Kaders bij het conceptueel model

Programma Pandemisch Parate Informatievoorziening (PP-IV)

Versiebeheer

VERSIE	DATUM	STATUS	AUTEURS	OMSCHRIJVING
0.1	22-5-2023	Concept	Rutger van der Poll Harry van Steenoven Holke Visser	Initiëel concept
1.0	02-06-2023	Publiceerbaar concept	Rutger van der Poll Harry van Steenoven Holke Visser	Gereed voor Marktconsultatie
1.1	20-06-2023	Bijgesteld concept		Opgeslagen werkversie bij aanpassing naam document in 'Conceptueel model Platform voor de Toekomst'
1.3	10-08-2023	Bijgesteld concept		Nieuwe werkversie t.b.v verwerken reviewcomments
1.4	09-09-2023	Bijgesteld concept		Nieuwe werkversie
1.5	13-10-2023	Bijgesteld concept		Nieuwe werkversie
1.5.1	15-12-2023	Bijgesteld concept	Rutger van der Poll Harry van Steenoven	Niet functionele eisen (hoofdstuk 3) aangescherpt t.b.v. PvE AIZ
1.5.2	17-01-2024	Bijgesteld concept	Rutger van der Poll	NORA principes 11, 13 en 14 toegevoegd
1.9	22-03-2024	Bijgesteld concept	Rutger van der Poll Harry van Steenoven	Versie ter goedkeuring
1.9.1	03-05-2024	Bijgesteld concept	Rutger van der Poll	BIO, CRA en Besluit vaststelling bewaartermijn logging opgenomen
1.9.2	14-05-2024	Versie voor aanbesteding	Rutger van der Poll	NEN7503, NEN7518, NEN7520, NEN7540, NTA 7516, ISO27017 en ISO27018 opgenomen

Inhoudsopgave

Referenties

Referenties Intern

Ref. nr.	Document	Versie	Auteur	Documentlocatie
IR002	High Level Design IZB	V1.1 / 27 september 2022	RIVM / GGDGHOR	intern
IR003	Visie op Informatiebeveiliging en Privacybescherming (IB&P)	V1.0 / 27 april 2021		intern
IR004	Doelarchitectuur Identity and Access Management	V1.0 / 18 oktober 2022	René Klarenbeek	intern
IR005	Kaderstelling privacy - dataplatform	V2.0 / 7 april 2023	Mart van Delzen	intern
IR007	HLD Vervolg	V0.91 / 20230222	RIVM / GGD GHOR NL	intern
IR008	Doelarchitectuur Informatievoorziening IZB.pptx	V0.9 / 20230713	RIVM / GGD GHOR NL	
IR012	Uitwerking iStrategie 2024-2027 GGD GHOR Nederland	januari 2024	CIO	Uitwerking iStrategie 2024 - 2027.pdf

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/
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

In deze bijlage zijn de kaders en niet-functionele eisen opgenomen horende bij het conceptueel model. Waar het conceptuele model richting geeft aan de manier waarop handen en voeten wordt gegeven aan de pandemische paraatheid (in de technische voorzieningen die ten grondslag liggen aan de processen van de GGD-en), geven deze kaders vooral aan waaraan moet worden voldaan bij die oplossing.

Dit document is een inventarisatie van de van toepassing zijnde kaders en (in een aantal gevallen) is een selectie gemaakt welke daarvan impact hebben op welke van de bouwblokken in het conceptueel model.

2 Kaders

Het platform dient te voldoen aan eisen die geformuleerd zijn in wetten, regelgeving, beleid, etc. "Kaders" is de algemene term die we gebruiken 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. We onderscheiden de volgende soorten kaders:

- Kaders publieke gezondheid;
- Zorg-ICT kaders (standaarden, normen);
- Overheidskaders (Wet- en regelgeving, overheidsbeleid);
- Europese kaders;
- Privacy en security kaders.

2.1 Kaders Publieke Gezondheid

2.1.1 Uitwerking iStrategie 2024-2027 GGD GHOR Nederland

Op technologisch vlak realiseren we als sector publieke gezondheid een landelijke, duurzame en goed beheerde IT-infrastructuur dat als technisch fundament dient voor landelijke generieke zorg- en bedrijfsapplicaties van ons bovenregionale IV- en datalandschap.

De generieke basisvoorzieningen van dit technisch fundament, de zogeheten digitale snelweg bevatten basisvoorzieningen met betrekking tot:

- **Veilige toegang**: veiligheid
- **Cloud**: schaalbaarheid en beschikbaarheid
- **Externe koppelvlakken**: uitwisselbaarheid
- **Fysieke netwerken**: uitwisselbaarheid en veiligheid
- **Security-diensten**: veiligheid en beschikbaarheid
- **Privacy-diensten**: waarborging van persoonsgegevens

Om de generieke basisvoorzieningen te ontwikkelen, implementeren, beheren en vernieuwen is passende dienstverlening nodig.
In de vorm van een platform voegen we extra generieke voorzieningen toe aan de informatievoorziening van de GGD'en zowel in reguliere als in opgeschaalde situaties. Dit platform bestaat uit een aantal basisvoorzieningen en servicevoorzieningen:

2.1.1.1 BASISVOORZIENINGEN

De basisvoorzieningen maken de landelijke IV-ondersteuning van onze primaire processen in de diverse werkvelden mogelijk. Ons gemeenschappelijke bovenregionale digitale samenwerkingsplatform om veilig te werken met data en applicaties, bevat vier basisvoorzieningen:

- **GGD Digitale identiteit**: veilige toegang tot GGD-systemen voor medewerkers en ketenpartners
- **GGD Digitale Werkplek**: veilige digitale toegang tot applicaties en data
- **GGD Connect**: koppelvlakken voor GGD'en en ketenpartners én koppeling naar PGO's voor burgers
- **GGD Dataservices**: generieke datadiensten om te gebruiken met lokale en authentieke brondatasets van GGD'en

2.1.1.2 GGD SHARED SERVICE ORGANISATIE

De GGD Shared Service Organisatie (GGD SSO) ingericht bij GGD GHOR Nederland, levert de gezamenlijke IV-diensten op basis van beheer en onderhoud, leveranciersmanagement, inkoop, contractmanagement, diensten en servicelevels tegen een marktconforme prijs. De Shared Service Organisatie richt ook een beheerorganisatie in, waarbij beheer in een opgeschaalde situatie ook door een andere partij kan worden uitgevoerd.

2.1.1.3 GGD CLOUD COMPETENCE CENTER

Het GGD Cloud Competence Center (GGD CCC) is een multidisciplinair team van professionals. Dat team ondersteunt organisaties op strategisch, tactisch en operationeel niveau bij het adopteren van en werken in de cloud. Het CCC is ook de centrale plek waar expertise over en afstemming tussen IV- en IT-teams samenkomen. Op die manier worden professionals optimaal bediend en is er transparante controle op veiligheid en kosten.

2.1.1.4 GGD SECURITY OPERATIONS CENTER

Het GGD Security Operations Center (GGD SOC) monitort de computer- en netwerkactiviteiten in een organisatie. Log-informatie van applicaties en apparaten in het bedrijfsnetwerk wordt verzameld en onderzocht op afwijkende zaken. Hier draait het dus om relevante informatie over de beveiliging van alle systemen en apparaten en het monitoren van gebruiksgedrag en -risico's. Alle informatie leidt tot inzicht in hoe veilig de medewerkers, het netwerk, de systemen en hard- en software in de organisatie functioneren.

Met het platform wordt deze bouwsteen gerealiseerd. Initieel ter ondersteuning van de gezamenlijke IZB-data en applicaties, later ook voor de andere domeinen van de publieke gezondheid.

2.1.2 LFI Business Requirements

De LFI (Landelijke Functionaliteit Infectieziektebestrijding) wordt een nieuwe, landelijke crisisorganisatie die ervoor gaat zorgen dat Nederland een toekomstige pandemie beter kan bestrijden. Hierbij werkt zij nauw samen met GGD-en (Gemeentelijke Gezondheidsdienst) en andere partijen uit de infectieziektebestrijding, andere departementen, veiligheidsregio's en gemeenten. De LFI is ondergebracht bij het RIVM.

Zodra de LFI is opgericht, gaat zij 2 dingen doen:

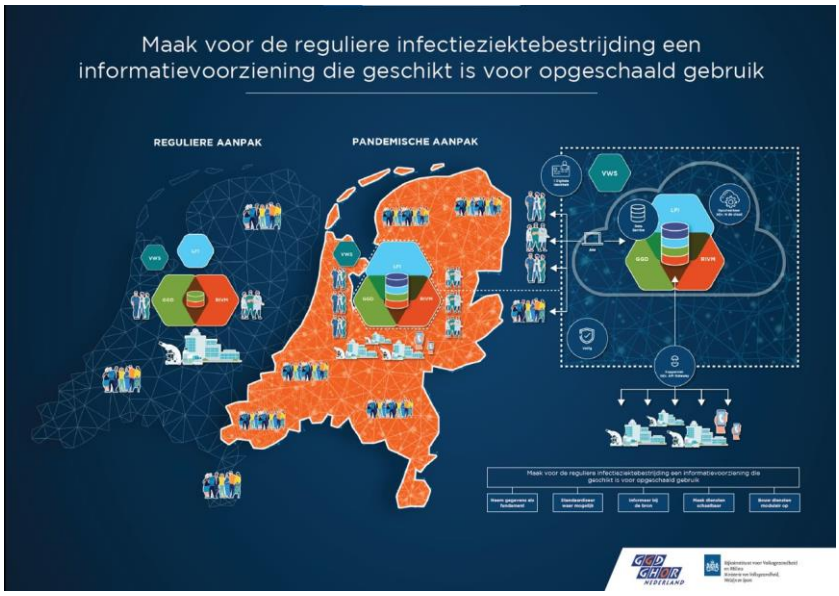
1. Bij een nieuwe pandemie zorgt de LFI voor snelle opschaling en aansturing van de medisch-operationele processen. Hiervoor stuurt de LFI tijdens een nieuwe pandemie de 25 GGD-en namens de minister van VWS (Ministerie van Volksgezondheid, Welzijn en Sport) centraal aan.

2. De LFI regelt dat de medisch-operationele processen centraal worden voorbereid. Dankzij deze duidelijke, landelijke aansturing kan Nederland een toekomstige pandemie slagvaardiger bestrijden. De al bestaande organisaties blijven de huidige COVID-19-pandemie bestrijden.

De LFI is midden 2023 operationeel. Vanuit de LFI zijn Business Requirements opgeleverd [REF:ER014].

2.1.3 High Level Design IZB / Doelarchitectuur Informatievoorziening IZB

Vanuit het programma Verbinden & Versterken is in samenwerking met LFI en RIVM een gezamenlijk Doelarchitectuur Informatievoorziening IZB [REF:IR008] opgesteld (voorheen: High Level Design (HLD) [REF:IR002]) voor het IV-platform ten behoeve van Infectie Ziekte Bestrijding (IZB) in reguliere en pandemische situaties.



De doelarchitectuur is gebruikt als opdrachtbeschrijving voor het ontwerp van een generiek platform vanuit het programma Pandemisch Parate Infectieziektebestrijding (PP-IV).

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

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

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

De doelarchitectuur stelt functionele en niet-functionele eisen aan het platform:

- Het IV-landschap is aantoonbaar schaalbaar, wendbaar, robuust en betrouwbaar;
- Gegevensuitwisseling digitaal, geautomatiseerd en gestandaardiseerd binnen het (pandemisch) zorgnetwerk, d.w.z. met alle ketenpartners;
- Processen met een nationaal of internationaal karakter zijn uniform en lokaal uitbreidbaar en worden ondersteund door IV;

- Gegevenskwaliteit wordt continu en geautomatiseerd bewaakt;
- ICT-landschap is voorbereid op digitale dienstverlening aan burgers. De 'burger'-reis kan flexibel worden ondersteund;
- Generieke (voor alle GGD-en) & specifieke (voor afzonderlijke GGD-en) functies kunnen vanuit één platform worden geserviced;
- Alle functies t.b.v. security, privacy & compliance vallen binnen controle van de uitvoerende organisaties. Dit betekent dat de GGD-en security, privacy & compliance voor de gezamenlijke voorzieningen dienen te organiseren.

2.1.4 PURA (NORA)

PURA is de referentie architectuur voor de Publieke Gezondheid. De PURA is een nadere uitwerking van de NORA.

Zie: https://www.noraonline.nl/wiki/PURA_(Publieke_gezondheid_Referentie_Architectuur)

NORA is de Nederlandse Overheid Referentie Architectuur. De NORA definieert 5 kernwaarden van dienstverlening (Vertrouwen, Veilig, Toekomstgericht, Doeltreffend, Doelmatig) met bijbehorende kwaliteitsdoelen en architectuurprincipes.

Zie: https://www.noraonline.nl/wiki/Kernwaarden_van_Dienstverlening

In de doelarchitectuur zijn 5 principes aangewezen die richtinggevend zijn voor het platform. Om te voldoen aan privacy en security by design zijn de 3 bijhorende principes ook geselecteerd. In onderstaande tabel zijn deze principes en bijhorende implicaties opgenomen.

NORA					
Princi-pe nr	Princi-pe	Stelling	Rationale	Implicatie nr	Implicatie
NAP07	Bouw dienste n modul air op	Maak bij de ontwikkeling van diensten gebruik van een modulaire indeling met een maximale interne samenhang en minimale externe koppelingen.	Door diensten modulair op te bouwen en te ontkoppelen wordt de flexibiliteit vergroot, wat leidt tot meer wendbaarheid, meer hergebruik en duurzaamheid.	NAP07.01 Organisatorisch	Diensten vullen elkaar aan
				IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie
				IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag
				IMP031 Informatie	Ontwerp op modulaire wijze
				IMP029 Organisatorisch Informatie Applicatie	Scheid proces van data
				IMP030 Informatie	Scheiding van datasets
				IMP087 Applicatie	Verwerk bericht-interactie persistent
				IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's
				IMP039 Grondslagen	Zorg voor open specificaties
NAP08	Standa ardise er waar	Standaardise er waar het kan, maak specifiek	Standaardisatie reduceert variëteit en kosten, en zorgt voor een betere	IMP034 Grondslagen	Gebruik de standaard met het meest specifieke werkingsgebied

	mogelijk	waar het moet.	interoperabiliteit en beveiliging. Hiermee komt bovendien een grotere wendbaarheid tot stand. Door te kiezen voor open standaarden wordt vendor lock-in voorkomen.	IMP035 Organisatorisch	Gebruik een actueel register met standaarden
				IMP038 Informatie	Gebruik gestandaardiseerde referentiedata
				IMP075 Organisatorisch	Gebruik open standaarden voor modellering
				IMP089 Organisatorisch	Gebruik standaard oplossingen
				IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk
				IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS
				IMP076 Organisatorisch	Maak afspraken over nieuwe (en oude) versies van standaarden
				IMP026 Organisatorisch	Pas je eigen proces en organisatie aan aan de standaard oplossing
				IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe
				IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden
NAP10	Neem gegevens als fundament	Gebruik gegevens als fundament voor het ontwerp, realisatie en doorontwikkeling van de dienst en richt het beheer hiervan goed in.	De kwaliteit en toegankelijkheid van gegevens bepaalt de waarde van de dienst. De onderliggende gegevens kennen meestal een veel langere levenscyclus dan de systemen waarin deze verwerkt worden. Als gegevens op duurzame wijze toegankelijk zijn gemaakt voor mens én machine kunnen deze gegevens dienen als fundering voor verschillende diensten in verschillende toepassingen, door de tijd en over de hele keten heen. Daarom is het essentieel dat het beheer van gegevens in de keten	IMP001 Informatie	Beschrijf informatieobjecten in een model
				IMP021 Organisatorisch Informatie Applicatie	Bevorder hergebruik van gegevens
				IMP049 Informatie	Draag zorg voor juiste en actuele en volledige informatie
				IMP044 Grondslagen	Hanteer bewaartermijnen voor informatie
				IMP051 Informatie	Leg auditlogs vast bij de bronregistratie van het gegeven
				IMP048 Informatie	Leg de context van een informatieobject vast in metadata
				IMP050 Informatie	Maak gegevens herleidbaar tot de bron (herkomst)
				IMP003 Grondslagen Informatie	Maak zoveel mogelijk data beschikbaar als open data
				IMP047 Informatie	Pas de FAIR dataprincipes toe
				IMP052 Applicatie	Sla informatie op in een duurzaam toegankelijk bestandsformaat

