen (bouwblokken) van de primaire IZB toepassingen op het platform: Multichannel Presentatie Services, Applicatie Services en Data Services.

Deze lagen zijn met elkaar geïntegreerd tot applicatie-functionaliteit in een *decoupled* architectuur; dat wil zeggen dat zij onderling op basis van API's (system/data API's, Process API's en Experience/Convenience API's) met elkaar communiceren.

Het gecentraliseerd management van deze API's is onderdeel van de *Applicatie Layering*.
Hiermee is het bouwblok samen met *Multi Channel Presentatie Services* en *Applicatie Services* de technische invulling van de dienst *PL7 – Applicatie Compositie*.

De voorziening zorgt dat:

- Veilige en betrouwbare toegang mogelijk is tussen de verschillende (*decoupled*) lagen van het platform;

5.13.2 Eisen vanuit LFI

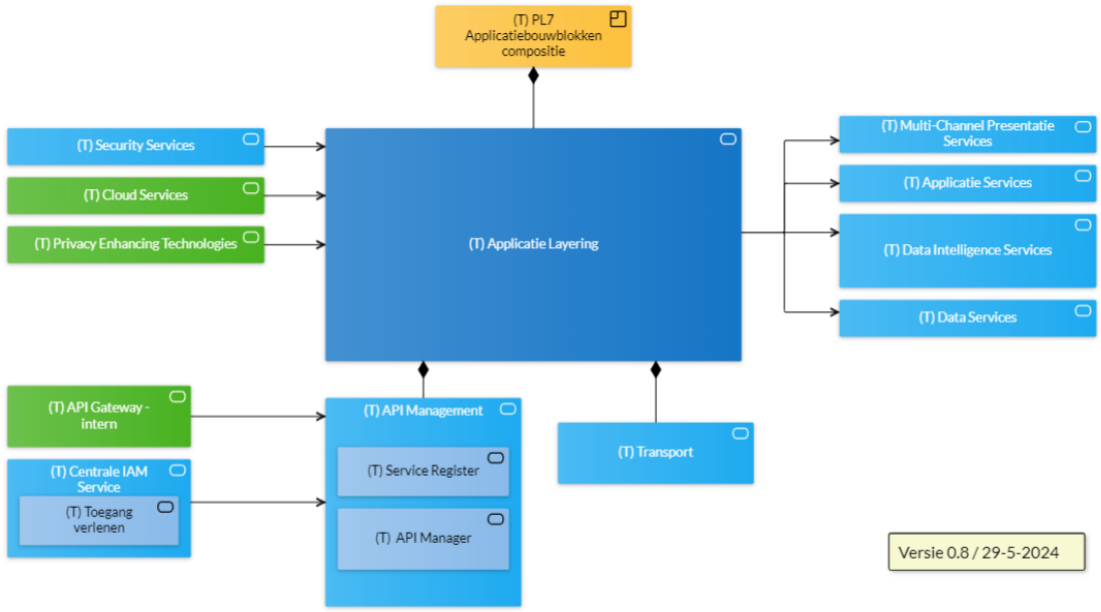
In onderstaande tabellen zijn de eisen vanuit LFI weergegeven die specifiek van toepassing zijn op het bouwblok *Applicatie Layering*.

Bron: LFI BRQ				Implicatie Applicatie Layering
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (run-modus) dient dermate te zijn dat genoemde cijfers ondersteund worden.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA afspraken en het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.
1.1.4.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk om vastgestelde beleidswijzigingen en/of vastgestelde wijzigingen in LCI-richtlijnen die leiden tot wijzigingen in bestaande werkinstructies/werkprocessen, middels aangepaste configuratie binnen 24 uur uniform door te voeren bij alle uitvoerders.	Aanpassingen binnen het domein model dienen binnen 24 uur over de gehele stack (o.a. API-register bijwerken) actief te zijn.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers.
1.1.7.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het opschalen en doorvoeren van wijzigingen ten behoeve van de landelijke bestrijding van een A-infectieziekten vormt geen belemmering in de ondersteuning van de bestrijding van overige infectieziekten waarvan de bestrijding door het IV/ICT-landschap wordt ondersteund.	Voor Applicatie Layering is de mogelijkheid tot schaling van belang, bijv. m.b.t. API's, API-gateway en -management, dus ook hier rekening houden met genoemde cijfers.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw

			zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
4.1.1.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	Alle componenten volledig en snel schaalbaar.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorziet in het efficiënt en effectief ondersteunen van gebruikers in medisch-operationele processen zodanig dat grote volumes aan handelingen verwerkt kunnen worden met een zo beperkt mogelijke inzet van personeel.	Alle componenten volledig en snel schaalbaar.
4.2.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	De regie- en beheerorganisatie van uitvoerders zijn voorbereidt op het leveren van functionele support aan eindgebruikers tijdens warme fase. *[met warme fase wordt pandemische situatie bedoeld]*	Functioneel support dient ingericht te worden.
5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) van de services (indien gehost wordt op Cloud Services) dient dermate te zijn dat genoemde cijfers ondersteund worden.

5.1.7.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Gegevenskwaliteit wordt continue en geautomatiseerd bewaakt. En er wordt proactief op gerapporteerd. Applicaties waarin bronregistraties worden ingevoerd voorkomen actief registratiefouten, signaleren actief registratiefouten en bieden sturingsinformatie op datakwaliteit.	Op het platform zullen de applicaties de data middels data-API's benaderen.
6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)security processen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Rekening houdend met genoemde schaalbaarheid.

5.13.3 Inrichting



Uitgangspunten voor de implementatie van het bouwblok *Applicatie Layering* zijn:

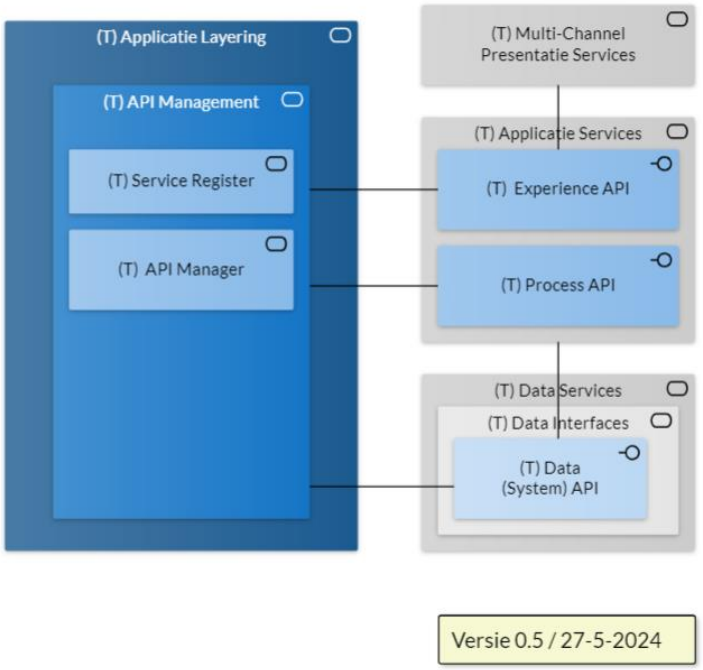
1. Koppelingen worden gerealiseerd m.b.v. van API's en micro-services t.b.v. horizontale schaalbaarheid;
2. Er moet snelle adaptie kunnen zijn van nieuwe of vernieuwde API's (flexibiliteit en aanpasbaarheid);
3. Beheersbaarheid en governance op gegevensuitwisseling (auditeerbaar en traceerbaar);
4. Gebruik van API's moet uitgaan van de API-strategie van de Nictiz (REF: ER012 API-strategie voor de zorg);

De componenten van de *Applicatie Layering* worden (verticaal) ingezet ten behoeve van koppelingen tussen verschillende IZB bouwblokken (*decoupled*).

5.13.4 Onderdelen van de Applicatie Layering

API Management

De *Applicatie Layering* faciliteit verzorgt het beheer en de beveiliging (API Management) van de Application Programming Interfaces (API) die in het AIZ landschap zijn geïmplementeerd. Ook verzorgt het bouwblok de adresseerbaarheid van deze API's d.m.v. een Service Register.



In bovenstaande figuur zijn de bouwblokken aangegeven waarin communicatie via API's gebeurt. De verschillende API's zijn ingedeeld volgens de typologie zoals die gehanteerd wordt door Nictiz:

- Data (System) API's
  Data (System) API's zijn de koppelvlakken die de directe toegang van en naar gegevens in de data services en data opslag verzorgen. Deze API's zijn onderdeel van de *Data Services;*
- Process API's
  Met process API's kunnen data worden gecombineerd en de samenwerking van meerdere data API's georkestreerd ten behoeve van specifieke informatiebehoeften. Proces API's zijn onderdeel van *Applicatie Services* en *Data Intelligence Services.*
- De process API's zorgen zowel voor de gegevens-toegang tussen de verschillende bouwblokken (verticaal) als tussen de elementen zoals microservices onderling binnen een bouwblok (horizontaal).
- Experience/Convenience API's
  De experience API's leveren data in de combinaties die nodig zijn voor de verschillende kanalen, zoals mobiele apps, webformulieren e.d. Deze API's worden gebruikt door de *Multi-Channel Presentatie Services*.

Transport

De *Transport*-functies van het *Applicatie Layering* bouwblok zijn belast met alle aspecten van het transport tussen de verschillende "loosely coupled" bouwblokken (lagen) van centrale IZB toepassingen.

Transport is nauw gerelateerd aan het *bouwblok PL8b veilige netwerktoegang. Transport* is de place-holder voor alle zaken m.b.t. performance (bandbreedtes, throttling, Quality of Service etc.) - zowel in reguliere als pandemische situaties (schaalbaarheid) - en beveiliging (encryptie e.d.) van gegevensuitwisselingen.

5.13.5 Koppelvlakken

Applicatie Layering maakt gebruik van:

- Security Services: Alle activiteit op de koppelvlakken dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok Security Services;
- Cloud Services (indien PaaS of IaaS) - container technologie;

Applicatie Layering wordt gebruikt door:

- Multi-Channel Presentatie Services;
- Applicatie Services;
- Data Intelligence Services;
- Data Services;

5.13.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die m.b.t. het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-7c.01	Koppelingen worden bij voorkeur gerealiseerd m.b.v. van API's en micro-services t.b.v. horizontale schaalbaarheid.	Ten behoeve van schaalbaarheid en omdat dit de facto standaard en bewezen technologie is.
PAB-7c.02	De *Applicatie Layering* verzorgen het API Management voor alle API's die in de bouwblokken Applicatie Services en Data Services zijn geïmplementeerd.	Centraal beheer en governance bevorderen eenduidigheid en verminderen daarmee de kans op fouten.
PAB-7c.04	Gebruik van API's moet uitgaan van de API-strategie van de Nictiz (REF: ER012 API-strategie voor de zorg).	Standaardisatie en interoperabiliteit.

5.14 Veilige Applicatie- en Datatoegang (PL8a)

5.14.1 Definitie

Het virtuele bouwblok *Veilige Applicatie- en Datatoegang* bestaat uit de voorzieningen die nodig zijn om gebruikers op een veilige manier toegang te geven tot de applicaties en data op het platform. Dit geldt zowel voor beveiliging van client als client-software. Hiermee is het bouwblok samen *met PL8b Veilige Netwerktoegang* de technische invulling van de dienst *PL8 Veilige applicatie- en dataontsluiting.*

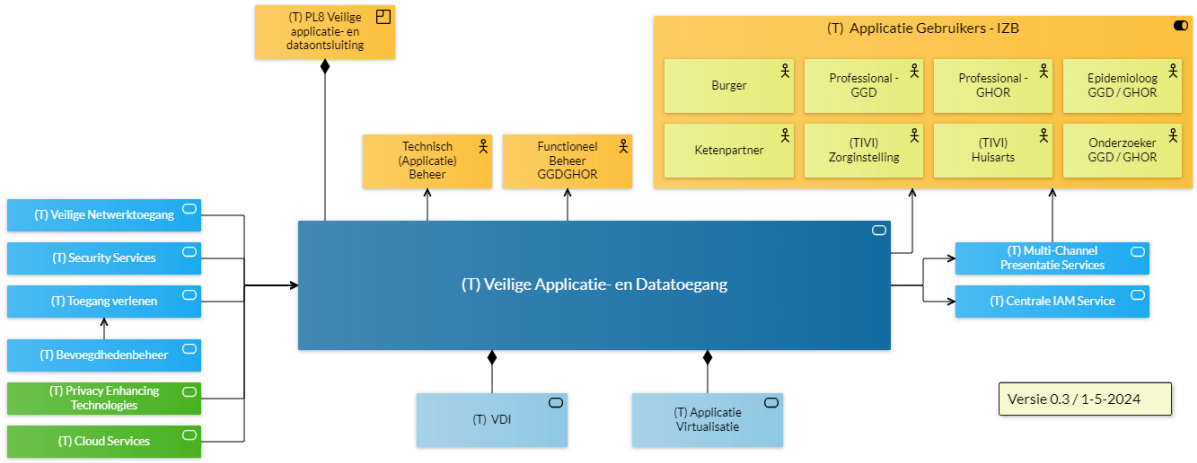
5.14.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Veilige Applicatie- en Datatoegang
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Veilige Applicatie- en Datatoegang dient dermate schaalbaar te zijn dat 130.000 professionals gelijktijdig kunnen deelnemen.

1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA afspraken en het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
4.2.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	De regie- en beheerorganisatie van uitvoerders zijn voorbereidt op het leveren van functionele support aan eindgebruikers tijdens warme fase. *[met warme fase wordt pandemische situatie bedoeld]*	Functioneel support dient ingericht te worden.

6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)security processen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Rekening houdend met genoemde schaalbaarheid.

5.14.3 Inrichting



In bovenstaande figuur is het bouwblok *Veilige Applicatie- en Datatoegang* weergegeven met zijn onderdelen en de aangrenzende bouwblokken die gebruik maken van of gebruikt worden door *Veilige Applicatie- en Datatoegang*.
Welke vormen van *Veilige Applicatie- en Datatoegang* van toepassing zijn is ervan afhankelijk voor wie de toegang wordt gerealiseerd; hierin worden onder andere de volgende actoren onderscheiden:

- Burgers
- Medewerkers/professionals van GGD-en, GHOR en GGD GHOR Nederland
    - (Zorg) professionals
    - Onderzoekers
    - (Functioneel en technisch) Beheerders
- Ketenpartners
    - Callcenter medewerkers (zoals bij Coronapandemie ingezet)
    - Laboratoria
    - RIVM
- Zorginstellingen en Huisartsen

5.14.4 Onderdelen van Veilige Applicatie- en Datatoegang

Het bouwblok Veilige Applicatie- en Datatoegang biedt de faciliteiten voor het op een veilige manier beschikbaar stellen en/of toegankelijk maken van applicaties en data aan gebruikers, ook in pandemische situaties waarin in zeer korte tijd toegang gegeven moet worden aan grote hoeveelheden gebruikers die dikwijls vanaf onbekende en daarom niet vertrouwde locaties werken.

Er zijn verschillende oplossingen mogelijk om applicaties bij de (eind) gebruikers te brengen, afhankelijk van doelgroep, type device, type applicatie (web, fat client, mobile app etc.) en classificatie van de applicatie. Als voorziening van veilige applicatietoegang zijn installatie en configuratie van m.n. het clientdeel van

toepassingen van belang, bijvoorbeeld als onderdeel van Continuous Integration and Delivery (CI/CD). Daarnaast is het van belang dat installaties op zo'n manier en plaats gebeuren dat het uitvoeren, en de configuratie- en executiebestanden van de toepassingen adequaat beveiligd kan worden (Distributie).

Nieuw te ontwikkelen applicaties zullen altijd worden voorzien van een web-based (http) client, maar het platform moet ook ruimte bieden aan bestaande (*legacy*) applicaties (zie ook: Multi-Channel Presentatie Services).
Voor de inzet van deze (client-) applicaties moeten ze geïnstalleerd en/of gedistribueerd worden naar fysieke of virtuele client-devices.
Omdat client-locaties en -apparaten (van burgers, ketenpartners, maar ook van de afzonderlijke GGD-en) niet onder controle van het platform vallen, en het type device op voorhand dikwijls niet bekend is, is het belangrijk zo weinig mogelijk gegevens en processing naar de clientapparaten te distribueren.
Het bouwblok PL8a omvat hiervoor de volgende onderdelen:

Virtual Desktop Infrastructure (VDI)

Het platform moet m.n. tijdens de opschalingsfase bij een pandemie, heel snel maar toch veilig grote hoeveelheden interne en externe gebruikers van een werkplek kunnen voorzien die toegang biedt tot de applicaties en data op het platform. Een manier om dit te faciliteren, is de inrichting van een Virtual Desktop infrastructuur (VDI) voor het aanbieden van virtuele desktops. Met VDI wordt de workload vanaf het gebruikersapparaat verplaatst naar een centrale server omgeving waarin applicaties en gegevens (centraal) zijn beveiligd. De eisen die aan de fysieke werkstations worden gesteld, worden op deze manier triviaal waardoor al beschikbare of eenvoudig aan te schaffen werkstations volstaan.

Omdat VDI op cloud-platformen wordt gehost, is de oplossing bijzonder schaalbaar.
VDI wordt opgenomen in een gezoneerd en beveiligd netwerk (zie ook Veilige Netwerktoegang). Daarmee is de oplossing ook geschikt voor de realisatie van Privileged Access Workstations (PAW) als jumpstation voor (functioneel) beheerders.

Applicatie Virtualisatie

In bepaalde gevallen waarin geen (privacy-) gevoelige gegevens worden verwerkt of slechts door de betrokken burger zelf, kan ook applicatie virtualisatie worden gebruikt, waarbij applicaties in een 'bubble' gecombineerd met ondersteunende software en configuraties wordt uitgevoerd op het client device. Met deze manier van softwaredistributie kunnen applicaties op allerlei verschillende typen apparaten en besturingssystemen worden uitgevoerd, zonder dat ze daarop hoeven te worden geïnstalleerd. In veel gevallen kan dit in zgn. *streaming* modus gebeuren, waarbij -delen van - applicaties al kunnen worden uitgevoerd zonder dat de applicatie in haar geheel is opgehaald vanaf de (streaming-) server.

5.14.5 Koppelvlakken

Veilige Applicatie- en Datatoegang wordt gebruikt door

- Multi-Channel Presentatie Services
- Centrale IAM Services

Veilige Applicatie- en Datatoegang maakt gebruik van

- Veilige Netwerktoegang
- Security Services: Alle activiteit op de Multi-Channel Presentatie Services dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok Security Services;
- Toegang verlenen (Centrale IAM Service)
- Privacy Enhancing Technologies
- Cloud Services

5.14.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die m.b.t. het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-8a.01	Het platform voorziet in veilige toegang tot zijn applicaties en data voor verschillende type client-apparaten en vanaf verschillende locaties.	Client apparatuur is (op voorhand) niet bekend.

5.15 Veilige Netwerktoegang (PL8b)

5.15.1 Definitie

Het virtuele bouwblok *Veilige Netwerktoegang* bestaat uit de voorzieningen die nodig zijn om gebruikers, applicaties en systemen langs een veilige verbinding toegang te geven tot de applicaties en gegevens op het platform.

Tegelijkertijd verhinderen deze voorzieningen toegang tot (delen van) het platform voor gebruikers, applicaties en systemen waarvoor niet expliciet toestemming tot toegang is verleend.

Het bouwblok Veilige Netwerktoegang levert naast veilige netwerkvoorzieningen ook waarde in de uitvoering en governance van andere bouwblokken op het platform, zodat deze veiliger, wendbaarder en aanpasbaar blijven.

Het bouwblok *Veilige Netwerktoegang* is samen *met PL8b Veilige Netwerktoegang* de technische invulling van de dienst *PL8 Veilige applicatie- en dataontsluiting.*

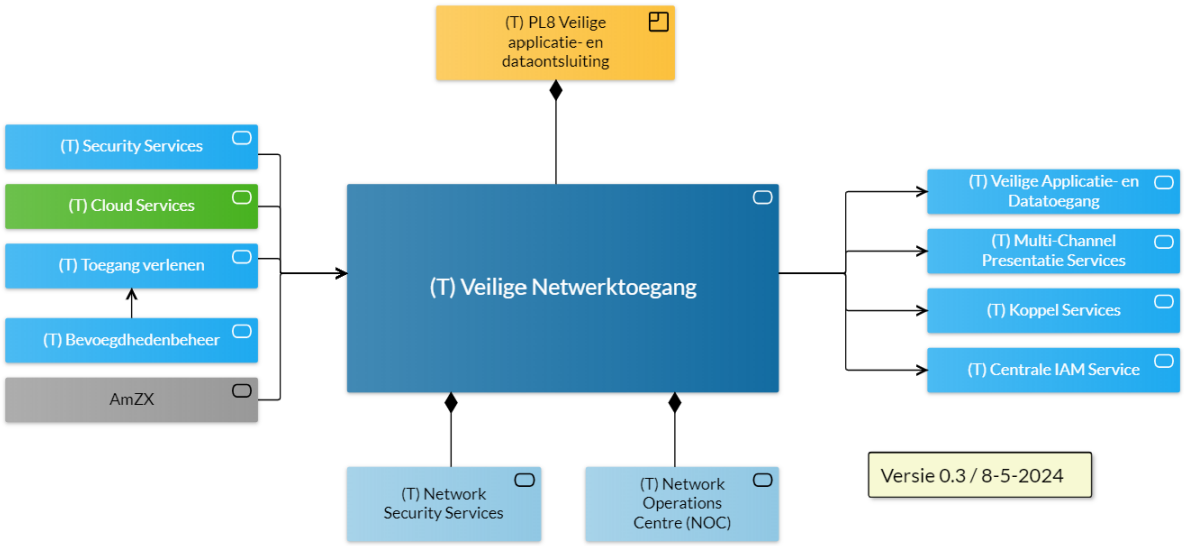
5.15.2 Eisen vanuit LFI

Bron: LFI BRQ				Implicatie Veilige Netwerktoegang
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Veilige Netwerktoegang dient dermate schaalbaar te zijn dat 130.000 professionals gelijktijdig kunnen deelnemen.
1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dat de uitvoer van opgeschaalde medische operationele processen ondersteund dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,95%, met een maximaal dataverlies (RPO) van 30 minuten en een maximale uitvalduur van het IV/ICT-landschap van 6 uur (RTO). Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Middels SLA afspraken en het realiseren van redundantie en geo-spreiding wordt hier rekening mee gehouden.