			op orde is, vanaf het ontstaan ervan tot en met de vernietiging (conform bewaartermijnen).	IMP073 Informatie	Stel van ieder gegeven de kwaliteit vast
				IMP058 Informatie	Stel voor ieder gegeven de unieke bron vast
				IMP046 Organisatorisch	Stel één verantwoordelijke vast voor ieder gegeven
				IMP002 Informatie	Voorkom verlies van informatie
NAP12	Informeer bij de bron	Maak bij de dienst gebruik van gegevens die afkomstig zijn uit een bronregistratie.	Voor betrouwbare dienstverlening is het hergebruik van de juiste informatie en documenten van cruciaal belang. Om de kwaliteit over de juistheid van een gegeven te borgen, moet duidelijk zijn welke organisatie bepaalt wat de juiste informatie is. Uitgangspunt is dat er voor gegevens waar de overheid gebruik van maakt, altijd één bron bestaat, die leidend is.	IMP060 Applicatie	Bepaal autorisaties met metadata
				IMP021 **(herhaling)** Organisatorisch Informatie Applicatie	Bevorder hergebruik van gegevens
				IMP059 Informatie	Geef de voorkeur aan halen i.p.v. brengen van gegevens
				IMP055 Organisatorisch	Gegevens eenmalig uitgevraagd, uniek opgeslagen, meervoudig gebruikt
				IMP033 **(herhaling)** Applicatie	Koppel bronsystemen op basis van een passende classificatie
				IMP056 Organisatorisch Informatie	Registreer gegevens bij de bron
				IMP077 Organisatorisch	Stel de juridische aansprakelijkheid per gegevensobject vast
				IMP058 **(herhaling)** Informatie	Stel voor ieder gegeven de unieke bron vast
				IMP007 Informatie	Verwijs naar de bron
				IMP057 Informatie	Weet welke (bron)gegevens in huis zijn
NAP15	Maak diensten schaalbaar	Bereid de dienst voor op veranderende werklast of reikwijdte.	Een schaalbare dienst kan omgaan met zowel verwachte als onverwachte intensivering of extensivering. Dit waarborgt de beschikbaarheid van de dienst en hiermee ook de wendbaarheid. Het voorkomt het ad hoc en onder hoge tijdsdruk realiseren van het opschalen van de dienst.	IMP085 **(herhaling)** Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS
NAP11	Pas doelbinding toe	Geef burgers en bedrijven de zekerheid dat informatie over hen alleen wordt gebruikt voor	Afspraken over het gebruik van informatie zijn nodig voor een vertrouwen in de dienstverlening. Door informatie niet te gebruiken voor andere processen of	IMP045 Grondslagen	Leg de doelbinding vast in de metadata van het gegevensobject
				IMP054 Informatie	Leg de grondslag en het doel van de gegevensverwerking vast

		de doelen waarvoor deze oorspronkelijk is verzameld.	diensten binnen de overheid, wordt zekerheid naar burgers en bedrijven geboden.	IMP004 Grondslagen Informatie	Minimaliseer het gebruik van gegevens
				IMP022 Grondslagen	Neem oorspronkelijke grondslag mee bij hergebruik diensten
				IMP032 **(herhaling)** Informatie	Ontwerp diensten met oog voor doelbinding en grondslag
				IMP053 Organisatorisch	Stel betrokkenen op de hoogte van het doel waarvoor gegevens verzameld worden
				IMP077 **(herhaling)** Organisatorisch	Stel de juridische aansprakelijkheid per gegevensobject vast
NAP13	Beheers risico's voortdurend	Maak in alle stappen van ontwerp en doorontwikkeling van de dienst de risico's inzichtelijk en stuur op een afgewogen beheersing ervan.	Wanneer helder in beeld is welke gevaren en bedreigingen van toepassing zijn voor de dienst, kun je gepaste beheersmaatregelen nemen. De manieren waarop componenten kunnen falen of hoe er misbruik van kan worden gemaakt zijn onderdeel van de risicoanalyse. Telkens kan dan de afweging worden gemaakt in welke mate de kosten en inspanningen van verdere mitigatie in verhouding staan tot de gevolgen als een risico zich voordoet. De bereidheid van de overheidsdienstverlener om restrisico's te accepteren maakt onderdeel uit van de afweging. Door risico's tijdig te onderkennen zijn beheersmaatregelen effectiever en efficiënter te implementeren.	IMP063 Organisatorisch	Bepaal de continuïteitseisen
				IMP078 Organisatorisch	Bewaak de continuïteit en stel een calamiteitenplan op
				IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen
				IMP080 Informatie	Controleer de verwerking van gegevens
				IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen
				IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen
				IMP085 **(herhaling)** Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS
				IMP015 Applicatie	Maak beveiligingsmaatregelen zo gebruiksvriendelijk mogelijk
				IMP061 Organisatorisch	Reduceer rest-risico's
				IMP070 Netwerk	Segmenteer het netwerk
				IMP064 Applicatie	Stel onweerlegbaarheid vast
				IMP084 Applicatie	Versleutel gegevens in rust en transport
				IMP086 Applicatie Netwerk	Zorg dat software up-to-date is
NAP14	Verifieer altijd	Verifieer doorlopend de juiste werking van de componenten en	Vertrouwen in het service-niveau van een overheidsdienstverlener, in de beschikbaarheid van een dienst, in de	IMP069 Netwerk	Hanteer het zero-trust model
				IMP019 Organisatorisch	Maak stelselafspraken over identificatie en authenticatie
				IMP068 Applicatie	Maak toegang tot applicaties en

		beheersmaatregelen van de dienst.	betrouwbaarheid van informatie, in de werking van een component, of de adequaatheid van beheersmaatregelen, is alleen gerechtvaardigd als de componenten en beheersmaatregelen van de dienst doorlopend wordt geverifieerd.		gegevens afhankelijk van authenticatieniveau
				IMP066 Applicatie	Richt een sterke logging en audit-trail in
				IMP070 **(herhaling)** Netwerk	Segmenteer het netwerk
				IMP064 **(herhaling)** Applicatie	Stel onweerlegbaarheid vast
				IMP065 Informatie	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces
				IMP067 Applicatie	Verifieer de werking van algoritmes
				IMP088 Applicatie	Verleen alleen strikt noodzakelijke toegangsrechten

2.2 Zorg-ICT kaders

2.2.1 NEN7510 – NEN7512 – NEN7513

Om invulling te geven aan de wetgeving (paragraaf 2.3) zijn Nederlandse Normen (NEN) opgesteld. NEN 7510 is een managementsysteemnorm, die een kader stelt voor het organiseren en borgen van informatiebeveiliging binnen een zorginstelling of toeleverancier. NEN 7512 (7510-2, 13.2) en NEN7513 (7510-2, paragraaf 12.4) zijn aanvullingen op (specifieke eisen uit) NEN 7510. De norm biedt een integraal Nederlandstalig kader voor informatiebeveiliging, toegespitst op de Nederlandse situatie in de zorg.

GGD GHOR NL heeft informatiebeveiligingsbeleid en richtlijnen opgesteld om daarmee invulling te geven aan de NEN-normeringen en daarmee dus ook Europese richtlijnen, zoals de NIS-2.

2.2.1.1 NEN 7510 - Informatiebeveiliging in de zorg

NEN 7510 is de norm voor informatiebeveiliging in de zorg. Naast het borgen van kwaliteitscriteria, vereist de norm NEN 7510 dat informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging. De NEN 7510 is gebaseerd op internationale standaarden voor informatiebeveiliging, de ISO / IEC 27000-reeks.

Zie: https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg

2.2.1.2 NEN 7512 - Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling

NEN 7512 is een norm voor de vertrouwensbasis voor gegevensuitwisseling. NEN 7512 is van toepassing op de elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, met zorgverzekeraars en andere partijen die bij de zorg zijn betrokken. Deze norm is in twee opzichten een aanvulling op de richtlijnen die NEN 7510 aan organisaties in de zorg geeft voor hun informatiebeveiliging. In de eerste plaats richt deze norm zich op de zekerheden die partijen elkaar moeten bieden als voorwaarde voor vertrouwde gegevensuitwisseling. Ten tweede levert deze norm een nadere invulling voor een aantal van de richtlijnen van NEN 7510.

Zie: https://www.nen.nl/nen-7512-2022-nl-297137

2.2.1.3 NEN 7513 - Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers

NEN 7513 is een norm voor het vastleggen van acties op elektronische patiëntdossiers.

De in deze norm beschreven logging voorziet in de stelselmatige geautomatiseerde registratie van gegevens rond de toegang tot het patiëntdossier, die controle van de rechtmatigheid ervan mogelijk maakt. Deze norm biedt zorgaanbieders aanwijzingen voor het loggen en gebruik van de logging om te voldoen aan wettelijke verplichtingen en levert ontwikkelaars van informatiesystemen een aantal eisen waaraan hun systemen zullen moeten voldoen.

Zie: https://www.nen.nl/nen-7513-2018-nl-245399

2.2.2 NEN7503 - Gegevensuitwisseling in de zorg - Elektronische verwerking en uitwisseling van gegevens voor het voorschrijven en ter hand stellen van medicatie

NEN 7503 specificeert de use cases voor het voorschrijven en het ter hand stellen van medicatie en de daarvoor benodigde verwerking en uitwisseling van medicatiegegevens. NEN 7503 formuleert eisen voor zorgaanbieders om hiervoor de gecertificeerde informatiesystemen zorgvuldig in te zetten en te beheren. NEN 7503 specificeert daarnaast de eisen waaraan informatiesystemen en de elektronische berichtuitwisseling tussen voorschrijvers van medicatievoorschriften en verstrekkers van geneesmiddelen moeten voldoen.

Zie: https://www.nen.nl/nen-7503-2022-nl-294742

2.2.3 NEN7518 - Identificatie & authenticatie (in ontwikkeling)

Deze norm legt vereisten vast om de identificatie en authenticatie van zorgprofessionals te waarborgen bij het uitwisselen van patiëntengegevens. Het is van essentieel belang dat zowel patiënten als zorgprofessionals vertrouwen hebben in het correct uitwisselen van de juiste patiëntinformatie. De norm legt geen verplichtingen op met betrekking tot openbare identificatie- en authenticatiemiddelen, maar het is mogelijk dat aanvullende eisen in de norm worden opgenomen die relevant zijn voor dergelijke voorzieningen.

Zie: https://www.nen.nl/egiz-werkgroep-nen-7518-identificatie-authenticatie

2.2.4 NEN7520 – Autorisatie (in ontwikkeling)

Geen nadere informatie gepubliceerd.

2.2.5 NEN7540 - BgZ-uitwisseling tussen instellingen voor medisch specialistische zorg

NEN 7540 specifieert twee usecases voor de uitwisseling van de BgZ tussen instellingen voor medisch specialistische zorg. De twee usecases zijn: uitwisseling BgZ bij verwijzing of overdracht en opvraging BgZ bij eerdere behandelaar. NEN 7540 formuleert eisen voor zorgaanbieders om hiervoor de gecertificeerde zorginformatiesystemen en elektronische uitwisselingssystemen zorgvuldig in te zetten en te beheren.

Zie: https://www.nen.nl/nen-7540-2024-nl-319920

2.2.6 NTA 7516 - Medische informatica - Eisen voor veilige e-mail en chatapplicaties (uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie)

NTA 7516 stelt functionele specificaties vast voor het veilig uitwisselen van persoonlijke gezondheidsinformatie tussen professionals onderling en tussen professionals en personen, bijvoorbeeld via e-mail. NTA 7516 is van toepassing op alle vormen van ad-hoc uitwisseling van persoonlijke gezondheidsinformatie tussen twee of meer mensen, waartoe e-mail, maar ook chatapplicaties (al dan niet aangeboden binnen een berichtenportaalfunctionaliteit) worden gerekend.

Zie: https://www.nen.nl/nta-7516-2019-nl-254878

2.2.7 MedMij

Stichting MedMij heeft regels gemaakt voor het veilig uitwisselen van medische gegevens. Persoonlijke gezondheidsomgevingen (PGO's) en zorgverleners met een MedMij-label volgen deze regels. Via MedMij kun je op een veilige manier een kopie van je medische gegevens in je PGO zetten.

Uit: Homepage van Stichting MedMij

MedMij is dé Nederlandse standaard voor het veilig en betrouwbaar uitwisselen van gezondheidsgegevens tussen burgers en gezondheidsprofessionals.

Uit: Factsheet-Veiligheid-september-2021.pdf (medmij.nl)

Impact: De relevante kaders zijn uit de publicaties van MedMij gedestilleerd en verwerkt in het hoofdstuk Kaders en implicaties per bouwblok.

2.2.8 Nationale visie en strategie op het gezondheidsinformatiestelsel

Uitgangspunt is dat de nodige medische gegevens beschikbaar zijn voor burgers, patiënten, zorgverleners, mantelzorgers, onderzoekers en beleidsmedewerkers om te gebruiken voor gezondheid, preventie en/of zorg.

Uiteindelijk moet deze visie ertoe leiden dat:

- Burgers kunnen meebeslissen over voor hen passende zorg en alle data beschikbaar hebben om dat te kunnen doen;
- Zorgverleners met de juiste data betere en veilige zorg kunnen leveren met meer mogelijkheden om gezondheid te bevorderen;
- Onderzoekers en beleidsmakers met de beschikbare data kennis kunnen vergroten en gefundeerd en effectief kunnen sturen.

Uit: Kabinet komt met Nationale Visie op het gezondheidsinformatiestelsel | Nieuwsbericht | Rijksoverheid.nl

Impact: De relevante kaders zijn uit de Nationale visie en strategie op het gezondheidsinformatiestelsel gedestilleerd en verwerkt in het hoofdstuk Kaders en implicaties per bouwblok.

2.2.9 Nictiz: Medicatieproces 9

In de standaard Medicatieproces 9 is een scheiding tussen logistieke en therapeutische informatie aangebracht en wordt voor het vastleggen en uitwisselen van gegevens uitgegaan van de vier stappen van het medicatieproces: voorschrijven, verstrekken, toedienen en gebruik.

Het functioneel ontwerp licht de verschillende werkstromen toe. De publicatie van ART-DECOR bevat een uitwerking van de dataset, scenario's met de bijbehorende waardesets. Ook de HL7 templates en het XML-materiaal zijn in deze publicatie beschikbaar.

Uit: Medicatieproces 9 2.0.0 - Nictiz

Impact: De relevante kaders zijn uit Nictiz: Medicatieproces 9 gedestilleerd en verwerkt in het hoofdstuk Kaders en implicaties per bouwblok.

2.2.10 Nictiz: API Requirements for Dutch Healthcare

Deze specificatie stelt eisen aan Application Programming Interfaces (API's) in de Nederlandse Gezondheidszorg. Het belang van het voldoen aan een gemeenschappelijke reeks eisen en dus de waarde van deze specificatie is om:

- Bevorder transparantie door duidelijke vereisten vast te stellen voor documentatie, testbaarheid, vindbaarheid en API-onboarding procedures en -overeenkomsten
- Harmoniseer API-vereisten en ontwerp tussen verschillende (nationale) programma's voor uitwisseling van gezondheidsinformatie en toegang van patiënten tot gezondheidsinformatie
- Garandeer een bepaald kwaliteitsniveau voor alle API's die zijn opgenomen in de Nederlandse API-bibliotheek voor de gezondheidszorg
- Innovatie bevorderen door de beschikbaarheid van systeemgegevens en door applicatiefunctionaliteit bloot te leggen

API's die voldoen aan de eisen in deze specificatie mogen worden opgenomen in de Nederlandse API-bibliotheek voor de zorg. API's die zijn opgenomen in de Nederlandse API-bibliotheek voor de gezondheidszorg zijn beter vindbaar en voldoen waarschijnlijk aan de vereisten in deze specificatie. Daarom voldoen ze aan een bepaald kwaliteitsniveau.
Deze specificatie is ontwikkeld als onderdeel van de Nictiz API-strategie.

Vertaald uit: [Introduction - API Requirements for Dutch Healthcare (nictiz.github.io)]

Impact: De relevante kaders zijn uit Nictiz: API Requirements for Dutch Healthcare gedestilleerd en verwerkt in het hoofdstuk Kaders en implicaties per bouwblok.

2.2.11 Ministerie van VWS: Actieplan Zorg-ICT-markt

Het Actieplan moet bijdragen aan de effectieve en efficiënte ICT-systemen die nodig zijn voor de verbetering van elektronische gegevensuitwisseling en (op termijn) databeschikbaarheid in de zorg. Sleutelwoorden in dit plan zijn openheid, transparantie, overheidsregie en minder vrijblijvendheid.