1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.
3.1.2.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	Het IV/ICT-landschap ondersteunt de medisch-operationele processen zodanig dat het mogelijk is om, afhankelijk van de aard en ernst van de pandemie, bepaalde processtappen door burgers uit te laten voeren (bijvoorbeeld door een modulaire opzet).	De omgeving wordt gekoppeld aan LSP t.b.v. PGO's.
4.2.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	De regie- en beheerorganisatie van uitvoerders zijn voorbereidt op het leveren van functionele support aan eindgebruikers tijdens warme fase. *[met warme fase wordt pandemische situatie bedoeld]*	Functioneel support dient ingericht te worden.

5.15.3 Inrichting

In onderstaande figuur is het bouwblok *Veilige Netwerktoegang* weergegeven met zijn onderdelen en de aangrenzende bouwblokken die gebruik maken van of gebruikt worden door *Veilige Netwerktoegang*.



5.15.4 Onderdelen van Veilige Netwerktoegang

Het bouwblok Veilige Netwerktoegang omvat de volgende onderdelen:

1. Network Security Services
2. Network Operations Centre (NOC)

Network Operations Centre (NOC)

Een Network Operations Centre (NOC) is een stelsel van voorzieningen waar voortdurend de prestaties en gezondheid van een netwerk wordt bewaakt door preventieve, proactieve en reactieve operaties uit te voeren, om zo te beschermen tegen netwerkstoringen en -uitval. Door een NOC in te zetten kan een integraal, compleet en real-time beeld over alle betrokken netwerken worden gecreëerd, waarmee tijdig afwijkingen kunnen worden gesignaleerd. Naar aanleiding hiervan kunnen met preventieve of reactieve maatregelen problemen worden voorkomen of verholpen.

Het NOC houdt onder meer toezicht op netwerktechnologie en -voorzieningen (van bedrading tot verbindingen naar servers, data en/of applicaties), draadloze netwerken, aangesloten netwerkapparatuur zoals firewalls en ook op apparatuur, IoT (*internet of things*) -apparaten en smartphones en telefonie.
Een NOC kan door GGD-en en GGD GHOR Nederland zelf worden ingericht en bemenst, of geheel of gedeeltelijk worden uitbesteed.

Functies van een NOC

Het platform gaat het Network Operations Centre gebruiken om optimale netwerkprestaties en -beschikbaarheid te handhaven en tegelijk een continue uptime te garanderen aan de netwerkgebruikers van het platform. Het NOC is verantwoordelijk voor een hele reeks vitale activiteiten, waaronder:

- Bewaking van het netwerk op problemen die onmiddellijke aandacht vereisen, vooral die welke van buiten de netwerkperimeter komen;
- Het beheren en het monitoren van de networkrouting, (v)LAN switching, SD-WAN en multi-protocol implementaties, VPN-verbindingen;
- Het rapporteren van gebruik, performance en stabiliteit van het netwerk aan de verschillende stakeholders door middel van rapportages en dashboards.

Wat is het verschil tussen een NOC en een SOC?

Het opsporen en verhelpen van storingen die de netwerksnelheid en -beschikbaarheid kunnen verminderen is de verantwoordelijkheid van technici in het NOC. Terwijl technici in het SOC verantwoordelijk zijn voor het opsporen van cyberveiligheidsbedreigingen en het reageren op beveiligingsincidenten.

Network Security Services

De Network Security Services zijn een stelsel van technische netwerkvoorzieningen waarmee alle transport van gegevens over netwerken veilig kan plaatsvinden.

Aangezien het landschap bestaat uit een combinatie van diverse cloud gebaseerde (deel-) oplossingen, moet de beveiliging binnen en rondom het landschap beveiligd worden door middel van cloud-gebaseerde beveiligings-voorzieningen. Toegang van buiten het platform naar onderdelen van het platform zal altijd via deze voorzieningen gebeuren, evenals het onderlinge verkeer tussen de verschillende bouwblokken van het platform zelf.
Voor de beveiliging van alle verkeer van, naar en tussen de verschillende bouwblokken wordt een combinatie van beveiligingsmodellen toegepast waarmee alle vormen van extern verkeer centraal en uniform beheerd en bewaakt kunnen worden. Dit betekent dat alle "extern" verkeer met bijvoorbeeld ketenpartners via de cloud-gebaseerde technologieën moet verlopen.

Zero Trust Network Access

Directe toegang tot applicaties zal voor medewerkers van GGD, GHOR en GGD GHOR Nederland beveiligd worden d.m.v. een Zero Trust Network Access (ZTNA) oplossing.

ZTNA is een beveiligingsoplossing (gebaseerd op het Zero Trust Security model) die op een veilige manier toegang geeft tot applicaties en gegevens vanaf externe locaties. Toegangsbeheer wordt geregeld op basis van policies, en toegang wordt alleen verleend voor specifieke applicaties. Dit in tegenstelling tot VPN waarmee toegang aan een heel (sub) netwerk wordt verleend of geweigerd.

De security roadmap van GGD GHOR Nederland voorziet in de inzet van een ZTNA-oplossing voor medewerkers.

Risk Based Authentication

Met Risk Based Authentication (RBA) wordt toegang tot applicaties en/of gegevens verleend of geweigerd op basis van attributen uit de context waarin toegang wordt gevraagd (zoals IP-nummer, aanwezigheid van actuele anti-virus software op client device etc.) en die zijn vastgelegd in toegangspolicies (ABAC).

Risk Based Authentication is een vorm van Attribute Based Access Control en is onderdeel van Acces Management en Acces Control, zie IAM.

Virtual Private Network (VPN)

VPN biedt de mogelijkheid om een beveiligde netwerkverbinding tot stand te brengen bij gebruik van openbare netwerken. VPN's versleutelen het internetverkeer en verbergen de online identiteit. Dit maakt het voor derden moeilijker om activiteiten online te volgen en gegevens te stelen. De versleuteling vindt plaats in real time.

AmZX en andere zorgnetwerken

Het communiceren via specifieke zorgnetwerken bevordert de beveiliging en snelheid waarmee veilige voorzieningen kunnen worden geïmplementeerd. Het platform wordt aangesloten op de AmZX en andere zorg-specifieke netwerken, waarmee de veilige netwerktoegang tussen GGD-locaties onderling en centrale

voorzieningen op het platform wordt gerealiseerd. De Amsterdam Zorg Exchange (AmZX) is een voorbeeld van een zorg-specifiek netwerk waarin verschillende VPN-connecties zijn gecombineerd tot een community network ten behoeve van verschillende zorginstellingen, waaronder de verschillende GGD-en. Door deze netwerkvoorziening kunnen de instellingen veilig onderling communiceren en de op het AmZX netwerk aangeboden diensten bereiken, waaronder basisregistraties en andere netwerkknooppunten.

Firewalls

Het platform wordt onder meer beveiligd met behulp van firewall services, waaronder web application firewalls (WAF's). De firewall voorzieningen worden gebruikt om tussen de verschillende bouwblokken en tussen het platform als geheel en de 'buitenwereld' om applicaties, data en infrastructuur af te schermen. Hiervoor worden de firewall services voor verschillende taken ingezet:

- Screening van het netwerkverkeer in de netwerklaag (packet filtering firewall), of applicatielaag (application layer firewall)
- Bewaking van connectie status (stateful firewall)
- Bewaking van specifieke compute resources (hostbased / clientbased firewall)
- Bewaking van (delen van) netwerken (network firewall)

Cloud-gebaseerde netwerk edge services

Cloud-gebaseerde netwerk edge services zorgen ervoor dat de toegang voor gebruikers van client apparatuur wordt geoptimaliseerd met behulp van (cloud) edge servers. Omdat de client devices met het platform communiceren via deze gedistribueerde en redundant uitgevoerde voorziening wordt de latency (vertraging) geminimaliseerd en de communicatie tussen client en applicaties en data op het platform robuust en in hoge mate schaalbaar.

Intrusion prevention en detectie functies (IPS/IDS)

Het platform voorziet ook in Intrusion Prevention and Detection functies door middel van een Intrusion Detection Systeem (IDS). Deze monitort en analyseert alle netwerkverkeer en kan aan de hand van bekende patronen afwijkende verzoeken herkennen en melden. Het systeem doet deze herkenning o.a. op basis van:

- Eerdere aanvallen. De technologie signaleert alle netwerkverkeer met dezelfde signatuur als bij bekende eerdere geslaagde aanvallen op andere servers.
- Machine Learning. Het systeem gebruikt informatie uit alles wat er op een gemiddelde dag op het netwerk gebeurt en verfijnt daarmee de toegepaste beschermingsmechanismen.

Er bestaan een aantal Intrusion Detection functies, voor:

- Netwerksystemen - deze analyseren al het verkeer op alle devices vanaf een bepaald punt
- Host-systemen - deze analyseren het verkeer van en naar onafhankelijke devices op uw netwerk en laten alle andere devices met rust
- Systemen op protocolbasis - deze plaatsen een beschermlaag tussen een device en de server en monitoren al het verkeer tussen de twee
- Systemen op basis van applicatieprotocollen: deze plaatsen een beschermlaag tussen een groep servers en analyseren hoe deze onderling communiceren
- Hybride systemen: deze combineren verschillende van de hierboven beschreven benaderingen in een specifiek systeem

Een Intrusion Prevention System (IPS) monitort het verkeer ook. Het doel van een IPS is het voorkomen van schade, en naast de detectie functies wordt bij een verdacht voorval dat verkeer geblokkeerd. Het SOC-team start daarna met onderzoeken en bepalen of het veilig is om de poorten weer open te zetten.