Het Actieplan is opgebouwd uit verschillende onderdelen, langs vier indelingsprincipes. Hierbij zijn uit het Actieplan het 'wie doet wat' de punten t.b.v. programma's en projecten, en ICT-leveranciers en hun vertegenwoordiging opgenomen:

1. Het gezondheidsinformatiestelsel & de zorg-ICT-markt;
   a. Landelijke Meerjarenagenda zorg-ICT-portfolio
      - Programma's en projecten: leveren specificaties aan van de ICT-eisen waaraan ICT-leveranciers moeten voldoen en de planning voor technische implementatie.
      - ICT-leveranciers en hun vertegenwoordiging: leveren landelijk niveau input op de Meerjarenagenda. Op sectoraal niveau participeren de relevante ICT-leveranciers bij het beoordelen van de haalbaarheid van ICT-eisen en planningen.
   b. Monitor zorg-ICT-markt
      - Programma's uit het zorg-ICT-portfolio: leveren informatie aan ten aanzien van het behalen van ICT-doelen uit de Meerjarenagenda, de mate waarin aan hun specificaties voldaan wordt.
      - Vertegenwoordigers van zorg-ICT-leveranciers: organiseren (gefaciliteerd door VWS) de aanlevering van informatie vanuit hun achterban ten aanzien van hun releaseplanningen in relatie tot de afspraken uit de sectorale ontwikkelagenda's.
   c. Communicatie
      - Koepels van leveranciers en zorgaanbieders: doorzetten communicatie naar hun achterban.
   d. Governance en vertegenwoordiging

- ICT-leveranciers: leveren vertegenwoordigers op strategisch en tactisch niveau en ondersteunen de feedback loop richting de diverse achterbannen. Borgen het leveren van informatie ten behoeve van onder andere Meerjarenagenda en monitor.

2. De vraagkant;
   a. (Cross)sectoraal leveranciersmanagement
      - Opdrachtgevers hierbij zijn de relevante koepels, gemandateerd door de sectorale zorgaanbieders en in samenwerking met sectorale leveranciers.
   b. (Academy) digitaal leiderschap
   c. Sturing op ICT-kwaliteit en betaalbaarheid via zorg inkoop
   d. Catalogus/marktplaats ICT-systemen
      - Leveranciers: publiceren van ICT-diensten en -producten.
3. De aanbodkant;
   a. Convenant/gedragscode
      - (Vertegenwoordiging van) ICT-leveranciers en zorgaanbieders: ondertekenen convenant met zelfbinding.
   b. (Juridisch) onderzoek naar verantwoorde winsten
      - ICT-leveranciers, Zorgaanbieders, EZK, ACM: input aanleveren voor onderzoek
4. De ICT-systemen.
   a. ZIB-transitie
   b. Onderzoek verplichting landelijk dekkend netwerk
   c. Strategie Data beschikbaar in openXis
      - ICT-leveranciers: aanleveren best practices, bijvoorbeeld ten aanzien van innovatie & sanering legacy; beoordelen van concept strategie.

Samenvattend wil VWS middels dit Actieplan in 2025 leveranciersmanagement in alle zorgsectoren ingeburgerd hebben. Door een nieuw op te richten jaarlijkse monitor wil VWS haar beleid op de zorg-ICT-markt in de gaten houden en evalueren.

Uit: Projectformat PID (overheid.nl)

2.2.12 Architectuurprincipes DIZRA (Manifest)

DIZRA is de afkorting voor Duurzaam Informatiestelsel Zorg Referentie Architectuur. Het is een van de familieleden van de NORA familie.

DIZRA is in opdracht van het Informatieberaad Zorg ontwikkeld. Het informatiestelsel is nodig om de zorg nog beter, betaalbaarder en toegankelijker te maken.

Het Informatieberaad Zorg heeft DIZRA vastgesteld. De Architectuurboard Zorg hanteert DIZRA als kader voor haar adviezen. In het proces van toelating van bouwstenen voor het informatiestelsel in de zorg stelt het Informatieberaad Zorg de DIZRA verplicht onder het regime van "pas toe of leg uit".

De zorg bouwt aan een duurzaam informatiestelsel. Een stelsel waarin data en services digitaal vindbaar, toegankelijk, uitwisselbaar en herbruikbaar zijn. DIZRA is de referentiearchitectuur voor dit informatiestelsel in de zorg. Het is een product van IT-Architecten voor IT-Architecten. Met DIZRA borgen we de samenhang en de duurzaamheid van het informatiestelsel, we delen kennis en verhogen de kwaliteit.

Dit doen we door het beschrijven van een manifest met uitgangspunten. Het manifest beschrijft de uitgangspunten voor het maken van architectuurkeuzes.

Uit: https://www.noraonline.nl/wiki/Duurzaam_Informatiestelsel_Zorg_ReferentieArchitectuur_(DIZRA)

Het manifest beschrijft onderstaande uitgangspunten:

- Regie op eigen gezondheidsgegevens voor cliënten;
- Gemeenschappelijke taal;
- Data bij de bron;
- Gelijk speelveld voor alle leveranciers;
- Duurzaam informatiestelsel;
- FAIR-data;
- Machine leesbaar;
- Federatief;
- Open internationale standaarden.

Uit: https://dizra.gitbook.io/dizra/manifest

Onderstaand wordt per uitgangspunt in deze paragraaf uitgewerkt:

- De impact op het programma en het te realiseren platform;
- De relatie met de NORA principes die aangewezen zijn in het HLD IZB.

De uitwerking is niet nader uitgesplitst over de verschillende bouwblokken, omdat de impact ook terugkomt in andere kaders.

In het informatiestelsel hebben cliënten **regie op hun eigen gezondheidsgegevens** en kunnen deze gegevens meenemen en delen in hun reis door het zorglandschap en in het netwerk van zorgverleners en ondersteuners dat zich rondom hen vormt.

- De impact op het programma en het te realiseren platform:
  - Het platform moet cliënten de mogelijkheid geven om hun eigen gezondheidsgegevens te delen met of te blokkeren voor zorgverleners en ondersteuners.
- Relatie NORA principes uit HLD IZB: geen
  - Wel behandeld in kaders Nationale visie en strategie op het gezondheidsinformatiestelsel.

In het informatiestelsel **spreken we een gemeenschappelijke taal** en hanteren gemeenschappelijke terminologie, waarbij we de contextuele verschillen omarmen.

- De impact op het programma en het te realiseren platform:
  - Het programma PP-IV levert onder andere een platform dat het mogelijk maakt de semantiek die in het domeinmodel gedefinieerd is te weerspiegelen.
  - Het platform maakt naast de levering van de data ook de levering van metadata over betekenis en gebruik van deze data mogelijk.
- Relatie NORA principes uit HLD IZB:
  - NAP 10: Neem gegevens als fundament

De **data blijft bij de bron**, onder de verantwoordelijkheid van de bronhouder, voor een veilig en vertrouwd informatiestelsel waarin het voor cliënten transparant is welke bronhouders welke gezondheidsgegevens registreren en wie het raadpleegt.

- De impact op het programma en het te realiseren platform:
  - Het platform bewaart data waarbij data onder verantwoordelijkheid van de bronhouder wordt bewaard.

    - Het platform dient bij gebruik zoveel mogelijk te verwijzen naar de bron i.p.v. kopie opslaan, comply or explain.
    - Het platform houdt een logregistratie bij over welke bronhouder welke gezondheidsgegevens registreert en wie het raadpleegt.
    - Het platform geeft cliënten toegang tot deze logregistratie over de eigen gezondheidsgegevens.
- Relatie NORA principes uit HLD IZB:
    - NAP 12: Informeer bij de bron

De bronhouder van cliëntgegevens is verwerkingsverantwoordelijke volgens de AVG.

Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordelijke-en-verwerker

Het informatiestelsel hanteert een **gelijk speelveld voor alle leveranciers**. Afspraken worden gemaakt over het gebruik van standaarden, niet over het gebruik van een product of dienst. Iedere organisatie kiest haar eigen leveranciers voor het implementeren van de standaarden.

- De impact op het programma en het te realiseren platform:
    - Het programma dient met de leveranciers afspraken te maken over het implementeren van standaarden niet over te leveren producten of diensten.
- Relatie NORA principes uit HLD IZB:
- NAP 08: Standaardiseer waar mogelijk

Het informatiestelsel is **duurzaam** doordat het relevant is en blijft. Het omarmt voor nu en in de toekomst de complexiteit van meerdere standaarden in een stelsel waarin verandering en innovatie welkom is.

- De impact op het programma en het te realiseren platform:
    - Platform dient de huidige ICT-standaarden voor de zorg te ondersteunen en aanpasbaar zijn voor nieuwe en gewijzigde standaarden.
    - Het programma dient om te kunnen gaan met de complexiteit van meerdere technische standaarden.
    - Het programma dient om te kunnen gaan met wijziging van technische standaarden.
- Relatie NORA principes uit HLD IZB:
    - NAP 08: Standaardiseer waar mogelijk

Data wordt enkelvoudig geregistreerd bij de bron en vervolgens beschikbaar gesteld voor meervoudig gebruik in verschillende toepassingen. Hiervoor hanteert het informatiestelsel de **FAIR-data** principes.

- De impact op het programma en het te realiseren platform:
    - Data dient beschikbaar gesteld te worden via API's en die dienen te voldoen aan de FAIR principes.
    - Het platform maakt eenmalige registratie bij de bron en meervoudig gebruik voor verschillende toepassingen mogelijk, rekening houdend met doelbinding.
- Relatie NORA principes uit HLD IZB:
    - NAP 10: Neem gegevens als fundament

Data is **machineleesbaar**, machines begrijpen de data, zonder daarbij de leesbaarheid van deze data voor mensen uit het oog te verliezen. Dit opent de mogelijkheden van data-analyse en data-science.

- De impact op het programma en het te realiseren platform:
    - De koppelservices van het platform dienen API's ter beschikking te stellen die machine leesbaar zijn.
- Relatie NORA principes uit HLD IZB:
    - NAP 10: Neem gegevens als fundament

In het informatiestelsel wordt **federatief** samengewerkt aan afspraken voor data en voor services. Iedereen implementeert deze afspraken en is aanspreekbaar op het nakomen van de afspraken en de kwaliteit van de implementatie.

- De impact op het programma en het te realiseren platform:
    - Maakt het mogelijk dat de "afspraken voor data en services" in het platform eenvoudig vertaald kunnen worden naar technische specificaties middels configuratie van het domein model en genereren van wijzingen op het platform.
    - De technologie voor het beheer van het domeinmodel ondersteunt een verticale data-architectuur die de consistentie tussen conceptueel en implementatiemodel bewaakt en deze inzichtelijk maakt voor audit doeleinden.
- Relatie NORA principes uit HLD IZB: geen

Semantische en technische interoperabiliteit wordt in het informatiestelsel gerealiseerd door te kiezen voor open internationale standaarden. Iedere deelnemer aan het stelsel moet voldoen aan de standaarden die zijn afgesproken.

- De impact op het programma en het te realiseren platform:
    - Het platform moet voldoen aan internationale technische standaarden, zoals IHE XDS, FHIR en REST.
- Relatie NORA principes uit HLD IZB:
    - NAP 08: Standaardiseer waar mogelijk

2.3 Overheidskaders

2.3.1 Wetgeving

Om invulling te geven aan de wetgeving zijn Nederlandse Normen (NEN) opgesteld. (paragraaf 2.2.1)

Voor de volledigheid zijn de onderkende wetten waaraan voldaan moet worden benoemd. Deze zijn niet verder uitgewerkt in het hoofdstuk kaders en implicaties per bouwblok.

2.3.1.1 WPG – Wet Publieke Gezondheid

De Wet publieke gezondheid regelt de organisatie van de openbare gezondheidszorg, de bestrijding van infectieziektecrises en de isolatie van personen/vervoermiddelen die internationaal gezondheidsgevaren kunnen opleveren. Ook regelt de wet de jeugd- en ouderengezondheidszorg.

Uit: https://www.rivm.nl/meldingsplicht-infectieziekten/wet-publieke-gezondheid

Zie: Wet publieke gezondheid

2.3.1.2 AVG – Algemene verordening gegevensbescherming

De Algemene verordening gegevensbescherming (AVG) regelt wat er allemaal wel en niet mag met de persoonsgegevens van mensen. Bij elk gebruik van persoonsgegevens geldt dat de privacy-inbreuk zo klein mogelijk moet zijn. De AVG regelt ook wat de privacy-rechten van mensen zijn als organisaties hun gegevens

verwerken. Bijvoorbeeld dat zij recht hebben op informatie over het gebruik van hun gegevens. En dat zij inzage en rectificatie van hun gegevens mogen vragen. De AVG bepaalt dat een organisatie alleen persoonsgegevens mag verwerken als daarvoor minimaal 1 grondslag is.

Uit: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

Zie: Uitvoeringswet Algemene verordening gegevensbescherming

2.3.1.3 WGBO - Wet op de geneeskundige behandelovereenkomst

Als patiënt heb je recht op informatie over je ziekte, de behandeling en de mogelijke gevolgen daarvan. Je mag alleen worden onderzocht en behandeld met jouw toestemming. Ook heb je recht op inzage in je medisch dossier. En dat zijn nog maar een paar rechten. Alle patiënten-rechten zijn vastgelegd in de Wet op de geneeskundige behandelovereenkomst (WGBO).

Uit: https://www.patientenfederatie.nl/over-de-zorg/patientenrechten

Zie: Afdeling 5 Burgerlijk Wetboek Boek 7

Conform de WGBO is het noodzakelijk dat alle instanties die medische dossiers verwerken aantoonbaar voldoen aan de normen van NEN-7510 en dat NEN-7512 en NEN-7513 als leidraad wordt gehanteerd.

2.3.1.4 WOO – Wet open overheid

De wet is bedoeld om overheden transparanter te maken en moet ervoor zorgen dat overheidsinformatie beter vindbaar, uitwisselbaar, eenvoudig te ontsluiten en goed te archiveren is. Op 1 mei 2022 is de Wet open overheid (Woo) in werking getreden. Het grote verschil tussen de huidige Woo en de WOB betreft de actieve openbaarmaking van overheidsinformatie.

Uit: https://www.digitaleoverheid.nl/wet-open-overheid/

Zie: Wet open overheid

2.3.1.5 Wegiz – Wet elektronische gegevensuitwisseling in de zorg

In de Wegiz staat dat gegevensuitwisseling tussen zorgaanbieders in sommige gevallen elektronisch moet verlopen. Het is nu vaak nog zo dat een dossier wordt overgetypt of dat een patiënt of cliënt meerdere keren zijn situatie aan zorgverleners moet uitleggen. Door elektronisch met elkaar uit te wisselen, gaat de informatie die nodig is voor de behandeling sneller en met minder kans op fouten van de ene zorgaanbieder naar de andere. En dat maakt het voor de patiënt en cliënt veiliger en makkelijker.

In de normen die worden ontwikkeld voor de gegevensuitwisselingen onder Wegiz, staan afspraken over taal en techniek. ICT-leveranciers moeten deze afspraken inbouwen in de systemen die zij voor de zorg ontwikkelen. Zij moeten hun producten en diensten op basis van deze normen laten certificeren.

Uit: https://www.gegevensuitwisselingindezorg.nl/wegiz

Zie: https://wetten.overheid.nl/BWBR0048095/2023-10-05

Vereisten van de Wegiz resulteren erin dat onder andere normenkaders NEN-7503 en NEN-7540 van toepassing zijn.

2.3.1.6 *Wabb - Wet algemene bepalingen Burgerservicenummer*

De Wabb introduceert het Burgerservicenummer (BSN) voor de klantcontacten tussen burger en overheid waarbij het gebruik van een persoonsnummer nodig is ten behoeve van eenduidige identificatie en registratie van personen en voor de gegevensuitwisseling tussen overheidsorganisaties onderling.

Voor het gebruik van het BSN in de zorg is het wetsvoorstel Wet gebruik Burgerservicenummer in de zorg.

Uit: https://www.eerstekamer.nl/wetsvoorstel/30312_wet_algemene_bepalingen

Zie: Wet algemene bepalingen Burgerservicenummer

2.3.1.7 *Wabvpz - Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg*

In de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) wordt het gebruik van het Burgerservicenummer (BSN) en bepaalde vormen van elektronische uitwisseling van medische gegevens tussen zorgverleners geregeld. Daarnaast geeft deze wet patiënten het recht om hun dossier elektronisch in te mogen kijken of er een afschrift van te ontvangen. Tenslotte zijn in de Wabvpz ook artikelen opgenomen over de logging.

Uit: https://www.avghelpdeskzorg.nl/onderwerpen/wabvpz

Zie: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

De wet schrijft voor dat aan NEN-7513 moet worden voldaan en dat middels NEN-7510 en NEN-7512 moet worden zorggedragen voor een veilig en zorgvuldig gebruik van elektronische uitwisselsystemen waarmee medische gegevens worden uitgewisseld.

2.3.1.8 *Wdo - Wet digitale overheid*

De Wet digitale overheid regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een substantiële of hoge mate van betrouwbaarheid. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. De wet stelt daarnaast open standaarden verplicht. Hiermee implementeert Nederland de Europese richtlijn over toegankelijkheid van overheidswebsites en apps.

Uit: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/

Zie: https://wetten.overheid.nl/BWBR0048156/2023-05-12/0

2.3.1.9 *Wbni - Wet beveiliging netwerk- en informatiesystemen (cybersecuritywet)*

De Cybersecuritywet strekt ter implementatie van de zogenoemde NIB-richtlijn van de Europese Unie (richtlijn 2016/1148).

Vanwege de inhoudelijke samenhang en overlap zijn de bepalingen van de Wet gegevensverwerking en meldplicht cybersecurity overgeheveld naar de Cybersecuritywet.

Uit: Cybersecuritywet - NORA Online

Zie: wetten.nl - Regeling - Wet beveiliging netwerk- en informatiesystemen - BWBR0041515 (overheid.nl)

2.3.1.10 *Wkkgz - Wet kwaliteit, klachten en geschillen gezondheidszorg; 'de kwaliteitswet*

Uit onderzoek blijkt dat mensen niet altijd tevreden zijn over de manier waarop zorgverleners hun klacht afhandelen. De afhandeling van een klacht duurt lang en gebeurt op een onpersoonlijke manier. Mensen willen zich gehoord voelen. En zij willen dat anderen in de toekomst niet hetzelfde overkomt.
Zorgverleners leren van klachten en ongewenste gebeurtenissen in de zorg. Doel van de Wkkgz is dan ook: openheid over klachten en ongewenste gebeurtenissen en ervan leren. Om zo gezamenlijk de zorg te verbeteren.

De wet regelt het volgende:

- Een betere en snelle aanpak van klachten
- Zorgmedewerkers kunnen veilig incidenten melden
- Cliënt krijgt sterkere positie
- Uitbreiding meldplicht zorgaanbieders

Uit: Wet kwaliteit, klachten en geschillen zorg (Wkkgz) | Kwaliteit van de zorg | Rijksoverheid.nl

Zie: wetten.nl - Regeling - Wet kwaliteit, klachten en geschillen zorg - BWBR0037173 (overheid.nl)

2.3.1.11 *WVR – Wet veiligheidsregio's*

De Wet veiligheidsregio's (Wvr) omvat bepalingen over de brandweerzorg, de rampenbestrijding, de crisisbeheersing en de geneeskundige hulpverlening.

De Wet veiligheidsregio's (Wvr) bepaalt de taken van het bestuur van een veiligheidsregio en stelt een aantal basiseisen aan de organisatie van de hulpdiensten en de kwaliteit van het personeel en het materieel.

Uit: https://nipv.nl/wet-veiligheidsregios/

Zie: wetten.nl - Regeling - Wet veiligheidsregio's - BWBR0027466 (overheid.nl)

2.3.1.12 *Archiefwet*

Archiveren van overheidsinformatie is niet vrijblijvend. De Archiefwet verplicht elke overheidsorganisatie om haar informatie duurzaam toegankelijk te maken en te houden, en te vernietigen wanneer de bewaartermijn is verlopen.

De Archiefwet bevat de kaders waarbinnen de verplichting ingevuld moet worden. Bijvoorbeeld welke informatie gearchiveerd moet worden (alles wat voortkomt uit de taken van de overheid), wie daar verantwoordelijk voor is (het bestuur dat ook verantwoordelijk is voor de taken), hoelang informatie bewaard wordt (dat wordt per organisatie vastgelegd in een selectielijst), wanneer overbrenging plaatsvindt (in principe binnen twintig jaar) en wie de informatie mag inzien (na overbrenging iedereen, tenzij iemands belangen daarmee geschaad worden). In aanvulling op de Archiefwet zijn in het Archiefbesluit en de Archiefregeling deze kaders nader uitgewerkt.

Uit: Archiefwet | Nationaal Archief

Zie: wetten.nl - Regeling - Archiefwet 1995 - BWBR0007376 (overheid.nl)

2.3.1.13 *Algemene Wet Bestuursrecht*

Algemene regels over de verhouding tussen bestuursorganen en belanghebbenden bij het voorbereiden, nemen en toepassen van besluiten.

Uit: Algemene Wet Bestuursrecht - NORA Online

Zie: wetten.nl - Regeling - Algemene wet bestuursrecht - BWBR0005537 (overheid.nl)

2.3.1.14 *Besluit digitale toegankelijkheid overheid*

Iedereen moet informatie en diensten van de overheid kunnen bereiken en gebruiken. Dat geldt ook voor digitale informatie en diensten. Daarom moeten de websites en apps van overheidsorganisaties verplicht toegankelijk zijn.

Uit: https://digitoegankelijk.nl/wetgeving

Zie: Tijdelijk besluit digitale toegankelijkheid overheid

2.3.1.15 *Wet Diaz - Wet digitale identificatie en authenticatie in de zorg*

Het wetsvoorstel legt de focus op veilige identificatie en authenticatie voor de zorg met behulp van inlogmiddelen die voldoen aan betrouwbaarheidsniveau hoog én een door de overheid beheerd register voor het verstrekken van identificerende kenmerken van zorgaanbieders en zorgmedewerkers. Hiermee krijgen zorgaanbieders en zorgmedewerkers keuze in welke inlogmiddelen zij gebruiken, zo kunnen zij kiezen voor een middel dat het beste past bij de betreffende werkzaamheden. De goedgekeurde inlogmiddelen beschikken over het betrouwbaarheidsniveau hoog. Deze inlogmiddelen kunnen ook worden gebruikt door zorgverzekeraars en indicatieorganen om het Burgerservicenummer van cliënten te raadplegen.

Het voornemen is om inlogmiddelen goed te keuren die zijn erkend onder de Wet digitale overheid, zoals DigiD, gecertificeerd zijn onder de NEN 7518 en die beschikken over een PKI-O-certificaat. Deze nieuwe veilig inlogmiddelen gaan op termijn de huidige UZI-middelen vervangen.

Uit: https://www.internetconsultatie.nl/wetdiaz/b1

Wettekst: https://www.internetconsultatie.nl/wetdiaz/document/11536

Beleidskompas: https://www.internetconsultatie.nl/wetdiaz/document/11537

2.3.1.16 *Wet Computercriminaliteit III*

De wet Computercriminaliteit III versterkt in het wetboek van Strafrecht (Sr) en het wetboek van Strafvordering (Sv) de opsporing en vervolging van computercriminaliteit. Hiermee is de wetgeving aangepast aan de technologische ontwikkelingen op internet en het gebruik van computers voor communicatie en de verwerking en opslag van gegevens. Ook worden burgers beter beschermd tegen bijvoorbeeld het verleiden van een minderjarige tot ontucht (grooming) of de verspreiding van kinderpornografie en ernstige computercriminaliteit.

Uit: Wet Computercriminaliteit III - NORA Online

Zie: wetten.nl - Regeling - Wijzigingswet Wetboek van Strafrecht, enz. (verbetering en versterking opsporing en vervolging computercriminaliteit (computercriminaliteit III)) - BWBR0041368 (overheid.nl)

2.3.1.17 *Wet BRP - Wet basisregistratie personen*

Authentieke bron voor persoonsgegevens van burgers en van buitenlanders die met Nederland te maken hebben. De Basisregistratie Personen (BRP) bevat persoonsgegevens over alle ingezetenen van Nederland en over personen die niet in Nederland wonen - of hier slechts kort verblijven - maar die een relatie hebben met de Nederlandse overheid, de 'niet-ingezeten'.

De BRP is gebaseerd op twee bestaande administraties:

- GBA (Gemeentelijke Basisadministratie Persoonsgegevens): Gegevens over personen ingeschreven bij een Nederlandse gemeente. De GBA heeft op dit moment al de status van een basisregistratie;
- RNI (Registratie Niet-Ingezetenen). Gegevens over personen die niet in Nederland wonen, maar wel een relatie met de Nederlandse overheid hebben. Zoals grensarbeiders, buitenlandse studenten en 'pensionado's'.

Uit: BRP (Basisregistratie Personen) - NORA Online

Zie: wetten.nl - Informatie - Wet basisregistratie personen - BWBR0033715 (overheid.nl)

2.3.1.18 *VIR - Besluit voorschrift informatiebeveiliging rijksdienst 2007*

Het Besluit voorschrift informatiebeveiliging rijksdienst (VIR) geldt voor de Rijksdienst waartoe gerekend worden de Ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.

Dit voorschrift geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Informatiebeveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen.

Zie: https://wetten.overheid.nl/BWBR0022141/2007-07-01

2.3.1.19 *VIRBI 2013 - Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (onder voorbehoud)*

Op de beveiliging van bijzondere informatie zijn de bepalingen van dit voorschrift als aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) van toepassing.

Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen, behoudt de toegekende rubricering en wordt beveiligd volgens het overeenkomstige nationale beveiligingsniveau. Voor zover voor de beveiliging van dergelijke informatie als gevolg van het verdrag of de overeenkomst afwijkende of verdergaande beveiligingsbepalingen bestaan worden deze bepalingen toegepast.

Het besluit is van toepassing wanneer informatie bij en van GGD'en wordt geclassificeerd als Departementaal VERTROUWELIJK (Indien kennisname door niet-geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries). Dit kan bijvoorbeeld van toepassing zijn bij medische- en (bijzondere) persoonsgegevens van militairen en PEP's (Politically Exposed Person/politiek prominent persoon).

Zie: https://wetten.overheid.nl/BWBR0033507/2013-06-01

2.3.1.20 *NIS2 - Network & Information Systems - richtlijn Netwerk en Informatiebeveiliging (NIB)*

De NIS2-richtlijn richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de richtlijn moet bijdragen aan meer Europese harmonisatie en een

hoger niveau van cybersecurity bij bedrijven en organisaties. De NIS2 is de opvolger van de eerste NIS-richtlijn, ook wel bekend als de NIB, die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

Uit: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie

2.3.2 Rijksbreed cloudbeleid 2022

Onder het nieuwe beleid mogen overheidsdiensten, met enkele uitzonderingen, onder voorwaarden publieke clouddiensten gebruiken.

Uit: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/08/29/kamerbrief-rijksbreed-cloudbeleid-2022

De Kaderstelling Privacy houdt naast wetgeving ook rekening met het Rijksbreed cloudbeleid 2022.

2.3.3 BIO - Baseline Informatiebeveiliging Overheid

Iedere overheidsorganisatie moet de Baseline Informatiebeveiliging Overheid (BIO) hanteren als basis voor informatiebeveiliging. De BIO beschrijft aan welke controls uit de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017 moet worden voldaan. Bij alle controls dient, op basis van een individuele risicoafweging, bepaald te worden hoe aan de beveiligingsdoelstelling van de control voldaan kan worden.

Uit: https://bio-overheid.nl/category/producten?product=BIO

2.3.4 Besluit vaststelling bewaartermijn logging

Besluit van de Minister voor Medische Zorg van 27 juni 2019, kenmerk 1529221-190512-WJZ, houdende vaststelling van een bewaartermijn voor logging

De Minister voor Medische Zorg en Sport,

Gelet op artikel 5, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders, [hier staat: Vertegenwoordigende organisaties van zorgaanbieders en patiënten stellen, in overleg met de Autoriteit persoonsgegevens, overeenkomstig het bepaalde in NEN 7513 de bewaartermijn voor logging vast en maken die bewaartermijn bekend in de Staatscourant binnen 6 maanden na de inwerkingtreding van dit besluit. Indien niet binnen deze termijn een bewaartermijn bekend is gemaakt, stelt Onze Minister van Volksgezondheid, Welzijn en Sport een bewaartermijn vast en maakt die bekend in de Staatscourant]
Besluit:

De logging als bedoeld in het Besluit elektronische gegevensverwerking door zorgaanbieders, wordt ten minste 5 jaar bewaard vanaf het moment dat de logregel wordt geschreven.

Uit: https://wetten.overheid.nl/BWBR0042391/2019-09-01 en https://wetten.overheid.nl/BWBR0040238/2020-10-01/#Paragraaf1_Artikel5

2.4 Europese Kaders

Binnen de Europese Unie zijn – mede naar aanleiding van de Corona pandemie - diverse initiatieven om uitwisseling van gegevens in de gezondheidzorg te standaardiseren en zo de uitwisseling eenvoudiger en sneller te maken.

Deze implementatie-details voor deze initiatieven zijn op dit moment nog voldoende bekend om in het conceptueel model op te nemen; het platform zal daarentegen wel voorzien in de mogelijkheid standaarden en koppelingen snel te implementeren, dus ook ten behoeve van genoemde initiatieven. Deze kunnen vervolgens snel over het hele platform geactiveerd worden.

In de volgende paragrafen zijn deze initiatieven – en mogelijke implicaties voor het platform kort beschreven

2.4.1 eID / EUDI Wallet

Het eID is een soort Europese DigiD: in een digitale portemonnee (EUDI (European Digital Identity) Wallet) worden alle belangrijke persoonsgegevens opgeslagen. Het idee is dat het daarmee voor alle EU-onderdanen gemakkelijker wordt een bankrekening in een andere lidstaat te openen of een auto te huren. In het kader van IZB en Pandemische Paraatheid kunnen hiermee bijvoorbeeld ook vaccinatie bewijzen via de wallet eenvoudiger internationaal gedeeld worden.

Ieder Europees land maakt zijn eigen wallet-app. Het Nederlandse systeem heeft voorlopig als naam NL Wallet gekregen.
Later worden de verschillende wallet-apps aan elkaar gekoppeld, waardoor ze overal binnen de EU werken.

Het uiteindelijke doel van de Commissie is dat alle EU-burgers in 2025 met hun eigen eID-app aan de slag kunnen. De bewaking van de invoering ligt in Nederland bij Logius, de organisatie die ook DigiD verzorgt.

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

2.4.2 European Health Data Space (EHDS)

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. Het voorstel bestaat uit drie onderdelen: primair datagebruik, secundair datagebruik en regulering van de zorg-ICT-markt.

Het voorstel voor het primaire gebruik van zorgdata stelt de burger centraal en geeft burgers rechten waarmee zij meer controle en zeggenschap krijgen op de toegang en het gebruik van hun elektronische gezondheidsgegevens voor de levering van zorg.

Het secundaire gebruik van zorgdata behelst het gebruik van elektronische gezondheidsgegevens voor andere maatschappelijke doelen. Denk hierbij aan wetenschappelijk onderzoek, innovatie en beleidsvorming.

Het derde onderdeel betreft de ontwikkeling van een interne markt voor digitale gezondheidsproducten en -diensten, zoals elektronische medische dossiersystemen. De commissie wil de regels voor (product-)veiligheid, beveiliging en interoperabiliteit binnen de EU harmoniseren. Zo denkt zij de effectiviteit en efficiëntie van de gezondheidszorg te bevorderen. De verordening beoogt om alle gezondheidsgegevens bij de bron te houden.

Uit: https://www.gegevensuitwisselingindezorg.nl/european-health-data-space-ehds

Op dit moment is de invloed minimaal. De European Health Data Space (EHDS) is als voorstel nog in beweging en kan vanwege de onderhandelingen met alle Europese lidstaten nog veranderen. Daarom worden er nu

geen aanpassingen in de Wegiz aangebracht. Zinspelen op eventuele invloeden brengt te veel onzekerheden met zich mee én zorgt voor jarenlange vertraging.

Minister Kuipers geeft aan de Wegiz pas aan te passen vanaf het moment van de inwerkingtreding van de use-cases (aangewezen gezondheidsgegevens) onder het EHDS-voorstel. Dit heeft als voordeel dat de Wegiz pas aangepast wordt als en wanneer het noodzakelijk is. De verwachting is dat meer wetgeving aangepast moet worden bij de implementatie van de EHDS, zoals gebruikelijk is bij Europese wetgeving.

Uit: https://icthealth.nl/nieuws/vws-beantwoordt-top-5-vragen-over-wegiz/

De prioritaire gegevensuitwisseling in onze eigen Wegiz en in de EHDS komen grotendeels overeen.
Het centrale doel van de EHDS komt opmerkelijk overeen met dat van het MedMij Afsprakenstelsel voor gegevensuitwisseling tussen zorgaanbieder en patiënt: mensen volledige zeggenschap geven over het gebruik en het delen hun medische gegevens

Uit: https://icthealth.nl/nieuws/theo-hooghiemstra-nu-is-de-tijd-om-de-ehds-te-verbeteren/

2.4.3 Cyber Resilience Act (CRA)

Van babyfoons tot smartwatches, producten en software die een digitale component bevatten, zijn alomtegenwoordig in ons dagelijks leven. Minder duidelijk voor veel gebruikers is het beveiligingsrisico dat dergelijke producten en software kan opleveren.