Een IPS biedt bescherming tegen indringers van binnen- en buitenaf. Voor alle cases worden maatregelen ingeregeld op een IPS. Het kan hierbij onder meer gaan om de volgende maatregelen:

- Het beëindigen van malafide sessies. Het systeem kan bepalen waar de ongebruikelijke activiteit binnenkomt en deze toegang blokkeren, bijvoorbeeld door de TCP-sessie te beëindigen of het IP-adres te blokkeren
- Het aanpassen van Firewalls rules. Het systeem kan de configuratiefouten in de firewall instellingen detecteren waardoor de aanval kon plaatsvinden. Door de geprogrammeerde code te wijzigen, kunnen vergelijkbare aanvallen in de toekomst worden voorkomen
- Opschonen van malafide content. Het systeem kan scannen op beschadigde of malafide content op servers en deze verwijderen.

Het IPS werkt in real time en de technologie controleert elk pakket dat zich binnen de beschermde ruimte beweegt. Meldingen en -geautomatiseerde - acties vanuit een IPS moeten gecontroleerd worden door bijv. het NOC/SOC om het gevaar van vals-positieven te ondervangen.

Proxy Services

Proxy Services voorzien in filtering en/of caching van netwerkstromen tussen de (virtuele) werkplek van een gebruiker en de websites en -services. De proxy-services zijn onderdeel van de cloud-based netwerktechnologieën van het platform.

Om de veiligheid te vergroten worden forward proxy-services ingezet die verkeer evalueren, zodat bepaalde (verdachte en ongewenste) uitgaande verzoeken geblokkeerd kunnen worden.

Ten behoeve van load-balancing en om rechtstreekse communicatie met servers en/of applicaties te voorkomen worden reverse proxyservices gebruikt, zodat prestaties en beveiliging verbeterd worden.
Met de inzet van de proxy-services op het platform worden transparantie, vervorming en/of (hoge) anonimiteit in de gegevensstroom geborgd, en wordt het lastiger voor malafide websites om het gedrag van gebruikers en applicaties in kaart te brengen met technieken voor tracering.

5.15.5 Koppelvlakken

Veilige Netwerktoegang wordt gebruikt door

- Veilige Applicatie- en Datatoegang
- Multi-Channel Presentatie Services
- Koppel Services
- Centrale IAM Services

Veilige Netwerktoegang maakt gebruik van

- Security Services: Alle activiteit op de Multi-Channel Presentatie Services dient gemonitord en gelogd te worden. Verdere verwerking van de loggegevens gebeurt door het bouwblok Security Services;
- Cloud Services
- Toegang verlenen (Centrale IAM Service)

5.15.6 Architectuurbesluiten

In onderstaande tabel zijn de architectuurbesluiten beschreven die m.b.t. het bouwblok zijn geformuleerd.

ID	Architectuurbesluit	Rationale
PAB-8b.01	Het platform voorziet in veilige toegang tot zijn applicaties en data voor verschillende type client-apparaten en vanaf verschillende locaties	Verschillende locaties en typen client devices moeten kunnen worden aangesloten.
PAB-8b.02	Het volledige netwerkpad waarlangs toegang wordt gegeven tot applicaties of data is beveiligd, zowel extern als intern (zonering en segmentatie)	Met een gezoneerd en gesegmenteerd netwerkpad wordt de impact bij inbreuk van de beveiliging verkleind (isolation of impact).
PAB-8b.03	ZTNA is onderdeel van de security raadmap voor GGD GHOR Nederland en dus ook voor het platform	Met ZTNA kan een hogere graad van beveiliging worden gerealiseerd.
PAB-8b.04	Alle netwerkfuncties worden aangesloten en operationeel gestuurd door het Netwerk Operations Center (NOC)	Door netwerkfuncties integraal en gecentraliseerd aan te sturen vanuit een NOC wordt de beschikbaarheid (toegang tot applicaties en gegevens) en veiligheid van de verschillende netwerken en hun functies vergroot.
PAB-8b.05	Alle datastromen voor gebruikers, applicaties en gegevens lopen door veilige toegangsvoorzieningen.	Door gegevensstromen over de veilige toegangsvoorzieningen te laten lopen voor gebruikers, applicaties en gegevens wordt de veiligheid van de datastromen en kan sneller een integraal beeld van de risico's worden verkregen.
PAB-8b.06	De buitenste netwerkfuncties voor veilige netwerk toegang maken gebruik van Cloud-gebaseerde netwerktechnologieën.	Door Cloud-gebaseerde functies te gebruiken voor de buitenste netwerkvoorzieningen kunnen sneller (geautomatiseerd) en veiliger (op basis van secure-by design templates) gegevensstromen worden geïmplementeerd en het veilig beheren voor applicaties, gebruikers en gegevens gefaciliteerd.
PAB-8b.07	Alle op cloud gebaseerde infrastructuren maken gebruik van Cloud-gebaseerde netwerkfuncties.	Door Cloud-gebaseerde functies te gebruiken voor de cloud infrastructuren kunnen sneller (geautomatiseerd) en veiliger (op basis van secure-by design templates) gegevens stromen worden voorzien en beheerd voor applicaties, gebruikers en gegevens.
PAB-8b.08	Fysieke omgevingen maken op de perimeter gebruik van centraal voorziene Cloud-gebaseerde netwerkfuncties.	Door Cloud-gebaseerde functies te gebruiken voor de cloud infrastructuren kunnen sneller (geautomatiseerd) en veiliger (op basis van secure-by design templates) gegevensstromen worden voorzien en beheerd voor applicaties, gebruikers en gegevens. Ook wordt voorkomen dat vanuit gekoppelde omgevingen (bijv. van leveranciers) eigen internetverbindingen worden opgezet, zonder gebruik te maken van de netwerkfuncties die door het bouwblok veilige netwerktoegang gerealiseerd zijn.
PAB-8b.09	Gegevens voor het monitoren en verbeteren van de beveiliging van het platform worden doorgegeven	Informatie welke gegenereerd wordt door netwerkvoorzieningen zijn cruciaal voor het kunnen monitoren en beveiligen van het platform. Alle voorzieningen in dit bouwblok moeten en/of mogen worden gebruikt voor het leveren van gegevens aan het bouwblok Security Services.

6 Bijlagen

6.1 Fysieke Netwerken

6.1.1 Definitie

Het bouwblok Fysieke Netwerken is verantwoordelijk voor het veilig ontsluiten van centrale voorzieningen IZB op locaties binnen Nederland. Voornamelijk tijdens pandemische situaties zal er opgeschaald worden en zullen er vele honderden locaties ontsloten moeten worden. Dit gebeurt op basis van (aansluit)voorwaarden van GGD GHOR Nederland met behulp van dienstverlening van externe leveranciers. Het bouwblok Fysieke Netwerken valt niet onder een dienst met een PL-nummer, omdat dit bouwblok is toegevoegd nadat alle PL-nummers zijn toegekend.

Inrichting van het bouwblok is gebaseerd op Software Defined Networking (SDN). Dit maakt de automatisering van netwerktaken mogelijk en zorgt voor meer flexibiliteit, schaalbaarheid en efficiëntie in het netwerkbeheer. ZTNA zal worden toegepast binnen de beveiligde verbindingen zoals S2S-VPN, SD-WAN en SD-LAN om de toegang tot netwerkresources te beheren en te controleren op basis van strikte identiteitsverificatie en contextuele beoordeling

Gebruikers zullen gedurende een pandemische situatie via een schaalbare VDI oplossing toegang krijgen tot het beveiligde netwerk. Internet break-out mogelijkheden zullen ervoor zorgen dat het netwerk ontlast wordt. Hierdoor zullen gebruikers op vaste locaties, ad-hoc locaties of thuis toegang krijgen.

6.1.2 Eisen vanuit het LFI

De eisen van het LFI zijn voor fysieke netwerken specifiek gemaakt.

Bron: LFI BRQ				Implicatie Fysieke netwerken
Nr.	**IV/ICT-basiseis**	**Categorie**	**Operationele eis voor IV/ICT-landschap van uitvoerders**	
1.1.1.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek en processen	Het IV/ICT-landschap moet minimaal voorzien in de uitvoer van medisch-operationele processen waaraan gelijktijdig 130.000 professionals deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Fysieke Netwerken dient dermate schaalbaar te zijn, dat 130.000 professionals gelijktijdig op netwerk niveau op de verschillende locatie kunnen verbinden naar het pandemisch parate IV landschap met de vereiste bandbreedte. De vereiste kengetallen zullen gehanteerd worden als een absoluut minimum. De voorzieningen voor Fysieke Netwerken zullen een gedeelde verantwoordelijk worden waarbij telecom providers en partners zelf verantwoordelijk zijn voor de capaciteit en werking van hun onderdeel. De Fysieke Netwerken dienst zal met regelmaat in verschillende situaties worden getest en knelpunten worden gesignaleerd om tot een verbeterde dienst te komen. situatie een passende oplossing kunnen bieden.
1.1.2.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek en processen	Het IV/ICT-landschap voorziet in het snel – bijvoorbeeld binnen enkele dagen – (landelijk) opschalen van professionals voor de uitvoering van medisch-operationele processen.	Met leveranciers worden contract afspraken gemaakt over op- en afschaling tot op landelijk pandemisch niveau.