De Cyber Resilience Act (CRA) heeft tot doel consumenten en bedrijven die producten of software met een digitale component kopen of gebruiken, veilig te stellen. De wet zou zien dat ontoereikende beveiligingskenmerken tot het verleden behoren met de invoering van verplichte cyberbeveiligingsvereisten voor fabrikanten en detailhandelaren van dergelijke producten, waarbij deze bescherming zich gedurende de gehele levenscyclus van het product uitstrekt.

Het probleem dat in de verordening wordt aangepakt, is tweeledig.
Ten eerste is het ontoereikende niveau van cyberbeveiliging inherent aan veel producten, of ontoereikende beveiligingsupdates van dergelijke producten en software.
Ten tweede is het onvermogen van consumenten en bedrijven om op dit moment te bepalen welke producten cyberveilig zijn, of om ze zo in te stellen dat hun cyberbeveiliging wordt beschermd.

De Cyber Resilience Act garandeert:

- geharmoniseerde regels bij het in de handel brengen van producten of software met een digitale component;
- een kader van cyberbeveiligingsvereisten voor de planning, het ontwerp, de ontwikkeling en het onderhoud van dergelijke producten, met verplichtingen waaraan in elke fase van de waardeketen moet worden voldaan;
- een verplichting om zorgplicht te verlenen voor de gehele levenscyclus van dergelijke producten.

De verordening is aangekondigd in de EU-strategie voor cyberbeveiliging van 2020 en vormt een aanvulling op andere wetgeving op dit gebied, met name het NIS2-kader.

Zij is van toepassing op alle producten die direct of indirect op een ander apparaat of netwerk zijn aangesloten, met uitzondering van specifieke uitsluitingen zoals opensourcesoftware of diensten die reeds onder de bestaande regels vallen, wat het geval is voor medische hulpmiddelen, luchtvaart en auto's.

Uit: EU-wet inzake cyberweerbaarheid | Shaping Europe's digital future (europa.eu)

2.5 Privacy en security kaders

2.5.1 Kaderstelling Security

GGD GHOR NL heeft informatiebeveiligingsbeleid (IB-Beleid) en richtlijnen vastgesteld om daarmee invulling te geven aan alle kaders zoals geformuleerd in de Zorg-ICT-, Overheids- en Europese Kaders.

T.b.v. de maatregelen vanuit informatiebeveiliging zijn stellingen aangenomen (mei 2023) en voorzien van een dreigingsanalyse. De onderstaande set maatregelen moet gezien worden als een eerste set en zal worden uitgebreid naarmate de situatie zich ontwikkelt. De maatregelen zijn;

1. De leverancier zorgt voor een dynamisch en geautomatiseerd middelrapportage systeem van actieve componenten op het platform. Deze wordt meegestuurd in de logfeed naar het SOC van GGD GHOR Nederland.
2. De leverancier zorgt voor een verwerkingsrapportage systeem voor het gebruik van het platform door mensen en processen. Ook deze wordt meegestuurd in de logfeed naar het SOC van GGD GHOR Nederland.
3. Ongeautoriseerd gebruik van de data in het platform mag niet leiden tot herleidbare informatie (datalek).
4. Privilege Access Management (PAM) moet integraal onderdeel zijn van de registratie binnen het platform.
5. Retentie van data moet integraal opgesloten zitten in de data van het platform.
6. Het moet mogelijk zijn om autorisatie te koppelen aan eigen identity stores/brokers (ADFS/TiH) en aan externe digitale identiteit (DigiD, EU-initiatieven op dit vlak)
7. De leverancier levert een SBoM voor alle softwarecomponenten die zijn gebruikt. Zie Software Bill of Materials and Cybersecurity | Research | National Cyber Security Centre (ncsc.nl)
8. Ongeoorloofd gebruik van het Platform (onvoorzien gebruik) mag niet leiden tot dataexports. De leverancier heeft hier beveiligingsmiddelen voor ingebouwd. Wij zien hier graag een beschrijving van.
9. De leverancier is ISO27001 gecertificeerd en heeft 24x7 beheer en ontwikkel mogelijkheid.
10. De leverancier stuurt een voorbeeld SLA en DAP op die zij hanteren als 'de facto standaard' dat rekening houdt met, voor hen, externe SOC-diensten.
11. Leverancier heeft een of meerdere assurance verklaringen voor de producten die worden aangeboden.
12. Leverancier is aantoonbaar in control over zijn supply chain risico ten aanzien van hardware- en softwarekwaliteiten alsmede voorspelbare dienstverlening. Hij heeft hier een leveranciersrisicobeheersingsproces voor ingericht en geeft daar kennis van met een procesbeschrijving.
13. Leverancier is bereid om binnen 12 maanden na aanvang een accurance verklaring voor NEN7512:2022 aan te leveren. Voor de POS/POC fase is dit niet van toepassing.
14. Het versturen van informatie gebeurt altijd versleuteld.

2.5.2 Kaderstelling Privacy

Op basis van het beleid en richtlijnen is specifiek voor het programma PP-IV een Kaderstelling Privacy [REF:IR005] opgesteld. Onderstaande is een kopie uit deze kaderstelling. De kaderstelling bevat zelf ook de onderbouwing. Van de kaderstelling is een eerste impactbepaling gedaan, deze zijn opgenomen per bouwblok.

2.5.2.1 Basisprincipes AVG

Het dataplatform moet conform onderstaande basisprincipes van de AVG ingericht zijn.

Rechtmatigheid, behoorlijkheid en transparantie

Het dataplatform moet voorzien dat alle verwerkingen gebaseerd zijn op een juridische/wettelijke grondslag. Het dataplatform maakt inzichtelijk hoe en op welke manier data wordt verwerkt.

Doelbinding

Data in het dataplatform wordt alleen gebruikt voor het doel waarvoor de data is verkregen. Het dataplatform voorziet in een mogelijkheid om verdere verwerkingen pas na advies van de verwerkingsverantwoordelijke plaats te laten vinden. Het platform maakt het mogelijk om data die is verkregen op basis van toestemming te categoriseren dat deze niet is voor verdere verwerking.

Gegevensminimalisatie

Op het platform worden enkel persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken. Deze beoordeling vindt plaats door de verwerkingsverantwoordelijke. De privacy office biedt ondersteuning door te adviseren over de noodzakelijkheid van de verwerkingen.

Juistheid van gegevens

Het platform zorgt dat alle data die op het platform wordt verwerkt nauwkeurig en actueel is. Het platform controleert of data ontbreekt of foutief is.

Beperking van de opslag

Het platform voorziet in bewaartermijnen die automatisch worden gehanteerd. Het platform verwijderd data door deze te anonimiseren zodat aan de eisen van NEN7513 wordt voldaan.

Integriteit en vertrouwelijkheid

Het platform beschermt de persoonsgegevens door passende technische en organisatorische maatregelen welke zijn afgestemd met de afdeling security van GGD GHOR NL of de wensen van de GGD-en.

Verantwoordingsplicht

Het platform verantwoord de verwerkingen die op het platform plaatsvinden door de verwerkingsactiviteiten op te slaan, door datalekken te registeren, door DPIA's te verrichten en regels en procedures toe te passen voor de uitoefening van de rechten van de betrokkenen en de te nemen passende technische en organisatorische maatregelen.

2.5.2.2 Grondslagen

Het platform verwerkt persoonsgegevens enkel op basis van een rechtmatige grondslag van de AVG. Het platform zorgt dat elke verwerking van persoonsgegevens a priori is gecontroleerd door de verwerkingsverantwoordelijke. De privacy office van GGD GHOR NL heeft hierin een adviserende rol.

Verwerken van bijzondere persoonsgegevens

Het platform verwerkt alleen bijzondere persoonsgegevens wanneer een uitzonderingsgrond van artikel 9 lid 2 AVG van toepassing is. Het platform zorgt dat elke verwerking van bijzondere persoonsgegevens a priori is gecontroleerd door de verwerkingsverantwoordelijke. De privacy office van GGD GHOR NL heeft hierin een adviserende rol.

2.5.2.3 Rechten van betrokkenen

Het platform zorgt dat betrokkenen haar rechten op een eenvoudige wijze uit kunnen oefenen.

Informatieplicht

Aan de betrokkene moet duidelijk gemaakt worden welke persoonsgegevens verwerkt worden, waarom de organisatie dat doet, of de organisatie gegevens deelt met andere organisaties, hoelang de gegevens bewaard blijven en of de organisatie gegevens ontvangt van andere organisaties. Het platform communiceert door middel van een privacyverklaring al deze informatie richting de betrokkene.

Recht van inzage

Het platform moet via een digitale, beveiligde verstrekking de verwerkte persoonsgegevens van een betrokkene verstrekken. Deze verstrekking op een eenvoudige wijze toegang dit recht uit kunnen oefenen. Het platform verstrekt de informatie op een eenvoudige wijze en in begrijpbare vorm.

Recht op rectificatie

Het platform voorziet in een eenvoudige, laagdrempelige en snelle manier om persoonsgegevens te corrigeren. Het platform moet data een classificatie geven indien de juistheid daarvan door een betrokkene in twijfel wordt getrokken.

Recht op gegevenswissing (recht op vergetelheid)

Het platform is in staat waar noodzakelijk om binnen een aantal werkdagen een verzoek tot vergetelheid te honoreren. De verwijdering/anonimisering van persoonsgegevens vindt op een aantoonbare wijze plaats.

Recht op beperking van de verwerking

Het platform voorziet in een methode om een verwerking stil te leggen. Het platform informeert de ontvangers aan wie de persoonsgegevens openbaar gemaakt zijn van deze beperking.

Recht op gegevensportabiliteit

Het platform voorziet in een methode om binnen een maand medische dossiers van een betrokkene in een gestructureerd, veelgebruikt en machineleesbaar formaat aan betrokkene te verstrekken.

Burgerportaal

Het platform heeft een burgerportaal waar de betrokkene inzicht heeft in welke persoonsgegevens door de organisatie verwerkt zijn. In het portaal is logging zichtbaar waaruit blijkt op welke tijdstippen een persoon het dossier heeft geopend, welke functie deze persoon heeft en welke handelingen in het dossier zijn verricht.

Inloggen op een burgerportaal

Betrokkenen loggen via een beveiligde ingang in op het burgerportaal (DigiD of eIDAS of door de afdeling security ander gelijkgestelde inlogmethode).

Koppeling met het Landelijk Schakel Punt (LSP)

Het platform voorziet in een mogelijkheid om op wens van een betrokkene informatie te delen met het LSP.

2.5.2.4 Beveiliging van de verwerking

Het platform beschermt de persoonsgegevens door passende technische en organisatorische maatregelen welke zijn afgestemd met de afdeling security van GGD GHOR NL of de wensen van de GGD-en.

Monitoring en logging

Het platform logt medische gegevens conform NEN 7513. Het platform monitort en logt gegevens in real time. Loggegevens op medisch dossiers moeten twintig jaar bewaard blijven conform de eisen van artikel 15e Wabvpz.

2.5.2.5 *Privacy by design & Privacy by default*

Het platform wordt ontwikkeld met een zorgvuldige omgang met persoonsgegevens als fundamenteel principe (privacy by design). Het platform neemt daarvoor passende technische en organisatorische maatregelen.
Het platform stelt de standaardinstellingen in op de meest privacy-vriendelijke wijze (privacy by default).

Betrokkenheid van de privacy office, functionaris gegevensbescherming en regio's

Privacy by design en privacy by default wordt gewaarborgd doordat het platform de privacy office in elk stadium betrekt bij ontwikkelingen. Ook de functionaris gegevensbescherming(en) van GGD GHOR NL en de regionale GGD-en zijn betrokken.

Uitvoeren van DPIA's

Op alle modules van het platform zijn DPIA's uitgevoerd, waarmee de risico's voor de rechten van betrokkenen in kaart zijn gebracht.

Kennisgeving bij een inbreuk in verband met persoonsgegevens

Het platform heeft functionaliteiten waarmee bij een inbreuk op korte termijn (binnen 24 uur) te achterhalen is.

Bewaartermijnen

Het platform voorziet in bewaartermijnen die automatisch worden gehanteerd. Het platform verwijderd data door deze te anonimiseren zodat aan de eisen van NEN7513 wordt voldaan.

Registers

Vanuit het platform is het eenvoudig mogelijk om een verwerkingsregister te creëren die voldoet aan de wettelijke eisen.

Rol van de functionaris voor gegevensbescherming

GGD GHOR Nederland heeft volgens de wet een verplichting om een functionaris gegevensbescherming (FG) aan te stellen. Om de wettelijke taken van de FG mogelijk te maken verstrekt het platform aan de FG alle noodzakelijke informatie en middelen. Daarnaast is de FG betrokken bij de totstandkoming en ontwikkeling van het platform en de DPIA's over verwerkingen die in het platform plaatsvinden.

Mogelijkheid tot volgen van data

Het platform biedt een mogelijkheid om data uitwisselingen te traceren en in kaart te brengen.

Data access governance

Het platform is in staat het gebruik van gegevens te controleren, te beschermen en te auditen om de privacy te handhaven en te waarborgen.

2.5.2.6 *Eisen bij EPD*

Het platform implementeert de rechten van de cliënt en de plichten van de zorgaanbieder zoals gelden voor een EPD die voortvloeien uit de wettelijke eisen zoals opgenomen in boek 7 titel 7 afdeling 5 van het Burgerlijk Wetboek (Wet op de Geneeskundige Behandelingsovereenkomst), de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz), Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) en Wet algemene bepalingen Burgerservicenummer.

Verwijderverzoek conform WGBO

Het platform is in staat om binnen twee weken een verzoek tot verwijdering van het medisch dossier te honoreren. De verwijdering/anonimisering van persoonsgegevens vindt op een aantoonbare wijze plaats.

Verwerkers en sub-verwerkers

Partijen die een dienst verlenen voor het platform zullen conform de geldende eisen en afspraken van de GGD-en en GGD GHOR Nederland werken. Met elke partij is een verwerkersovereenkomst gesloten.

Wetenschappelijk onderzoek

Het platform beschikt over middelen om instanties toegang te geven tot specifieke gegevens van de database ten behoeve van wetenschappelijk onderzoek. Toegang wordt enkel verleend na toestemming van de verwerkingsverantwoordelijke(n). De gegevens die inzichtelijk zijn voor onderzoek zijn altijd gepseudonimiseerd of geanonimiseerd.

Publiekelijk cloudgebruik

Indien het platform (voor een deel) gehost wordt op een publieke host (bijvoorbeeld AWS), dan is dat conform de eisen uit het Rijksbreed Cloudbeleid, het implementatiekader risicoafweging cloudgebruik van 5 januari 2023 en de adviezen van de European Data Protection Board (EDPB).

3 Niet-Functionele eisen

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

3.1 Productkwaliteit (Product quality)

3.1.1 Functionele geschiktheid (Functional suitability)

De mate waarin een softwareproduct of computersysteem functies levert die voldoen aan de uitgesproken en veronderstelde behoeften, bij gebruik onder gespecificeerde condities.

3.1.1.1 Functionele compleetheid (Functional completeness)

De set van (platform-)functionaliteiten die alle gespecificeerde taken en gebruikersdoelen ondersteunen betreft het opgestelde HLD en de business requirements vanuit het LFI, welke als kader is opgenomen per bouwblok in het hoofdstuk Conceptueel Model.

3.1.1.2 Functionele correctheid (Functional correctness)

De uiteindelijk geleverde functies (software t.b.v. de infectieziektebestrijding en data uitwisseling met ketenpartners) worden geleverd vanuit het domeinmodel en de koppel services. Het domeinmodel wordt opgesteld met vertegenwoordigers van de GGD-en in samenwerking met het RIVM en zal zo bijdragen aan het beschikbaar stellen van de juiste resultaten met de benodigde nauwkeurigheid.

3.1.1.3 Functionele toepasselijkheid (Functional appropriateness)

De uiteindelijk geleverde functies (software t.b.v. de infectieziektebestrijding en data uitwisseling met ketenpartners) worden geleverd vanuit het domeinmodel en de koppel services. Het domeinmodel wordt opgesteld met vertegenwoordigers van de GGD-en in samenwerking met het RIVM en zal zo bijdragen aan het behalen van de IZB specifieke taken en doelen.

3.1.2 Prestatie-efficiëntie (Performance efficiency)

De prestaties in verhouding tot de hoeveelheid middelen gebruikt onder genoemde condities.