1.1.3.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap dient 24x7 beschikbaar te zijn met een beschikbaarheid van minimaal 99,9%. Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	Door middel van SLA- en DAP-afspraken en het realiseren van redundantie in leveranciers met geografische spreiding wordt hier rekening mee gehouden. Het ontwerp van de oplossing houdt, waar mogelijk, rekening met meervoudige uitvoering op component niveau om zo de gewenste van 99.9% beschikbaarheid van de dienst minimaal te garanderen in de juiste situatie. Onderdeel van het ontwerp van de leveranciers is tevens het uitwerken en realiseren van noodvoorzieningen waarbij professionals snel en effectief hun werkzaamheden weer kunnen uitvoeren indien delen uitvallen zoals netwerkapparatuur.
1.1.5.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap is en blijft up-to-date met gangbare communicatieprotocollen, infrastructuur en netwerk architectuur (bijvoorbeeld minimaal N-1).	De LCM en Update policy worden contractueel vastgelegd met de leveranciers. Tevens zullen ontwikkelingen in de markt nauwgezet gevolgd en overwogen worden. Continue verbeteringen aan de dienstverlening zijn een integraal onderdeel van de dienstverlening. Voor de netwerkcommunicatie dienstverlening wordt ingezet op proven (N-1) techniek.
1.1.8.	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Techniek	Het IV/ICT-landschap maakt het mogelijk te voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen) en NIS 2 voor netwerkbeveiliging.	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening. Speciale aandacht gaat uit naar NIS 2 wetgeving.
1.2.2	Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.	Organisatie en processen	Voldoen aan de wettelijke vereisten en de binnen-de-sector gangbare normen zoals NEN-7510 (beheersprocessen), 7512 (informatiedeling tussen zorgaanbieders) en 7513 (vastleggen van het gebruik van informatiesystemen).	GGD GHOR Nederland IV beleid wat onder meer is gebaseerd op NEN7510, 7512, 7513 en NIS 2 zijn als uitgangspunt/kaders opgenomen voor de bouw van het platform. Zie hiervoor kaderstelling security. Het betreft bij 1.2.2 organisatie en processen (governance) en bij 1.1.8 de techniek. Naast vigerende wet- en regelgeving zal, tijdens de levensloop van de dienstverlening, blijvend geanticipeerd worden op komende wet- en regelgeving die mogelijk van toepassing is op de dienstverlening.

3.1.2.	Het IV/ICT-landschap maakt digitale dienstverlenging aan burgers mogelijk.	Techniek	Fysieke Netwerken zorgt ervoor dat het IV wordt ontsloten en hiermee ondersteunt de medisch-operationele processen zodanig dat het mogelijk is om, afhankelijk van de aard en ernst van de pandemie, bepaalde processtappen door burgers uit te laten voeren (bijvoorbeeld door een modulaire opzet).	Burgers mogen erop vertrouwen dat Fysieke netwerken infrastructuur bij ketenpartners en op de test, priklocaties betrouwbaar functioneren en beschikbaar zijn conform contractuele afspraken en dienstverlening.
4.1.2.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap maakt de uitvoering van processen conform LCI-richtlijnen door uitvoerders mogelijk.	Alle componenten t.a.v. Fysieke netwerken zijn beschikbaar en snel schaalbaar met voldoende redundantie conform contractuele afspraken en dienstverlening. Zodat voorzien kan worden in piekbelasting bij een pandemische situatie. Dit wordt o.a. bereikt door geautomatiseerde opschaling en in te zetten op standaard diensten van leveranciers.
4.1.6.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Techniek	Het IV/ICT-landschap voorkomt een te grote afhankelijkheid van een of meerdere leveranciers (vendor lock-in). Applicaties moeten door nieuwe leveranciers overgenomen kunnen worden.	Alleen standaardoplossingen worden uitgevraagd, op basis van proven technology. Uitgangspunt is software defined networking. Op basis van policies moet een leverancier een geschikte oplossing/configuratie maken.
4.2.3.	Applicaties zijn gericht op het ondersteunen van hoog-volume processen.	Organisatie en processen	De regie- en beheerorganisatie van uitvoerders zijn voorbereid op het leveren van functionele support aan eindgebruikers tijdens warme fase.	Functioneel support en regie organisatie dienen zo ingericht te worden dat zij voorbereid zijn op het leveren van functionele support aan eindgebruikers tijdens warme fase.
5.1.1.	Gegevensregistratie en gegevensuitwisseling zijn digitaal, geautomatiseerd en gestandaardiseerd.	Techniek	Het IV/ICT-landschap moet near-realtime, digitale uitwisseling met de ketenpartners van gegevens uit de medisch-operationele processen ondersteunen bij 200.000 testafspraken per dag en 1.500.000 vaccinaties per week en waarbij gelijktijdig 130.000 professionals aan de processen deelnemen en 1.000.000 burgers per dag persoonlijke informatie raadplegen en/of afspraken plannen (cijfers o.b.v. ervaringen in de coronacrisis).	Inrichting (schaalbaarheid) worden op piekbelasting ontworpen. Aangezien de voorziening een onderdeel is van een keten van verschillende onderdelen zullen er op gezette tijden regressie testen op basis van dergelijke kenmerken gesimuleerd worden in een daarvoor ingerichte test- en acceptatieomgeving. Een dergelijke aanpak dient nader uitgewerkt te worden in samenwerking met andere belanghebbenden en verantwoordelijken van de andere onderdelen (uitvoerders) die deel uitmaken van de keten. Ketenpartners worden via Diginetwerk op het AMZX aangesloten.
6.1.3.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Techniek	Het IV/ICT-landschap dient 24x7 beschikbaar te zijn, met een beschikbaarheid van minimaal 99,9%. Voor cruciale applicaties dient bij uitval een noodprocedure beschikbaar te zijn.	De specifieke eisen zullen in het PvE worden meegenomen. Zowel in techniek als organisatie bij leveren en ondersteunen. Een noodprocedure zal ook incl. support moeten worden getest en zal in de PvE worden uitgevraagd.

6.2.1.	De organisatie en ICT zijn voorbereid op opschalen en afschalen.	Organisatie en processen	(Cyber)security processen en organisatie zijn schaalbaar en berekend op inzet van 130.000 professionals in combinatie met een (zeer) hoog risicoprofiel voor externe dreiging.	Schaalbaarheid van de oplossing en robuustheid tegen cyber bedreigingen zijn primaire uitgangspunten bij het ontwerp, realisatie en instandhouding van de oplossing. Rekening houdend met genoemde schaalbaarheid en dreigingsbeeld. Omdat de aangesloten gebruikers, endpoints, netwerken niet door de GGD-GHOR worden gecontroleerd en beheerd worden deze als onvertrouwd beschouwd. Hierom worden content inspectie en filtering toegepast en alleen verkeer dat hierdoorheen komt worden toegestaan. Aangesloten ketenpartners worden middels een SOC - SOC koppeling aangesloten. Bij aanvallen en dreigingen zullen deze gezamenlijk optrekken om de dienstverlening te beschermen. L&O is het aanspreekpunt voor operationele ondersteuning conform dienstverlening. Afstemming met uitvoerders van andere keten onderdelen maakt onderdeel uit van de governance van de totaaloplossing.

6.1.3 Inrichting

De inrichting en onderdelen van het bouwblok Fysieke Netwerken worden nog nader bepaald.

6.2 Architectuurbesluiten

ID	Architectuurbesluit	Rationale
PAB-0.01	Het IV-landschap wordt ingericht volgens een decoupled architectuur.	Een decoupled architectuur is er een waarin elk van de componenten weinig of geen kennis heeft van de definities van andere afzonderlijke componenten, of er gebruik van maakt. Deze methodiek verkleint het risico dat een wijziging in één component, zowel intern als extern, onverwachte veranderingen in andere delen veroorzaakt. Door de onderlinge verbindingen te beperken, kunnen problemen worden geïsoleerd.
PAB-0.02	Vanaf ontwerp t/m realisatie geldt voor alle producten, diensten en systemen het principe “security-by-design”.	Met 'security-by-design” worden alle componenten zo veilig mogelijk ontworpen en gerealiseerd en t.o.v. elkaar afgeschermd. Hierdoor wordt de impact van een eventuele inbreuk geminimaliseerd.
PAB-0.03	Alle componenten die ingezet worden voor het platform voldoen aan het principe “security-by-default”.	Out-of-the-box worden de meest veilige configuraties gebruikt. Verlichting van de veiligheidsmaatregelen gebeurt dan gecontroleerd en expliciet.
PAB-0.04	Asset- en configuratiemanagement zijn ingericht	Zonder asset- en/of configuratiemanagement kan inrichting, beheer en monitoring op het platform niet juist worden uitgevoerd.
PAB-0.05	Alle componenten voldoen aan de richtlijnen, wetten, principes, normen, standaarden en eisen zoals	Door te voldoen aan het gestelde in het kaderdocument wordt geborgd dat gebruikte componenten en oplossingen

	geformuleerd in het kader document [REF:IR006].	compliant en veilig zijn en de interoperabiliteit met (toekomstige) IV-ontwikkelingen mogelijk is.
PAB-1.01	Voor Identity Management wordt de Doelarchitectuur Identity and Access Management [REF:IR004] gevolgd.	De doelarchitectuur is vastgesteld en betreft de generieke, federatieve voorzieningen t.b.v. GGD-en, GHOR en GGD GHOR Nederland.
PAB-1.02	Het platform moet, zodra specificaties bekend zijn, worden toegerust voor aansluiting/gebruik van de EUDI Wallet.	Aansluiten bij Europese normen en wetgeving.
PAB-1.03	Access Management moet de mogelijkheid hebben om op basis van dataverwerkingsrollen en dataverwerkingsregels, welke zijn gespecificeerd in het domeinmodel, (geautomatiseerd) autorisaties toe te kennen.	In een data-centrisch landschap zijn dataverwerkingsrollen en -regels onderdeel van het domeinmodel.
PAB-1.03	Access Management moet de mogelijkheid hebben om op basis van dataverwerkingsrollen en dataverwerkingsregels welke zijn gespecificeerd in het domeinmodel geautomatiseerd autorisaties toe te kennen.	In een data-centrisch landschap zijn dataverwerkingsrollen en -regels onderdeel van het informatiemodel.
PAB-1.04	Consent registratie vindt bij voorkeur plaats d.m.v. Mitz	Nationale visie gezondheidsinformatiestelsel.
PAB-2.01	Alle cloud voorzieningen voor dataverwerking en -opslag worden afgenomen van datacenters gesitueerd in de Europese Economische Ruimte (EER)	Met deze eis wordt voldaan aan de voorwaarden aan het gebruik van public cloud voor medische gegevens zoals gesteld in het Rijksbreed cloudbeleid.
PAB-2.02	Implementatiemodel is hybrid cloud	• Private cloud t.b.v. hosting van data (data soevereiniteit). • Public Cloud voor out-scale mogelijkheden applicaties waarbij niet de maximale resources gereserveerd hoeven te worden.
PAB-2.03	Alle cloud-resources worden geautomatiseerd beheerd met Infrastructure as Code (IaC)	Door infrastructuur inrichting te automatiseren wordt: • De kans op (configuratie-) fouten verkleind; • Het on-demand klaarzetten van OTAP-omgevingen versimpeld.
PAB-2.04	Applicaties (modules) op de cloudomgeving worden aangeboden via container technologie.	Container technologie: • Verhoogt de portabiliteit; • Vereenvoudigt het beheer van micro-services; • Faciliteert segmentatie (vermindering impact bij wijzigingen en incidenten).
PAB-2.05	Alle containers op de cloudinfrastructuur worden beheerd met container-orkestratietechnologie	Het gebruik van container-orkestratietechnologie in de cloud zorgt voor een efficiënt beheer, schaalbaarheid en automatisering van container-gebaseerde applicaties.
PAB-2.06	Hosting redundant en geografisch gespreid	Beschikbaarheid en continuïteit met minimale uitval tijd.
PAB-2.07	Op- en afschalen van de cloudomgeving moet automatisch gebeuren op basis van de verbruikte resources	Op- en afschaling moet eenduidig, snel en foutloos gebeuren.
PAB-3a.01	Het platform maakt gebruik van de bestaande SOC/SIEM voorzieningen.	Er is een bestaande SOC/SIEM oplossing waarvoor een roadmap bestaat.