3.1.2.1 Snelheid (Time-behaviour)

De mate waarin antwoord- en verwerkingstijden en doorvoersnelheid van het platform tijdens de uitvoer van zijn functies moet voldoen aan de wensen, zoals geformuleerd in KPI's.

3.1.2.2 Middelenbeslag (Resource utilization)

De mate waarin de hoeveelheid en type middelen die gebruikt worden door het product of systeem tijdens de uitvoer van zijn functies moet voldoen aan de wensen, zoals geformuleerd in KPI's.

3.1.2.3 Capaciteit (Capacity)

De maximale limieten van de platform componenten dienen zodanig te zijn dat de componenten ten minste kunnen schalen naar de gestelde gewenste snelheid tijdens piekbelasting (pandemische situatie) zoals opgenomen in de LFI business requirements.

3.1.3 Uitwisselbaarheid (Compatibility)

De mate waarin een product, systeem of component informatie uit kan wisselen met andere producten, systemen of componenten, en/of het de gewenste functies kan uitvoeren terwijl het dezelfde hard- of software-omgeving deelt.

3.1.3.1 Beïnvloedbaarheid (Co-existence)

Door het gebruik van horizontaal en verticaal schaalbare cloud technologie en de vanuit de LFI business requirements gestelde piekbelasting tijdens een pandemie dient het platform zijn gewenste functies efficiënt uit te kunnen voeren zonder nadelige invloed op enig ander product.

3.1.3.2 Koppelbaarheid (Interoperability)

Doordat de GGD-en en het RIVM gezamenlijk een gemeenschappelijk domeinmodel opstellen waarin rekening wordt gehouden met alle ontwikkelingen op het gebied van interoperabiliteit en het inrichten van koppel services met o.a. een translatiefunctie zal het platform informatie kunnen uitwisselen en de uitgewisselde informatie kunnen gebruiken.

3.1.4 Bruikbaarheid (Usability)

De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om effectief, efficiënt en naar tevredenheid gespecificeerde doelen te bereiken in een gespecificeerde gebruikscontext.

3.1.4.1 Herkenbaarheid van geschiktheid (Appropriateness recognisability)

Doordat de GGD-en en het RIVM gezamenlijk een gemeenschappelijk domeinmodel opstellen waaruit de softwarefuncties worden gemaakt kunnen de gebruikers direct herkennen dat het platform geschikt is voor hun behoeften.

3.1.4.2 Leerbaarheid (Learnability)

Zie de LFI business requirements: '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.' De presentatie laag dient te voorzien in een uniforme look & feel.

3.1.4.3 Bedienbaarheid (Operability)

Zie de LFI business requirements: 'Applicaties zijn eenvoudig in gebruik en snel – bijvoorbeeld binnen één dag – aan te leren. De presentatie laag dient te voorzien in een uniforme look & feel, zoals de layout van schermen (plaatsing informatie- en control elementen zoals hyperlinks en buttons) en manieren van interactie met de gebruiker. De bedienbaarheid zal daarmee aanzienlijk toenemen t.o.v. de huidige situatie waarin verschillende applicaties gebruikt worden t.b.v. de IZB.

3.1.4.4 Voorkomen gebruikersfouten (User error protection)

Zie de LFI business requirements: '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 datacentrische inrichting inclusief invoer bewerkingsregels die foutieve invoer voorkomen.

3.1.4.5 Volmaaktheid gebruikersinteractie (User interface aesthetics)

Zie de LFI business requirements: '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 WCAG (Web Content Accessibility Guidelines) richtlijnen.

3.1.4.6 Toegankelijkheid (Accessibility)

Onderdeel van het platform is het bouwblok Multi Channel Presentatie Services, zodat mensen met de meest uiteenlopende eigenschappen en mogelijkheden om een gespecificeerd doel te bereiken in een gespecificeerde gebruikscontext, dit ook kunnen doen. WCAG gaat ook over de digitale toegankelijkheid.

3.1.5 Betrouwbaarheid (Reliability)

De mate waarin een systeem, product of component gespecificeerde functies uitvoert onder gespecificeerde condities gedurende een gespecificeerde hoeveelheid tijd.

3.1.5.1 Volwassenheid (Maturity)

Zie de LFI business requirements: 'Het ICT-landschap is aantoonbaar wendbaar, robuust en betrouwbaar.' Dit requirement is uitgedrukt in capaciteit, schaalbaarheid, beschikbaarheid, aanpasbaarheid, up-to-date zijn en het voldoen aan de NEN7510, 7512 en 7513.

3.1.5.2 Beschikbaarheid (Availability)

Zie de LFI business requirements voor IZB: '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.' Vanwege deze eis wordt het gehele platform zo ingericht en zal er geen onderscheid zijn voor latere niet IZB-functionaliteiten die gerealiseerd worden op het platform (eenduidigheid van beheer). Middels SLA afspraken en het realiseren van redundantie en geo spreiding wordt hier rekening mee gehouden.

3.1.5.3 Foutbestendigheid (Fault tolerance)

Het hele platform wordt gerealiseerd op cloud technologie met onderliggende redundante infrastructuur componenten, zodat het platform blijft werken bij hardwarefouten.

Applicaties worden opgebouwd uit microservices. Bij softwareontwikkeling moet eigenlijk altijd uitgegaan worden dat er fouten worden gemaakt, maar de error-handling dient ervoor te zorgen dat dit geen ongecontroleerde effecten oplevert.

Het platform gaat uit van een uitbreidbaar datacentrische inrichting inclusief invoer bewerkingsregels die foutieve invoer voorkomen.

3.1.5.4 Herstelbaarheid (Recoverability)

De leverancier treft de maatregelen die toepasselijk zijn voor de diverse beschikbaarheidseisen (BIV-classificaties).

Voorbeelden van systeemherstelbaarheid zijn clustering, log retention en automatic failover. Door gebruik te maken van Cloud Services zijn veel van deze maatregelen direct beschikbaar.

Dit geldt ook voor herstelbaarheid van gegevens (RTO en RPO), waarbij back-up en recovery onderdelen zijn van de opslag services.

Zie ook de NORA principes: 'Fouten in de bitopslag automatisch gedetecteerd kunnen worden en te herstellen zijn.'

3.1.6 Beveiligbaarheid (Security)

De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

3.1.6.1 Vertrouwelijkheid (Confidentiality)

Het platform wordt federatief ontsloten. Op basis van de BIV-classificatie zal waar nodig multi-factor authenticatie worden afgedwongen. Vanwege het federatieve stelsel wordt toegankelijkheid per persoon of

rol bepaald door de afnemende partijen zoals de GGD-en, maar ook door de context (b.v. locatie) en bedrijfsregels. De toegangscontrole wordt geïmplementeerd door de GGD GHOR NL. NEN7510 wordt als kader gehanteerd.

3.1.6.2 Integriteit (Integrity)

Het platform en daarmee eveneens de data services wordt federatief ontsloten. Op basis van de BIV-classificatie zal multi-factor authenticatie waar nodig worden afgedwongen. Vanwege het federatieve stelsel wordt toegankelijkheid per persoon of rol bepaald door de afnemende partijen zoals de GGD-en. De toegangscontrole wordt geïmplementeerd door de GGD GHOR NL. NEN7510 wordt als kader gehanteerd. Dit geldt eveneens voor de toegang door leveranciers. In de maatregelen is o.a. opgenomen dat alle bewerkingen op gegevens met een hoge integriteitsclassificatie wordt gemonitord en gecontroleerd door het SOC van GGD GHOR NL.

3.1.6.3 Onweerlegbaarheid (Non-repudiation)

Logging wordt ingeregeld 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 en 2. SIEM

3.1.6.4 Verantwoording (Accountability)

Logging wordt ingeregeld 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 en 2. SIEM

3.1.6.5 Authenticiteit (Authenticity)

In het domeinmodel wordt in de metadata de bron van gegevens opgenomen (traceerbaarheid). Deze is vooraf geverifieerd.

3.1.7 Onderhoudbaarheid (Maintainability)

De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden door de aangewezen beheerders.

3.1.7.1 Modulariteit (Modularity)

Het gehele platform is modulair opgebouwd. Zelfs de applicaties die uiteindelijk aangeboden worden zijn uit (herbruikbare) modules opgebouwd. Dit zorgt ervoor dat wijzigingen van een component minimale impact heeft op andere componenten.

3.1.7.2 Herbruikbaarheid (Reusability)

De modules van het platform zijn basisvoorzieningen welke hergebruikt kunnen worden voor domeinen waar de GGD-en buiten de IZB verantwoordelijk voor zijn. De applicaties die uiteindelijk aangeboden worden zijn uit (herbruikbare) modules opgebouwd.

3.1.7.3 Analyseerbaarheid (Analysability)

Het gehele platform wordt vanuit conceptueel model tot uiteindelijk ontwerp geborgd in de architectuurtool BlueDolphin, waardoor de impact op geplande wijzigingen effectief en efficiënt zijn te beoordelen in het change managementproces. Hiervoor levert de leverancier initieel en bij alle wijzigingen de benodigde informatie aan. Tevens zal er systeemlogging van elk onderdeel plaatsvinden en deze logging wordt centraal verzameld binnen de GGD GHOR NL.

3.1.7.4 *Wijzigbaarheid (Modifiability)*

Door de modulaire opbouw van het platform zijn aanpassingen per microservice door te voeren. Basis van de microservices is het domeinmodel. Aanpassingen binnen het domeinmodel dienen binnen 24 uur over de gehele keten (incl. RIVM) actief te zijn. In de overeenkomst met de leverancier worden hiervoor werkprocessen gedefinieerd.

3.1.7.5 *Testbaarheid (Testability)*

Door de modulaire opbouw van het gehele platform zijn testcriteria effectief en efficiënt per component, inclusief directe koppelingen, vast te stellen, wat initieel in een Proof of Solution zal worden gedaan en later volgens OTAP-concept.

3.1.8 Overdraagbaarheid (Portability)

De mate waarin een systeem, product of component effectief en efficiënt overgezet kan worden van één hardware, software of andere operationele of gebruiksomgeving naar een andere.

3.1.8.1 *Aanpasbaarheid (Adaptability)*

Door het maximaal gebruik van containtertechnologie en gevirtualiseerde cloud technologie is de omgeving zonder al te grote aanpassingen over te zetten naar verschillende cloud leveranciers. Op basis van het domeinmodel zullen uiteindelijk de softwarecomponenten gerealiseerd worden. Dit domeinmodel is uitbreidbaar, waarmee aanpasbaarheid gerealiseerd wordt.

3.1.8.2 *Installeerbaarheid (Installability)*

Het hele platform wordt gerealiseerd op cloud technologie, waar mogelijk container technologie. Applicaties worden opgebouwd uit microservices. Infrastructure as Code wordt gebruikt om effectief en efficiënt installaties, updates of verwijderingen uit te voeren in een gespecificeerde omgeving.

3.1.8.3 *Vervangbaarheid (Replaceability)*

Door de modulaire opbouw van het platform zijn bouwblokken met minimale impact te vervangen. Per bouwblok wordt gedetailleerd beschreven wat de technische en niet technische functionaliteiten zijn, zodat dit opnieuw uitgevraagd kan worden. Applicatiefunctionaliteiten worden per microservice opgebouwd en zijn daardoor eveneens te vervangen.

3.2 Geschiktheid voor gebruik (Quality in use)

3.2.1 Effectiviteit (Effectiveness)

De nauwkeurigheid en volledigheid waarmee gebruikers gespecificeerde doelen behalen wordt gerealiseerd doordat het onderliggende domeinmodel voor en met de GGD-en, maar ook met het RIVM, wordt ontwikkeld.

3.2.2 Efficiëntie (Efficiency)

Het hele platform wordt gerealiseerd op cloud-technologie, waar mogelijk container technologie, zodat het platform blijft werken bij hardware-fouten. Applicaties worden opgebouwd uit microservices. De schaalbaarheid zorgt voor de juiste effectiviteit. Hulpbronnen buiten het platform vallen buiten scope van dit programma.

De efficiëntie van het platform wordt bepaald door de snelheid waarmee vanuit een geformuleerd domeinmodel eindgebruiker-applicaties worden gerealiseerd.

3.2.3 Voldoening (Satisfaction)

De mate waarin gebruikersbehoeften vervuld worden als het product of systeem gebruikt wordt in een gespecificeerde gebruikscontext.

3.2.3.1 Bruikbaarheid (Usefulness)

Het platform wordt voor en met de GGD-en ontwikkeld. Het onderliggende domeinmodel wordt eveneens voor en met de GGD-en, maar ook met het RIVM ontwikkeld, om zo maximaal bij te dragen aan de gestelde doelen. Het advies is 'begin klein en breid uit'. Resultaten en consequenties zijn dan direct te constateren en indien nodig aan te passen.

3.2.3.2 Vertrouwen (Trust)

Het platform wordt voor en met de GGD-en ontwikkeld. Het onderliggende domeinmodel wordt eveneens voor en met de GGD-en, maar ook met het RIVM ontwikkeld. De directe betrokkenheid dient voor het vertrouwen te zorgen. Doordat security en privacy by design worden toegepast op alle onderdelen van het platform wordt de kans op een vertrouwensbreuk geminimaliseerd.

3.2.3.3 Plezier (Pleasure)

Door de opbouw van het platform, zal de bruikbaarheid en vertrouwen bijdragen aan het plezier van een gebruiker. De mate waarin een gebruiker plezier behaalt uit het verwezenlijken van zijn of haar persoonlijke behoeften valt buiten de scope van dit programma.

3.2.3.4 Welzijn (Comfort)

Door de mogelijkheid om applicaties via verschillende kanalen aan te bieden (multi-channel) kan het kanaal gebruikt worden welke het beste aansluit bij het fysieke welzijn van de gebruiker.

3.2.4 Vrijwaring tegen risico (Freedom from risk)

De mate waarin een product of systeem het potentiële risico beperkt met betrekking tot economische status, mensenlevens, gezondheid of de omgeving.

3.2.4.1 Economisch-risico-beperking (Economic risk mitigation)

Security en Privacy by Design zijn uitgangspunten van het ontwerp van het gehele platform. NORA principes NAP11, NAP13 en NAP14 met hun implicaties vormen de basis hiervoor. *Security by Design* wordt vormgegeven door het opstellen van een dreigingsanalyse en het maken van BIV-classificaties, welke resulteren in een normenselectie die beschrijft welke normen specifiek moeten worden ingevuld. *Privacy by Design* wordt vormgegeven door het opstellen van een DPIA. De normenselectie en DPIA houden rekening met de principes. Daar waar potentiële risico's met betrekking tot financiële status, efficiënte werking, commerciële eigendommen, reputatie of andere middelen in de beoogde gebruikscontexten worden onderkend, worden in de oplossing mitigerende maatregelen getroffen.

3.2.4.2 Gezondheids- en veiligheidsrisicobeperking (Health and safety risk mitigation)

Security en Privacy by Design zijn uitgangspunten van het ontwerp van het gehele platform. NORA principes NAP11, NAP13 en NAP 14 met hun implicaties vormen de basis hiervoor. *Security by Design* wordt vormgegeven door het opstellen van een dreigingsanalyse en het maken van een BIV-classificaties, welke resulteren in een normenselectie, die beschrijft welke normen specifiek moeten worden ingevuld. *Privacy by Design* wordt vormgegeven door het opstellen van een DPIA. De normenselectie en DPIA houden rekening met de principes. Daar waar potentiële risico's met betrekking tot personen beperkt in de beoogde gebruikscontexten worden onderkend, worden in de oplossing mitigerende maatregelen getroffen.

3.2.4.3 *Omgevingsrisicobeperking (Environmental risk mitigation)*

Security en Privacy by Design zijn uitgangspunten van het ontwerp van het gehele platform. NORA principes NAP11, NAP13 en NAP 14 met hun implicaties vormen de basis hiervoor. *Security by Design* wordt vormgegeven door het opstellen van een dreigingsanalyse en het maken van een BIV-classificaties, welke resulteren in een normenselectie, die beschrijft welke normen specifiek moeten worden ingevuld. *Privacy by Design* wordt vormgegeven door het opstellen van een DPIA. De normenselectie en DPIA houden rekening met de principes. Daar waar potentiële risico's met betrekking tot eigendommen of de omgeving beperkt in de beoogde gebruikscontexten worden onderkend, worden in de oplossing mitigerende maatregelen getroffen.

3.2.5 Contextdekking (Context coverage)

De mate waarin een product of systeem gebruikt kan worden met effectiviteit, efficiëntie, vrijheid van risico en voldoening zowel in de gespecificeerde gebruikscontexten als in niet initieel gespecificeerde gebruikscontexten.