PAB-3a.02	Alle IV-voorzieningen worden aangesloten op de Security Services voor de betreffende IV-voorziening voordat ze in productie gaan.	Het onder controle krijgen van de juiste security baseline voor IV-voorzieningen is een continu proces. Het aangesloten zijn van alle IV-voorzieningen op Security Services draagt bij aan een betere en snellere bescherming tegen aanvallen en kwetsbaarheden.
PAB-3a.03	Alle gegevensuitwisseling tussen de componenten van Security Services en met andere bouwblokken gebeurt (exclusief) via het component Verwerken Security Informatie en Metagegevens.	Hiermee wordt maximale controle bereikt voor de correcte, en tijdige verwerking van Security Gegevens.
PAB-3a.04	De IV-voorzieningen van leveranciers, zorg- en ketenpartners en GGD GHOR Nederland die data bewerken of uitwisselen met het platform, leveren altijd beveiligingsgegevens aan op de centrale Security Services.	Alle verwerking en opslag van gegevens die eigendom zijn van de GGD'en wordt gecontroleerd en gemonitord.
PAB-3a.05	Alle IV-voorzieningen van zowel leveranciers als zorg- en ketenpartners en GGD GHOR Nederland die onderdeel uitmaken van het platform, wisselen de beveiligingsgegevens met Security Services uitsluitend uit via de centrale Verwerken Security Informatie en Metagegevens voorziening.	Verspreiding van security-gegevens over verschillende systemen is ongewenst omdat daardoor onvoldoende controle op gebruik en misbruik van deze gegevens kan worden uitgevoerd.
PAB-3a.06	De situationele informatie (context) die nodig is voor de interpretatie van security gegevens moeten bij de security gegevens worden bewaard.	Alle benodigde metagegevens, zoals onder andere beschreven in NEN7513, en overige asset en configuratie managementinformatie, worden meegestuurd naar de Security Services gegevens voorzieningen. Daarmee kan Security Services de opgevangen security gegevens verrijken met situationele informatie om security gegevens te kunnen interpreteren.
PAB-3a.07	Voor het vergroten van de volwassenheid volgens het SOC Capability Maturity Model (SOC-CMM) worden de producten gebruikt die vanuit SOC-CMM beschikbaar worden gesteld (op dit moment zijn dat xlsx bestanden).	Eenheid van taal en standaardisatie. SOC-CMM is in Nederland de de-facto standaard welke ook gebruikt wordt door Z-CERT.
PAB-3a.08	Asset en configuratie management informatie-uitwisseling gebruiken OWASP Bill-of-Materialen (BOM's) cyclonedx gegevens formaat	OWASP heeft een open dataformaat ontwikkeld samen met leveranciers van hardware en software. Dit formaat moet binnen de asset en configuratie managementprocessen gebruikt worden voor het uitwisselen van BOM's. Deze geeft daarmee altijd een up-to-date inzicht in de geleverde goederen binnen de diensten en oplossingen.
PAB-3a.09	Voor het bouwblok Security Services wordt het woordenboek gebruikt zoals dat is opgesteld en wordt onderhouden door Cyberveilig Nederland. bron: https://cyberveilignederland.nl/woordenboek	Het gebruik van dit externe woordenboek bevordert de communicatie met leveranciers en professionals.
PAB-3a.10	De verwerking van security-gegevens, zoals beschreven in de dienst "Verwerken Security Informatie en Metagegevens" wordt uitgevoerd	Op deze manier is het mogelijk om meerdere SOC en SIEM oplossingen tegelijk gebruik te laten maken van de centrale functies voor de verwerking van

	in een andere oplossing dan een SIEM oplossing.	securitygegevens en is het relatief eenvoudig om een gebruikte SOC en SIEM oplossing te vervangen.
PAB-3a.11	Security gegevensverwerking en opslag draaien op zeer schaalbare oplossingen	De Security Services voor de verwerking en opslag van security-gegevens moeten ten minste zo schaalbaar zijn als de voorzieningen die zij monitoren.
PAB-3a.13	Alle Security Services voorzieningen maken, voor de verwerking en opslag van securitygegevens, gebruik van de functie Opslaan Securityinformatie en Metagegevens.	Op deze manier wordt voldaan aan de eis vanuit afdeling Compliance om invulling te geven aan de uitvoering van NEN-7513 door security informatie en gebeurtenissen gescheiden op te slaan.
PAB-3b.01	Voor de bescherming van privacygevoelige gegevens wordt gebruik gemaakt van Privacy Enhancing Technologies (PET).	PET bieden een hoge mate van bescherming.
PAB-4a.01	Aanmaken van audit-log records gebeurt in de data services. Andere services, zoals Applicatie- en Koppel Services, leveren hiervoor de metadata.	Het werkelijk verlenen of weigeren van toegang (acces control) op basis van (input-) regels gebeurt in data services.
PAB-4a.02	Data Services en Opslag Services worden bij elkaar gehost	Performance van de data toegang moet ook voor de grote aantallen transacties tijdens pandemieën gegarandeerd zijn.
PAB-4b.01	Primaire (OLTP) data van het platform wordt alleen via de API's van de Data Services benaderd.	(Fysieke) opslag is transparant om modulariteit ten behoeve van flexibiliteit te borgen.
PAB-5.01	Koppelingen worden bij voorkeur gerealiseerd m.b.v. van API's en micro-services t.b.v. horizontale schaalbaarheid.	Ten behoeve van schaalbaarheid en omdat dit de facto standaard en bewezen technologie is.
PAB-5.02	De *Koppel Services* verzorgen het API Management van alle API's die in het landschap zijn geïmplementeerd.	Centraal beheer en governance bevorderen eenduidigheid en verminderen daarmee de kans op fouten.
PAB-5.03	De *Koppel Services* verzorgen ook veilige voorzieningen voor 'traditionele' vormen van gegevensuitwisseling.	Niet alle ketenpartners kunnen al koppelen met moderne koppelvlakken zoals Rest-API's.
PAB-5.04	Gebruik van API's moet uitgaan van de API-strategie van de Nictiz (REF: ER012 API-strategie voor de zorg).	Standaardisatie en interoperabiliteit.
PAB-6.01	Data virtualisatie heeft voorkeur boven ETL/ELT.	NORA implicatie 'Verwijs naar de bron'. Verwijzen naar de bron heeft voorkeur boven een kopie uit die bron.
PAB-6.02	Dataleveringen aan afnemers verlopen altijd via het DIP, dus niet direct vanuit de (interne) Data Services.	Op deze wijze is er een centraal punt in het landschap waarlangs data uit de applicaties naar "buiten" gaat en is beheer van de dataleveringen minder complex.
PAB-6.03	Voor toegang voor eindgebruikers tot dataproducten, met name dashboards, rapporten en bestanden wordt gebruik gemaakt van de IAM Services.	Gecentraliseerd beheer van gebruikerstoegang.
PAB-6.04	Uitwisseling van data via API services heeft de voorkeur boven andere technieken.	Ten behoeve van schaalbaarheid en omdat dit de de facto standaard is.
PAB-7a.01	Multi-Channel Presentatie Services voorzien uitsluitend in het omzetten van informatie tussen de verschillende kanalen en de applicatie services.	Door de *decoupled* architectuur worden presentatie (look & feel) en verwerking gescheiden en kunnen ze onafhankelijk van elkaar worden aangepast / vervangen.
PAB-7a.02	De inrichting en het beheer van de presentatieaspecten, zoals stijl en interactie, moet over de	Op deze manier wordt eenvormigheid en eenduidigheid afgedwongen en het beheersgemak vergroot.

	verschillende kanalen eenvoudig en eenduidig zijn en via één interface mogelijk zijn.	
PAB-7a.03	De voorziening is inclusief.	Digitale inclusie gaat over meedoen op digitaal gebied voor iedere burger. Niet iedereen kan digitale diensten even makkelijk gebruiken. De overheid wil dit op verschillende manieren verbeteren. Het ontwerp houdt, daar waar mogelijk, rekening met deze groep van eindgebruikers.
PAB-7a.04	Channel Presentatie Services kunnen ook aangesloten worden op andere content leverende systemen dan het datacentrische landschap, zoals een digitale leer omgeving	Optimalisatie gebruik van de presentatie-voorzieningen
PAB-7b.01	Voor de implementatie van (generieke) applicatie componenten wordt gebruik gemaakt van micro-services.	Micro-services vergroten de schaalbaarheid, portabiliteit en herbruikbaarheid van applicatiefuncties.
PAB-7b.02	Communicatie tussen applicatie onderdelen gebeurt via API's.	Decoupled architectuur maakt vervanging van verschillende bouwblokken mogelijk met minimale impact voor overige bouwblokken.
PAB-7b.03	Presentatie (UX) voorzieningen worden niet door applicatie services , maar door Multi-Channel Presentatie bouwblok uitgevoerd.	Decoupled architectuur maakt vervanging van verschillende bouwblokken mogelijk met minimale impact voor overige bouwblokken.
PAB-7b.04	Aanmaken van Audit-log records gebeurt in de data services. Applicatie services leveren hier voor de metadata.	Het werkelijk verlenen of weigeren van toegang (acces control) op basis van (input-) regels gebeurt in data services.
PAB-7c.01	Koppelingen worden bij voorkeur gerealiseerd m.b.v. van API's en micro-services t.b.v. horizontale schaalbaarheid.	Ten behoeve van schaalbaarheid en omdat dit de facto standaard en bewezen technologie is.
PAB-7c.02	De *Applicatie Layering* verzorgen het API Management voor alle API's die in de bouwblokken Applicatie Services en Data Services zijn geïmplementeerd.	Centraal beheer en governance bevorderen eenduidigheid en verminderen daarmee de kans op fouten.
PAB-7c.04	Gebruik van API's moet uitgaan van de API-strategie van de Nictiz (REF: ER012 API-strategie voor de zorg).	Standaardisatie en interoperabiliteit.
PAB-8a.01	Het platform voorziet in veilige toegang tot zijn applicaties en data voor verschillende type client-apparaten en vanaf verschillende locaties.	Client apparatuur is (op voorhand) niet bekend.
PAB-8b.01	Het platform voorziet in veilige toegang tot zijn applicaties en data voor verschillende type client-apparaten en vanaf verschillende locaties.	Verschillende locaties moeten kunnen worden aangesloten.
PAB-8b.02	Het volledige netwerkpad waarlangs toegang wordt gegeven tot applicaties of data is beveiligd, zowel extern als intern (zonering en segmentatie).	Met een gecompartimenteerd netwerkpad wordt de impact bij inbreuk van de beveiliging verkleind (isolation of impact).
PAB-8b.03	ZTNA is onderdeel van de security raadmap voor GGD GHOR Nederland en dus ook voor het platform.	Met ZTNA kan een hogere graad van beveiliging worden gerealiseerd.
PAB-8b.04	Alle netwerkfuncties worden aangesloten en operationeel	Door netwerkfuncties integraal en gecentraliseerd aan te sturen vanuit een NOC wordt de beschikbaarheid