3.2.5.1 *Contextcompleetheid (Context completeness)*

De contextcompleetheid is beschreven in bovenstaande paragrafen waarin effectiviteit, efficiëntie, vrijheid van risico en voldoening in alle gespecificeerde gebruikscontexten zijn beschreven.

3.2.5.2 *Flexibiliteit (Flexibility)*

Het hele platform is ontworpen en ingericht om snel in te kunnen springen op behoeftes die niet initieel gespecificeerd zijn in de requirements. Dit wordt o.a. gerealiseerd door de aanpasbaarheid van het onderliggende domeinmodel en de modulaire opbouw van het platform.

4 Kaders en implicaties per bouwblok

In dit hoofdstuk zijn de verschillende kaders en bijhorende implicaties per bouwblok uitgewerkt.

4.1 Algemene Kaders

Kaders die van toepassing zijn op specifieke bouwblokken zijn per bouwblok opgenomen. Hieronder zijn de kaders opgenomen die gelden voor het platform als geheel.

4.1.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Algemeen
IMP031 Informatie	Ontwerp op modulaire wijze	Realiseer complexe systemen op modulaire wijze. Dit doe je door het systeem zodanig te ontwerpen dat deze opgedeeld kan worden in modules. Elke module moet eigenschappen bevatten die het mogelijk maken om ze (via gestandaardiseerde koppelvlakken) aan elkaar te koppelen. Zodanig vormen ze in het geheel een complex systeem.	ALGEMEEN: De opbouw van het platform in bouwblokken, welke resulteert in verschillende services is een ontwerp op modulaire wijze
IMP029 Organisatorisch Informatie Applicatie	Scheid proces van data	Scheid proces van data en data van software. Zorg dat software hardware-agnostisch is. De afhankelijkheden tussen (proces-)onderdelen moeten bij voorkeur zo klein mogelijk zijn. Hierdoor blijft	ALGEMEEN: Door de opzet van Data Services, waar applicatie services weer gebruik van kunnen maken is data en software gescheiden. Processen worden door de datacentrische

		ontkoppeling op een later moment mogelijk.	aanpak verwerkt in het aan te leveren domein model. Hiermee wordt proces niet volledig van data gescheiden, maar het lijkt erop dat deze implicatie nog verwijst naar een applicatie centrische aanpak.
IMP039 Grondslagen	Zorg voor open specificaties	Zorg voor open specificaties. Zodat deze hergebruikt kunnen worden over instellingen heen. Dit voorkomt dat verschillende organisaties hetzelfde wiel moeten uitvinden. Zie ook EIF principle 2: "Openness", aanbeveling 4. EIF-brochure (pdf)	ALGEMEEN: er wordt gebruik gemaakt van open specificaties die al bestaan (bv forum standaardisatie). Vooralsnog is de aanname dat er geen specificatie wordt ontwikkeld, indien dat wel het geval is zal er rekening moeten worden gehouden met hergebruik.
IMP034 Grondslagen	Gebruik de standaard met het meest specifieke werkingsgebied	Gebruik de standaard met het meest specifieke werkingsgebied. Als deze conflicteert met bredere (internationale) standaarden, zorg dan in de sector voor afstemming daarmee.	ALGEMEEN: de algemeen geldende standaarden worden gebruikt, waar mogelijk toegespitst op de publieke gezondheidszorg (Nictiz).
IMP035 Organisatorisch	Gebruik een actueel register met standaarden	Maak gebruik van een actueel register met standaarden per toepassingsgebied. Functionele standaarden hebben betrekking op bijvoorbeeld gegevensuitwisseling, beveiliging, taalgebruik, digitale communicatie, etc. Standaarden met een organisatorisch werkingsgebied hebben betrekking op bijvoorbeeld de strafrechtketen, zorgketen, sociale zekerheid, financiën, etc.	ALGEMEEN: Er dient binnen GGD GHOR een register bijgehouden te worden, evt. kunnen dit verwijzingen zijn naar overzichten zoals het forum standaardisatie. Governance moet worden ingericht en er dient te worden afgedwongen dat in elk traject gebruik wordt gemaakt van de opgenomen standaarden. Idealiter wordt in het register de volgorde van gebruik aangegeven. Functie uit te voeren binnen de datacatalogus die nu al wordt ingericht vanuit Thema 3 datagedreven werken.
IMP075 Organisatorisch	Gebruik open standaarden voor modellering	Organisaties werken volgens een open standaard voor o.a. architectuur-, data- en procesmodellering die door alle samenwerkende partijen op uniforme wijze wordt toegepast. De gekozen open standaard is bepalend voor de keuze van modelleersystemen die deze standaard ondersteunen. Wissel modellen uit tussen organisaties op basis van open standaarden. Voorbeelden van modelleerstandaarden zijn ArchiMate (architectuur), UML (data) en BPMN (processen).	ALGEMEEN: GGD GHOR NL heeft voor de tool BlueDolphin gekozen waarmee in ArchiMate, BPMN en ERD gemodelleerd kan worden. T.b.v. modellering informatie/domeinmodel kan een andere taal wellicht beter aansluiten (b.v. DEMO). Van belang is dat GGD-en en RIVM dezelfde modelleertaal hiervoor gebruiken.
IMP076 Organisatorisch	Maak afspraken over nieuwe (en oude) versies van standaarden	De dienstverlener en de afnemers maken afspraken over de periode waarin overgegaan wordt op een nieuwe versie van de standaard. Wanneer een nieuwe versie van een standaard geïmplementeerd wordt, blijft de aanbieder de oude	ALGEMEEN: Uitgaande dat alle componenten als diensten beschreven gaan worden, dienen afspraken omtrent versies van standaarden opgenomen te worden in de dienstbeschrijving.

		versie ondersteunen zolang als dat volgens afspraak nodig is.	

4.2 Kaders Centrale IAM Service (PL1)

4.2.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Centrale IAM Service
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	N.v.t. Betreft een 'basisvoorziening' dienst. Deze dient wel als dienst beschreven te worden.
IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie	Verwerk als afnemer gegevens uit een bronsysteem met respect voor de classificatie van die gegevens. Geef het geen hogere classificatie voor beschikbaarheid en integriteit dan de bron, en geen lagere classificatie voor vertrouwelijkheid. Maak zo nodig afspraken met de aanbieder om hun classificatie aan te passen en in hun dienst bijpassende maatregelen daarvoor te implementeren.	Hoewel de bronnen de verschillende HR-systemen zijn, is de IAM omgeving het cumulatief en verzorgt de toegang tot alle systemen. Daardoor zal deze de hoogste classificatie krijgen. Hierdoor is direct voorbereid dat elke bron aangesloten kan worden.
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	Alleen de gegevens benodigd om een toegang te kunnen faciliteren mogen gebruikt worden.

IMP030 Informatie	Scheiding van datasets	Verdeel de informatie in afgebakende datasets, die ook elk afzonderlijk getoetst kunnen worden op het voldoen aan de AVG.	Door de federatieve opzet is dit automatisch gescheiden.
IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's	Gegevensuitwisseling tussen (web)applicaties gebeurt via Restful API's. De broneigenaar levert API's die voldoen aan de moderne RESTful standaarden. API's dienen centraal te worden beheerd in een API management systeem.	Onderliggende identity en access management oplossing van de GGD GHOR NL wordt aangesproken via API's.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van IAM-componenten
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing t.b.v. IAM

IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk Iaas.	Voorziening afnemen als SaaS, indien PaaS of IaaS laten landen op Cloud services.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.

IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP044 Grondslagen	Hanteer bewaartermijnen voor informatie	Informatie wordt niet langer bewaard en niet eerder vernietigd dan wettelijk is toegestaan. Dit betekent dat: Er een selectielijst is, waarin opgenomen de te vernietigen informatieobjecten of onderdelen daarvan. Er vastgesteld in de organisatie verankerd beleid is met betrekking tot vernietigen. Bevoegdheden, rollen en verantwoordelijkheden en beleid rondom vernietigen zijn belegd. De organisatie inzicht heeft in informatieobjecten, bewaartermijnen, processen, informatiesystemen en hun onderlinge samenhang.	Bevoegdheden, rollen en verantwoordelijkheden en beleid rondom vernietigen zijn belegd.
IMP060 Applicatie	Bepaal autorisaties met metadata	Autorisaties voor het verstrekken en gebruik van gegevens kan worden bepaald op basis van metadata. De beheerder die het gegeven beheert en het wil verstrekken voor verdere bewerking, voegt metadata toe aan de hand waarvan de beheerder en de afnemer een autorisatiebeslissing kan nemen.	Access control op basis van attributen o.a. uit het domeinmodel.
IMP077 Organisatorisch	Stel de juridische aansprakelijkheid per gegevensobject vast	Stel per informatie-object de bron vast, en daarmee de juridische aansprakelijkheid voor de juistheid van het object.	In federatief stelsel zijn aangesloten organisaties zelf verantwoordelijk en dus aansprakelijk voor authenticaties en het uitdelen van autorisaties
IMP045 Grondslagen	Leg de doelbinding vast in de metadata van het gegevensobject	De verwerkingshistorie inclusief doel van verwerking wordt vastgelegd bij het gegevensobject als metadata. Dit betekent dat de historie van acties waarin een gegevensobject wordt verwerkt (opvragen / vastleggen / wijzigen / verwijderen) inclusief het doel van de actie vastgelegd wordt bij het gegevensobject.	De Centrale IAM Service houdt een audittrail bij van manipulaties op de autorisatieregels waarin identiteitskenmerken (attributen die een natuurlijk persoon identificeren) gebruikt worden.
IMP054 Informatie	Leg de grondslag en het doel van de gegevensverwerking vast	Leg de grondslag en het doel vast, waarvoor informatie wordt uitgevraagd bij burgers en bedrijven. Aan het doel gekoppeld worden ook de eisen (kwaliteitscriteria) vastgelegd waaraan deze informatie moet voldoen. Houd er rekening mee dat het doel in de loop der tijd kan wijzigen.	Indien de Centrale IAM Service een bron gebruikt voor het nemen van een toegangsbeslissing dan dient de doelbinding van het gebruik van die bron vastgelegd te zijn.
IMP004 Grondslagen Informatie	Minimaliseer het gebruik van gegevens	Verzamel of vraag alleen die gegevens op die nodig zijn voor het strikte doel van de	Ieder procesbouwblok moet zich kunnen aanmelden, dus een

		dienstverlening. En houd de gegevensverwerking die hierop volgt in proportie met het doel. Dit voorkomt dat vertrouwelijke of privacygevoelige gegevens onnodig worden verwerkt.	identiteit hebben Aandachtspunt: lifecycle identiteiten.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. Data Services worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.
IMP080 Informatie	Controleer de verwerking van gegevens	Controleer de verwerking van gegevens: * Zijn de criteria voor juistheid, en tijdigheid vastgesteld? * Worden gegevens die vanuit een systeemvreemde omgeving ingevoerd zijn eerst gecontroleerd op juistheid, tijdigheid en volledigheid, voordat verdere verwerking plaatsvindt? * Worden te versturen gegevens gecontroleerd op juistheid, volledigheid en tijdigheid? * Worden ter verwerking aangeboden gegevens gecontroleerd op juiste, volledig en tijdige verwerking? * Worden kritieke gegevens die in verschillende gegevensverzamelingen voorkomen periodiek met elkaar vergeleken op consistentie? (Dit geldt alleen zolang de gegevens niet frequent en integraal worden gesynchroniseerd met de brongegevens)	N.v.t., omdat de gegevens om een autorisatiebeslissing te kunnen nemen uit autoritatieve bronnen komen waarvoor de eigenaren van die bronnen verantwoordelijk zijn. Dit is randvoorwaardelijk voor de juiste werking van dit bouwblok. Het bouwblok dient wel mogelijkheden te bieden om in geautomatiseerde (IDU) workflow beslismomenten op te nemen Het bouwblok moet ook voorzien in mogelijkheden (bijvoorbeeld d.m.v. rapportages of dashboards) de juistheid van gebruikte gegevens te controleren
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.

IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP015 Applicatie	Maak beveiligingsmaatregelen zo gebruiksvriendelijk mogelijk	Maak beveiligingsmaatregelen transparant voor de gebruiker en richt deze zo gebruiksvriendelijk mogelijk in. Verleid de gebruiker zo veel mogelijk om veilig te werken: zo leidt het afdwingen van gebruikersonvriendelijke beveiligingsmaatregelen vaak tot onveilige workarounds en ander onveilig gedrag.	Gebruikersvriendelijke UX voor o.a. MFA, maar ook het aanvragen van rechten.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats.
IMP064 Applicatie	Stel onweerlegbaarheid vast	Stel vast voor welke berichtenstromen of transacties onweerlegbaarheid van gegevens vereist is, zodat daarvoor aanvullende maatregelen genomen kunnen worden.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP084 Applicatie	Versleutel gegevens in rust en transport	Versleutel alle gegevensdragers waarop niet-publieke informatie staat, inclusief smartphones en laptops, conform de laatst bekende en geldende richtlijnen. Dit reduceert het risico op een gegevenslek bij verlies van een dergelijk apparaat.	Versleutel IAM-gegevens in rust en transport

		Neem voor niet-publieke gegevens ook adequate beveiligingsmaatregelen om ze te beschermen in transit. Dit kan door de verbinding te beveiligen, danwel door encryptie van de informatie zelf. Dit laatste heeft de voorkeur.	
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok
IMP069 Netwerk	Hanteer het zero-trust model	Ga nooit uit van het impliciete vertrouwen dat wie op een bepaald netwerk of systeem komt daar ook hoort: * Controleer overal het netwerkverkeer. * Controleer toegang per sessie. * Hanteer dynamische policies en gebruik daarbij de geldigheidsduur van de laatste authenticatie. * Blijf continue monitoren. Verzamel zoveel mogelijk gegevens om de beveiliging te blijven verbeteren. Dit wordt ook wel het 'zero-trust' model genoemd.	(Continuous) Authentication: * Controleer toegang per sessie. * Hanteer dynamische policies en gebruik daarbij de geldigheidsduur van de laatste authenticatie.
IMP019 Organisatorisch	Maak stelselafspraken over identificatie en authenticatie	Maak stelselafspraken om te komen tot één generiek digitaal stelsel voor identificatie en authenticatie of sluit aan bij een bestaand kanaaloverstijgend stelsel met afspraken over betrouwbaarheidsniveau's.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok. Via de Centrale IAM Service worden de stelselafspraken geborgd.
IMP068 Applicatie	Maak toegang tot applicaties en gegevens afhankelijk van authenticatieniveau	Een gebruiker dient allereerst geautoriseerd te zijn om een applicatie te mogen gebruiken of gegevens te mogen inzien. Hierbij speelt het behaalde niveau van authenticatie een rol. Als bijvoorbeeld informatie met een tweede factor (MFA) moet zijn afgeschermd krijgt de gebruiker geen toegang als hij/zij slechts met een gebruikersnaam/wachtwoord combinatie kan authenticeren. Na succesvolle authenticatie kan bepaald worden of een gebruiker de applicatie mag gebruiken (of informatie mag inzien) aan de hand van autorisatieregels.	Maak gebruik van RBAC. Step-up authenticatie. Van lager naar hoger authenticatie niveau. STORK stelsel - Secure idenTity acrOss boRders linKed.

IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Aanleveren audit- en logdata: * Manipulatie van rechtentoekenning, dus als iemand verhoogde rechten toegekend krijgt, of wordt toegekend aan een rolgroep. * Logging op runtime: wordt het verzoek toegekend of geweigerd. * Systeemlogging aanleveren.
IMP065 Informatie	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces	Controleer de kwaliteit van gegevens vanaf invoer en op ieder koppelvlak aan de hand van de vastgestelde kwaliteitseisen. Eenmaal geverifieerd hoeft een verificatie niet opnieuw plaats te vinden als de eerder uitgevoerde verificatie nog betrouwbaar is.	Controle op statistische afwijkingen in aangeleverde data vanuit bronsystemen en (automatische) response.
IMP088 Applicatie	Verleen alleen strikt noodzakelijke toegangsrechten	Ken geen rollen en toegangsrechten toe aan accounts van gebruikers en services tenzij dat strikt noodzakelijk is (Least Privilege).	Principe van Least Privilege wordt gehanteerd (security by design).