	gestuurd door het Netwerk Operations Center (NOC)	(toegang tot applicaties en gegevens) en veiligheid van de verschillende netwerken en hun functies vergroot.
PAB-8b.05	Alle datastromen voor gebruikers, applicaties en gegevens lopen door veilige toegangsvoorzieningen.	Door gegevensstromen over de veilige toegangsvoorzieningen te laten lopen voor gebruikers, applicaties en gegevens wordt de veiligheid van de datastromen en kan sneller een integraal beeld van de risico's worden verkregen .
PAB-8b.06	De buitenste netwerkfuncties voor veilige netwerk toegang maken gebruik van Cloud-gebaseerde netwerktechnologieën.	Door Cloud-gebaseerde functies te gebruiken voor de buitenste netwerkvoorzieningen kunnen we sneller (geautomatiseerd) en veiliger (op basis van secure-by design templates) gegevens stromen voorzien en beheren voor applicaties, gebruikers en gegevens.
PAB-8b.07	Alle op cloud gebaseerde infrastructuren maken gebruik van Cloud-gebaseerde netwerk functies.	Door Cloud-gebaseerde functies te gebruiken voor de cloud infrastructuren kunnen sneller (geautomatiseerd) en veiliger (op basis van secure-by design templates) gegevens stromen worden voorzien en beheerd voor applicaties, gebruikers en gegevens.
PAB-8b.08	Fysieke omgevingen maken op de perimeter gebruik van centraal voorziene Cloud-gebaseerde netwerk functies.	Door Cloud-gebaseerde functies te gebruiken voor de cloud infrastructuren kunnen sneller (geautomatiseerd) en veiliger (op basis van secure-by design templates) gegevensstromen worden voorzien en beheerd voor applicaties, gebruikers en gegevens. Ook wordt voorkomen dat vanuit gekoppelde omgevingen (bijv. van leveranciers) eigen internet verbindingen worden opgezet, zonder gebruik te maken van de netwerkfuncties die door het bouwblok veilige netwerktoegang gerealiseerd zijn.
PAB-8b.09	Gegevens voor het monitoren en verbeteren van de beveiliging van het platform worden doorgegeven	Informatie welke gegenereerd wordt door netwerkvoorzieningen zijn cruciaal voor het kunnen monitoren en beveiligen van het platform. Alle voorzieningen in dit bouwblok moeten en/of mogen worden gebruikt voor het leveren van gegevens aan het bouwblok Security Services.

6.3 Gebruikte afkortingen en termen

In onderstaande tabel is voor specifieke afkortingen en termen aangegeven in welke betekenis ze in dit document worden gebruikt.

Afk.	Term	Beschrijving	Opmerking
ABAC	Attribute Based Access Control	(contextuele) kenmerken/attributen van deze personen (ABAC).	
ACID	Atomic, Consistent, Isolated, Durable	Atomic - Each transaction is either properly carried out or the process halts and the database reverts back to the state before the transaction started. This ensures that all data in the database is valid.	
AMZ-X.	Amsterdam Zorg Exchange (AmZX)	zorg (community-) netwerk	
API	Application Program Interface	API's zijn technische koppelvlakken binnen en tussen digitale informatiesystemen. Zij ontsluiten data en transacties: de data die door die systemen worden vastgelegd en de transacties die door die systemen worden uitgevoerd. Voor data en transacties worden aparte typen API's onderscheiden:	

		System-API’s: De data interfaces proces API’s: gegevens-toegang tussen de verschillende bouwblokken (verticaal) als tussen de elementen zoals microservices onderling binnen een bouwblok (horizontaal). Ook de gegevenstoegankelijk met en naar externe bronnen (in de Koppel Services) worden via process-API’s ingeregeld. experience API’s: leveren data in de combinaties die nodig zijn voor de verschillende kanalen, zoals mobiele apps, webformulieren e.d. Deze API’s zijn onderdeel van de Multi-Channel Presentatie Services.
ASP	Attribute service provider	Verzamelt, controleert en creëert gebruikerskenmerken binnen digitale ID's
BASE	Basically Available, Soft State, Eventual consistency	Deze eigenschap verwijst naar het feit dat het databasesysteem altijd beschikbaar moet zijn om te reageren op verzoeken van gebruikers, zelfs als het geen onmiddellijke toegang tot alle gegevens kan garanderen. De database kan korte perioden van onbeschikbaarheid ervaren, maar moet zo zijn ontworpen dat downtime tot een minimum wordt beperkt en snel herstel van fouten mogelijk is.
BCO	bron- en contactonderzoek	Het bron- en contactonderzoek is een belangrijke taak van de tbc (Tuberculose)-bestrijding en wettelijk vastgelegd in de Wet publieke gezondheid (Wpg (Wet publieke gezondheid)).
BiSL	Business Information Services Library	Voorheen Business Information Service Management Library, is een raamwerk voor het uitvoeren van functioneel beheer en informatiemanagement.
BIV	Beschikbaarheid / Integriteit / Vertrouwelijkheid	BIV classificatie, Engels: CIA
BOM	Bill of Material	OWASP Bill-of-Material bron: https://cyberveilignederland.nl/woordenboek
BRQ	LFI Business Requirements (BRQ)	Eisen die de LFI stelt aan Pandemische Paraatheid.
BSN	Burger service nummer	Het burgerservicenummer (BSN) is uw eigen persoonsnummer voor contact met de overheid. Bijvoorbeeld voor zorg of belastingen.
BuRst	back-up- en restore	Kopie van computergegevens die elders zijn genomen en opgeslagen, zodat deze kunnen worden gebruikt om het origineel te herstellen na een geval van gegevensverlies
CA	Conditional Access	Met Conditional Access (CA) wordt toegang tot applicaties en/of gegevens verleend of geweigerd op basis van attributen uit de context waarin toegang wordt gevraagd (zoals IP nummer, aanwezigheid van actuele anti-virus software op client device etc.) en die zijn vastgelegd in toegangspolicies (ABAC).
CI/CD	Continuous Integration and Delivery	Methode voor het frequent leveren van applicaties naar (eind)klanten waarbij vrijwel alle stappen geautomatiseerd zijn.
CMM	Capability Maturity Model	Model dat aangeeft op welk niveau de software - ontwikkeling van een organisatie zit.
CSP	Cloud Service Provider	Leverancier van (managed) cloud diensten
DAG	Data Access Governance	Data Access Governance (DAG) biedt de mogelijkheid om te identificeren welke ongestructureerde
DAP	Dossier Afspraken en Procedures	Type overeenkomst waarin de wederzijds overeengekomen samenwerking tussen klant en leverancier zijn vastgelegd rondom een afgenomen dienst of product.
DBaaS	Database as a Services	Clouddatabase-aanbod dat klanten toegang biedt tot een database zonder dat ze de onderliggende infrastructuur hoeven te implementeren en beheren.
DBMS	Database management systeem	Hiermee wordt een systeem aangeduid dat als database opgeslagen gegevens ontsluit, bewaakt en beheert.
DevOps	Development Operations	DevOps integreert en automatiseert het werk van software development (Dev) en IT operations (Ops)

DIZRA	Duurzaam Informatiestelsel Zorg ReferentieArchitectuur	Architectuurprincipes DIZRA (Manifest)
DNSSEC	Domain Name System Security Extensions	Domeinnaam (DNS) Security Reeks uitbreidingsspecificaties van de Internet Engineering Task Force (IETF) voor het beveiligen van gegevens die worden uitgewisseld in het Domain Name System (DNS) in Internet Protocol (IP)-netwerken.
ECD	Elektronisch Client Dossier	Zie ook: EPD
EDR	Endpoint Detection & Response	Cybersecurity technologie die voortdurend een "eindpunt" (bijv. mobiele telefoon, laptop, Internet-of-Things-apparaat) bewaakt om kwaadaardige cyberdreigingen te beperken.
EER	Europese Economische Ruimte	De EER is tot stand gekomen na een akkoord tussen de Europese Unie en de Europese Vrijhandels Associatie (zonder Zwitserland). Bij de Europese Economische Ruimte (EER) horen alle EU-landen plus Liechtenstein, Noorwegen en IJsland.
EHDS	European Health Data Space	De European Health Data Space (EHDS) is een voorstel van de Europese Commissie om snel en makkelijk medische gegevens te kunnen uitwisselen en burgers toegang te geven tot hun gezondheidsdata.
EID	Elektronisch identiteitsbewijs	Bedrijven en consumenten kunnen hiermee hun identiteit elektronisch bewijzen.
ELT / ETL	Extract Load Transform / Extract Transform Load	Driefasig proces waarbij gegevens worden geëxtraheerd, getransformeerd (opgeschoond, opgeschoond, geschrobd) en geladen in een uitvoergegevenscontainer.
EPD	Elektronisch Patient Dossier	Zie ook: ECD Softwaresysteem waarin medische gegevens digitaal bewaard en beschikbaar gemaakt worden voor zorgprofessionals in ziekenhuizen en de geestelijke gezondheidszorg (GGZ) rondom een patiënt.
EUDI	European Digital Identity	Met uw Europese digitale identiteit heeft u de nodige documenten meteen bij de hand, want die zijn lokaal opgeslagen in uw eigen digitale portemonnee, bijvoorbeeld op uw smartphone. U kunt digitale kopieën maken en veilig naar de bank sturen. De bank kan uw documenten meteen verifiëren en uw lening verder afhandelen.
HCI	Health Care Intelligence Platform	Combinatie van Databuffet, HCI regulier en Logbuffet
HLD / HLD IZB	High Level Design IZB	(Functioneel) ontwerp van het toekomstig landschap ten behoeve van Infectie ziektebestrijding en Pandemische Paraatheid. De term HLD wordt niet meer gebruikt. Het HLD is opgevolgd door de Doelarchitectuur IZB
IaaS	Infrastructure as a Service	Vorm van cloud computing. De infrastructuur wordt virtueel aangeboden. De hardware waaronder servers, netwerkapparatuur en de werkstations zijn eigendom van de serviceprovider. De afnemer betaalt alleen voor hetgeen daadwerkelijk gebruikt wordt.
IaC	Infrastructure as Code	proces van het beheren en inrichten van computerdatacenterbronnen door middel van machinaal leesbare definitiebestanden, in plaats van fysieke hardwareconfiguratie of interactieve configuratietools.
IAM	Identity and Access Management	Vrij vertaald het beheer om er voor te zorgen dat de juiste "identiteiten" (denk daarbij vooral aan personen of computers), voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste faciliteiten.
IdP	Identity Provider	Een identiteitsprovider (afgekort IdP of IDP) is een systeementiteit die identiteitsgegevens voor principals maakt, onderhoudt en beheert en ook verificatieservices levert aan vertrouwende toepassingen binnen een federatie of gedistribueerd netwerk
IDS	Intrusion Detection System	Geautomatiseerd systeem dat hackpogingen en voorkomens van ongeautoriseerde toegang tot een informatiesysteem of netwerk detecteert.

IDU	IDU (in-dienst/doorstroom/uit-dienst)	Het is een term die gebruikt wordt om de processen rondom de personeelscyclus van een organisatie te beschrijven.
IGA	Information Governance & Administration	In essentie gaat het bij IGA om het verhogen van de beveiliging en het verminderen van risico's door inzicht te bieden in wie toegang heeft tot welke systemen, bronnen, applicaties en waarom.
IoC	Indicators of Compromise	Signalen van vermoedelijk afwijkend gedrag
IPS	Intrusion Prevention System	Een IPS biedt bescherming tegen indringers van buitenaf en personen die zich al ergens in het netwerk bevinden.
ITIL	Information Technology Infrastructure Library	Referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie.
IZB	Infectie-ziektebestrijding (IZB)	Signalering, bestrijding en preventie van infectieziekten in Nederland
KPI	Key Performance Indicator	(KPI's) om procesevaluaties uit te voeren
LCI	Landelijke coördinatie infectieziektebestrijding	De Landelijke coördinatie infectieziektebestrijding coördineert zowel de bestrijding van infectieziekten in Nederland als de daarmee samenhangende communicatie om op landelijk en regionaal niveau
LCM	LifeCycle Management	LifeCycle Management is het proces van het beheren van de levenscyclus van een product. Het begint helemaal aan het begin van het product in de ontwerpfase en gaat door tot het einde van de levensduur of de buitengebruikstelling van het product. Er zijn verschillende soorten LifeCycle Management, zoals het beheer van de levenscyclus van applicaties in software, het beheer van de levenscyclus van gebouwen, het ontwerp en de bouw van gebouwen, engineering lifecycle management, een product- en softwareontwikkelingsplatform van IBM en beheer van de levenscyclus van informatie bij de opslag van computergegevens.
LFI	Landelijke Functie Opschaling Infectieziektebestrijding	De LFI heeft twee taken: 1. Opschaling en aansturing 2. Regie op de voorbereiding
LSP	Landelijk Schakelpunt	Regelt op een beveiligde manier het verkeer van berichten tussen zorgaanbieders en zorgverleners.
MDR	Managed Detection & Response	Combineert geavanceerde technologieën (zoals SIEM, EDR en NDR) en menselijke expertise om de organisatie beter te beschermen tegen cyberdreigingen.
MedMij	Medische Mij	MedMij is dé Nederlandse standaard voor het veilig uitwisselen van gezondheidsgegevens tussen zorggebruikers en zorgaanbieders.
MITZ	-	Mitz is een online toestemmingsvoorziening.
MP9	Informatiestandaard Medicatieproces 9	Set afspraken over eenduidige registratie en uitwisseling van medicatiegegevens
MPC	Multiparty Computation	Cryptografische techniek die meerdere partijen in staat stelt om bewerkingen uit te voeren op gegevens, op zo'n manier dat geen enkele partij iets leert dat verder gaat dan zijn eigen invoer en uitvoer van deze berekeningen.
MTLS	Mutual Transport Layer Security	Methode voor wederzijdse authenticatie.
NDR	Network Detection & Response (NDR)	Biedt een 360-graden kijk op netwerkverkeer. De technologie richt zich op het detecteren en reageren op verdacht gedrag binnen het netwerk.
NICTIZ	Nationaal ICT-Instituut in de Zorg	Nictiz is het competentiecentrum voor digitaal informatiemanagement in de zorg.
NOC	Network Operations Centre (NOC)	Stelsel van voorzieningen waar voortdurend de prestaties en gezondheid van een netwerk wordt bewaakt door preventieve, proactieve en reactieve operaties uit te voeren, om zo te beschermen tegen netwerkstoringen en -uitval.
NORA	Nederlandse Overheid Referentie Architectuur	De NORA richt zich op de publieke sector in het geheel en geldt dus voor alle domeinen en bestuurslagen. Afspraken in NORA maken samenwerken en informatie-uitwisseling mogelijk over bestuurslagen, ketens en domeinen heen.

NCSC	Nationaal Cyber Security Centrum (ncsc.nl)	Het NCSC is onderdeel van het ministerie van Justitie en Veiligheid. Als expert werkt NCSC aan een digitaal veilig Nederland. De digitale infrastructuur is van levensbelang: voor het betalingsverkeer, schoon water uit de kraan en om de voeten droog te houden.
OLAP	Online Analytical Processing	Technologie die wordt gebruikt om grote bedrijfsdatabases te organiseren en business intelligence te ondersteunen.
OLTP	Online Transaction Processing	Soort dataverwerking die bestaat uit het uitvoeren van een aantal transacties die gelijktijdig plaatsvinden, bijvoorbeeld tijdens online bankieren, winkelen, orderinvoer of het versturen van tekstberichten.
OWASP	Open Worldwide Application Security Project	In de OWASP top 10 staan de 10 grootste risico's op het gebied van beveiliging van webapplicaties. De OWASP top 10 wordt periodiek herzien. bron: https://cyberveilignederland.nl/woordenboek
PaaS	Platform as a Service	Vorm van cloudcomputing die als dienst wordt aangeboden, en biedt een platform aan waarmee klanten applicaties kunnen ontwikkelen, uitvoeren en beheren zonder de complexiteit van het bouwen en onderhouden van de infrastructuur die hier doorgaans mee samengaat.
PAM	Privileged Access Management	Een oplossing voor identiteitsbeveiliging die organisaties helpt beschermen tegen cyberdreigingen door ongeautoriseerde toegang tot kritieke resources te bewaken, te detecteren en te voorkomen.
PAW	Privileged Access Workstations	Speciale computeropstelling die speciaal is ontworpen voor taken die een verhoogde beveiliging vereisen.
PET	Privacy Enhanging Technologies	Technologieën die fundamentele principes voor gegevensbescherming belichamen door het gebruik van persoonsgegevens te minimaliseren en de gegevensbeveiliging te maximaliseren.
PP-IV	Pandemische Parate Informatie Voorziening	Naam van het programma om Pandemische Parate Informatie Voorziening te realiseren.
PQR	Post Quantum Readiness	Door Post Quantum cryptografie, gaat over het proactief ontwikkelen en bouwen van mogelijkheden om kritieke informatie en systemen te beveiligen tegen compromittering door het gebruik van quantum computers.
PURA	Publieke gezondheid Referentie Architectuur	Biedt een gedeelde basis om samen te bouwen aan een vraaggerichte informatievoorziening binnen de publieke gezondheid.
PvE	Programma van Eisen	Geschreven verzameling van eisen en wensen ten aanzien van een mogelijk te ontwerpen product, constructie, aan te schaffen dienst, of anderszins.
QoS	Quality of Service	
RBAC	Role Based Access Control	
RIVM		
RPO		
RTO		
SaaS		
SIEM	Security Information & Event Management	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
SLA		
SOC	Security Operations Center	
TLS		
TTM	Time To Market	
TTP / Data TTP	Trusted Third Party / Data Trusted Third Party	

UX	User experience	Presentatie (UX) voorzieningen
VDI	Virtual Desktop infrastructuur	
VPN	Virtual Private Network	VPN biedt de mogelijkheid om een beveiligde netwerkverbinding tot stand te brengen bij gebruik van openbare netwerken.
VVT		
VWS		
WAF	web application firewall	
WAP	web application proxy	
WCAG		
XDR	eXtended Detection and Response (XDR)	
XSOAR	Extended Security Orchestration, Automation and Response	
Z-CERT	Zorg- Computer Emergency Response Team	Z-CERT is a (CERT for institutions in the healthcare sector in the Netherlands
ZTNA	Zero Trust Network Access	ZTNA is een beveiligingsoplossing (gebaseerd op het Zero Trust Security model) die op een veilige manier toegang geeft tot applicaties en gegevens vanaf externe locaties.

6.4 Kengetallen ten tijde van pandemie

Omschrijving	Kengetal	Toelichting
Gelijktijdige burgers	10k	Burgers gelijktijdig actief op systemen.
Gelijktijdige gebruikers	10k-100k	Gebruikers van de systemen gelijktijdig actief tijdens pandemie.
Aantallen afspraken per dag	1 miljoen	In crisissituaties zullen wellicht tot 4 miljoen afspraken per week moeten worden verwerkt Omdat afspraken niet gelijkmatig over de week verspreid zijn moeten de systemen in staat zijn 1 miljoen afspraken per dag te verwerken (aanmaken én afhandelen).
Operationeel	24x7	
Beschikbaarheid	99,99%	
Schaalbaar	Continu	De configuratie van de omgeving is zodanig dat deze meeschaalt met het gebruik. Gebruik kan (bij een uitbraak bijvoorbeeld) in korte tijd (enkele dagen) sterke fluctuaties vertonen.
Servicetijden Opdrachtnemer	Max 16 x 7	Servicetijden voor derdelijns ondersteuning zijn afhankelijk van de fase waarin de pandemie zich bevindt. In de crisis-fase is 7 dagen in de week 16 uur per dag service noodzakelijk.
Reactietijd bij kritische verstoringen	15 minuten	
Capaciteit ondersteuning en doorontwikkeling per maand	2.150 uur	De minimale beschikbare capaciteit in uren per maand van inzetbare medewerkers bij Opdrachtnemer voor deze opdracht voor ondersteuning, ontwikkeling, analyse en management van het team en de relatie met Opdrachtnemer.

Zwarte Woud 2
3524 SJ Utrecht
ggdghor.nl