4.2.2 MedMij

Bron: MedMij		
Zie hiervoor Rollen, Core - MedMij Afsprakenstelsel - Verplicht - MedMij Afsprakenstelsel		
1.	De Aanbieder is verplicht bij het verstrekken van gegevens vanuit een gezondheidsdossier de identiteit van de persoon te verifiëren, al dan niet aan de hand van het Burgerservicenummer (BSN). MedMij gebruikt hiervoor de door het ministerie van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties toegelaten authenticatiemiddelen.	Vooralsnog is DigiD het enige toegelaten middel voor dit doel. Dient te voldoen aan: Verantwoordelijkheden, Core - MedMij Afsprakenstelsel - Verplicht - MedMij Afsprakenstelsel
2.	Een OAuth Resource Owner is een Persoon die een OAuth Client autoriseert voor toegang tot een OAuth Resource Server.	De toegang is beperkt tot het bereik van de verleende autorisatie. Dient te voldoen aan: Verantwoordelijkheden, Core - MedMij Afsprakenstelsel - Verplicht - MedMij Afsprakenstelsel

4.2.3 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Centrale IAM Service**
1	Alle betrokkenen in het netwerk van een persoon moeten de mogelijkheid hebben de data in die dossiers te kunnen raadplegen en gebruiken. Maar alleen als zij daartoe geautoriseerd zijn en die gegevens nodig hebben voor het leveren van passende hybride zorg met waarborgen voor patiëntveiligheid.	Organisaties federatief aangesloten op Centrale IAM Service moeten de mogelijkheid hebben de data in die dossiers te kunnen raadplegen en gebruiken.
2	Partijen in het zorgnetwerk zijn aangesloten op de landelijk dekkende en nationaal vastgestelde infrastructuren. Dit zodat zij elkaar eenvoudig kunnen bereiken, gegevens kunnen delen en ondersteund worden in de samenwerking	Koppeling DigiD dient gerealiseerd/gehandhaafd te blijven.

3	Onderdeel van het vertrouwensmodel is onder andere eenvoudige identificatie, authenticatie, autorisatie, logging, toestemming en behandelrelatie en de rollen en verantwoordelijkheden die daarbij horen	Eenvoudige autorisatie dient gerealiseerd te worden. Toestemming (Mitz) dient onderdeel van access control te zijn.
4	de invulling van generieke functies door middel van gemeenschappelijke voorzieningen, zoals Mitz voor toestemmingen	Toestemming (Mitz) dient onderdeel van access control te zijn.
5	Ook is het van groot belang dat een zorgverlener een gekwalificeerd identificatiemiddel kan kiezen dat voor alle prioritaire gegevensuitwisselingen gebruikt kan worden. Essentieel is dat dit een gebruiksvriendelijke oplossing is.	In kaart brengen van gekwalificeerd identificatiemiddelen en gebruik daarvan mogelijk maken.

4.2.4 Nictiz: API Requirements for Dutch Healthcare

Nictiz: API Requirements for Dutch Healthcare - Centrale IAM Service		
nr	**Requirement**	**Hoofdstuk**
AG002	API Access Restriction Policies MUST be openly and freely available	API agreements
SC006	Specifications for 'System APIs' MUST use authentication and authorization models that are not specific to a use case or (type of) client or user	API security
SC008	All tokens used for client authentication MUST be signed using asymmetrical encryption	API security

4.2.5 Privacy

Kaderstelling Privacy		Centrale IAM Service
2.5.2.1	Doelbinding	Consent (Mitz) is onderdeel van het te nemen toegangsbesluit
2.5.2.3	Burgerportaal	
2.5.2.1	Juistheid van gegevens	Policies zijn onderdeel van het te nemen toegangsbesluit
2.5.2.1	Integriteit en vertrouwelijkheid	Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
2.5.2.4	Beveiliging van de verwerking	
2.5.2.3	Burgerportaal	Inloggen met DigiD mogelijk maken
2.5.2.4	Beveiliging van de verwerking	Verantwoordelijkheden en bevoegdheden in rollen
2.5.2.4	Beveiliging van de verwerking	Toegang op basis van hard- en software
2.5.2.5	Privacy by design & Privacy by default	Toegang tot gegevens op basis van het domeinmodel
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd

4.3 Kaders Cloud Services (PL2)

4.3.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Cloud Services
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten.	N.v.t. Betreft een 'basisvoorziening' dienst. Deze dient wel als dienst beschreven te worden.

		De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	N.v.t. Betreft een 'basisvoorziening' dienst.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van Cloud voorzieningen.
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing t.b.v. private en public Cloud Services.
IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en	Input: goedgekeurd cloud strategie (welke rekening houdt met rijksbreed cloudbeleid) t.b.v. keuze public/private. Exit strategie moet onderdeel zijn van de af te nemen dienst.

		netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk Iaas.	
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP002 Informatie	Voorkom verlies van informatie	Veranderingen in techniek, organisatie of gebruikerswensen mogen niet van negatieve invloed zijn op de duurzame toegankelijkheid van informatie. Hetzelfde geldt voor bitrot (verlies van informatie door verval van opslagmedia). Neem vooraf maatregelen om informatie toekomstbestendig te maken, zodat deze toegankelijk blijft voor de van toepassing zijnde vormen van (her)gebruik. Dit betekent dat: Leveranciersafhankelijkheid wordt voorkomen. Analyse wordt gemaakt van welke gevolgen veranderingen (in techniek, organisatie, of gebruikerswensen) hebben voor de duurzame toegankelijkheid van informatie. Bij het ontwerpen van informatiesystemen na wordt gedacht over de te gebruiken technologie voor het beheren van informatie.	Aangezien de opslag services zullen 'landen' op Cloud Services dienen afspraken omtrent bitrot ook hier gemaakt te worden.
MP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. Data Services worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.

	maatregelen		
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats. Voor de bouwblokken die gebruik maken van de Cloud Services zal netwerksegmentatie op de Cloud Services worden ingericht. (internal firewalling) Op de Cloud Services worden ook de perimeter firewalls ingericht.
IMP084 Applicatie	Versleutel gegevens in rust en transport	Versleutel alle gegevensdragers waarop niet-publieke informatie staat, inclusief smartphones en laptops, conform de laatst bekende en geldende richtlijnen. Dit reduceert het risico op een gegevenslek bij verlies van een dergelijk apparaat. Neem voor niet-publieke gegevens ook adequate beveiligingsmaatregelen om ze te beschermen in transit. Dit kan door de verbinding te beveiligen, danwel door encryptie van de informatie zelf. Dit laatste heeft de voorkeur.	Op de Cloud Services zullen diensten worden ingericht die zorgen voor versleuteling van gegevens in rust en transport.
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren

4.3.2 Privacy

Kaderstelling Privacy		Cloud Services
2.5.2.1	Integriteit en vertrouwelijkheid	Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
2.5.2.4	Beveiliging van de verwerking	
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

4.3.3 ISO 27017 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

NEN-EN-ISO/IEC 27017 geeft richtlijnen voor informatiebeveiligingscontroles die van toepassing zijn op de levering en het gebruik van clouddiensten door het verstrekken van:

- aanvullende implementatierichtlijnen voor relevante controles gespecificeerd in ISO/IEC 27002;
- Aanvullende controles met implementatierichtlijnen die specifiek betrekking hebben op cloudservices.

Deze aanbeveling/Internationale Standaard biedt controles en implementatierichtlijnen voor zowel cloudserviceproviders als klanten van cloudservices.

Zie: https://www.nen.nl/nen-en-iso-iec-27017-2021-en-279281

4.3.4 ISO 27018 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

NEN-EN-ISO/IEC 27018 stelt algemeen aanvaarde controledoelstellingen, controles en richtlijnen vast voor het implementeren van maatregelen ter bescherming van persoonlijk identificeerbare informatie (PII) in overeenstemming met de privacyprincipes in ISO/IEC 29100 voor de openbare cloud computing-omgeving. In dit document worden met name richtlijnen gespecificeerd op basis van ISO/IEC 27002, rekening houdend met de wettelijke vereisten voor de bescherming van PII die van toepassing kunnen zijn in de context van de informatiebeveiligingsrisico-omgeving(en) van een aanbieder van openbare clouddiensten. Dit document is van toepassing op organisaties van alle soorten en maten, inclusief openbare en particuliere bedrijven, overheidsinstanties en non-profitorganisaties, die informatieverwerkingsdiensten leveren als PII-verwerkers via cloud computing onder contract met andere organisaties. De richtlijnen in dit document kunnen ook relevant zijn voor organisaties die optreden als PII-controllers. PII-verwerkingsverantwoordelijken kunnen echter onderworpen zijn aan aanvullende wet- en regelgeving en verplichtingen op het gebied van PII-bescherming, die niet van toepassing zijn op PII-verwerkers. Dit document is niet bedoeld om dergelijke aanvullende verplichtingen te dekken.

Zie: https://www.nen.nl/nen-en-iso-iec-27018-2020-en-272121

4.4 Kaders Security Monitoring (PL3a)

4.4.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Security & Privacy
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	N.v.t. Betreft een 'basisvoorziening' dienst. Deze dient wel als dienst beschreven te worden.
IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie	Verwerk als afnemer gegevens uit een bronsysteem met respect voor de classificatie van die gegevens. Geef het geen hogere classificatie voor beschikbaarheid en integriteit dan de bron, en geen lagere classificatie voor vertrouwelijkheid. Maak zonodig afspraken met de aanbieder om hun classificatie aan te passen en in hun dienst bijpassende maatregelen daarvoor te implementeren.	De bronnen zijn de logbestanden van de aangesloten systemen. Ook hier betreft het cumulatief en zal daardoor de hoogste classificatie krijgen, zodat iedere bron aangesloten kan worden.
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	Alleen de gegevens met (wettelijke) grondslag die benodigd zijn voor systeemlogging en audit trails mogen gebruikt worden.
IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's	Gegevensuitwisseling tussen (web)applicaties gebeurt via Restful API's. De broneigenaar levert API's die voldoen aan de moderne RESTful standaarden. API's dienen centraal te worden beheerd in een API management systeem.	Applicatielogging t.b.v. auditing dient via API's te communiceren met het SOC/SIEM systeem.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen	Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van Security Monitoring componenten

		enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing t.b.v. security monitoring.
IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk Iaas.	Voorziening afnemen als SaaS, indien PaaS of IaaS laten landen op Cloud services.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.

IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP049 Informatie	Draag zorg voor juiste en actuele en volledige informatie	Een gebruiker kan er op vertrouwen dat een informatieobject, zoals deze in de bron is vastgelegd, juist, actueel en volledig is. Fouten kunnen worden gemeld en hersteld. Daarbij is het van belang dat herstelwijzigingen worden gelogd, zodat traceerbaar is hoe foutieve gegevens zijn verwerkt en wat het effect daarvan is. Dit betekent dat: De kwaliteit van de informatie transparant, verankerd en geborgd moet zijn binnen de processen van de verantwoordelijke en leverende organisatie (datamanagement). Er gebruik moet worden gemaakt van gestandaardiseerde gegevensmodellen, gegevenswoordenboeken en catalogussen ten behoeve van machinematige verwerking van gegevens. De informatie tijdens de gehele levenscyclus moet worden gemonitord, gecontroleerd, gevalideerd op basis van regels, kaders, normen en standaarden waarbij wijzigingen traceerbaar moeten worden gemaakt. De informatie tijdens de gehele levenscyclus regelmatig moet worden getoetst aan wet- en regelgeving en daar verantwoording over moet worden afgelegd. Er cyclisch gerapporteerd moet worden over de kwaliteit van de gegevens. Voor afwijkingen moeten de juiste maatregelen worden getroffen om de betrouwbaarheid en de kwaliteit van de informatie te kunnen waarborgen. De informatie moet door de gehele lifecycle gevolgd kunnen worden vanaf de oorsprong tot aan het verwerken, opslaan, bewerken en beschikbaar stellen en/of vernietigen. (data-lineage). Er gebruik moet worden gemaakt van authentieke- en/of kwalitatieve bronnen.	De informatie tijdens de gehele levenscyclus moet worden gemonitord, gecontroleerd, gevalideerd op basis van regels, kaders, normen en standaarden waarbij wijzigingen traceerbaar moeten worden gemaakt. De informatie tijdens de gehele levenscyclus regelmatig moet worden getoetst aan wet- en regelgeving en daar verantwoording over moet worden afgelegd.
IMP044 Grondslagen	Hanteer bewaartermijnen voor informatie	Informatie wordt niet langer bewaard en niet eerder vernietigd dan wettelijk is toegestaan. Dit betekent dat: Er een selectielijst is, waarin opgenomen de te vernietigen informatieobjecten of onderdelen daarvan. Er vastgesteld in de organisatie verankerd beleid is met betrekking tot vernietigen. Bevoegdheden, rollen en verantwoordelijkheden en beleid rondom vernietigen zijn belegd. De organisatie inzicht heeft in informatieobjecten, bewaartermijnen, processen, informatiesystemen en hun onderlinge samenhang.	Logbestanden worden niet langer bewaard dan wettelijk is toegestaan. Moet dus nader bepaald worden.
IMP051 Informatie	Leg auditlogs vast bij de bronregistratie van het gegeven	Als eigenaar van de bron wil je inzicht hebben in de toegang en inzage (CRUD) van de gegevens die vanuit de bron worden	Leg auditlogs vast bij de bronregistratie van het gegeven.

		gebruikt. Voorkom dat auditgegevens verspreid raken over afnemende applicaties.	
IMP059 Informatie	Geef de voorkeur aan halen i.p.v. brengen van gegevens	Geef de voorkeur aan het halen (pull) i.p.v. het brengen van gegevens (push).	Loginformatie dient waar mogelijk aangeleverd te worden.
IMP045 Grondslagen	Leg de doelbinding vast in de metadata van het gegevensobject	De verwerkingshistorie inclusief doel van verwerking wordt vastgelegd bij het gegevensobject als metadata. Dit betekent dat de historie van acties waarin een gegevensobject wordt verwerkt (opvragen / vastleggen / wijzigen / verwijderen) inclusief het doel van de actie vastgelegd wordt bij het gegevensobject.	Audittrail op gegevensverwerking wordt geleverd vanuit Data Services. Audittrail voor manipulaties op de autorisatieregels wordt geleverd vanuit de Centrale IAM Service.
IMP004 Grondslagen Informatie	Minimaliseer het gebruik van gegevens	Verzamel of vraag alleen die gegevens op die nodig zijn voor het strikte doel van de dienstverlening. En houd de gegevensverwerking die hierop volgt in proportie met het doel. Dit voorkomt dat vertrouwelijke of privacygevoelige gegevens onnodig worden verwerkt.	Leg per security use case vast welke (audit-) data nodig is en verzamel niet méér dan die gegevens en bewaar deze niet langer dan strikt noodzakelijk en toegestaan.
IMP022 Grondslagen	Neem oorspronkelijke grondslag mee bij hergebruik diensten	Bij hergebruik van diensten kijken zowel aanbieder als afnemer opnieuw naar de oorspronkelijke grondslag en doelbinding. Als dat nodig blijkt passen zij pseudonimisering dan wel anonimisering van de data toe. Dit houdt in dat bij te ontwikkelen functionaliteit de oorspronkelijke grondslag bepalend is voor de hergebruikmogelijkheden.	Beleid bepaalt eventuele (wettelijke) grondslag voor hergebruik van gegevens uit (audit) logdata.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	RPO moet 0 zijn vanwege auditeerbaarheid en traceerbaarheid. MTO en RTO worden bepaald door de diensteigenaar.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.
IMP080 Informatie	Controleer de verwerking van gegevens	Controleer de verwerking van gegevens: * Zijn de criteria voor juistheid, en tijdigheid vastgesteld? * Worden gegevens die vanuit een systeemvreemde omgeving ingevoerd zijn eerst gecontroleerd op juistheid, tijdigheid en volledigheid, voordat verdere verwerking plaatsvindt? * Worden te versturen gegevens gecontroleerd op juistheid, volledigheid en tijdigheid? * Worden ter verwerking aangeboden gegevens gecontroleerd op juiste, volledig en tijdige verwerking? * Worden kritieke gegevens die in verschillende gegevensverzamelingen voorkomen periodiek met elkaar vergeleken op consistentie? (Dit geldt alleen zolang de gegevens niet frequent en integraal worden gesynchroniseerd met de brongegevens)	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok. Het bouwblok moet voor sommige functies (b.v. tijdige alerting bij cyber-aanvallen) wel tijdig worden voorzien ((near)-realtime) van de juiste gegevens. Daarnaast moet het bouwblok de verwerkingscapaciteit hebben om ontvangende systemen (zoals dashboards) tijdig te voorzien van informatie die het bouwblok heeft gecreëerd. De logdata die in dit bouwblok wordt aangeleverd mag niet

			gemanipuleerd worden (juistheid).
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats.
IMP064 Applicatie	Stel onweerlegbaarheid vast	Stel vast voor welke berichtenstromen of transacties onweerlegbaarheid van gegevens vereist is, zodat daarvoor aanvullende maatregelen genomen kunnen worden.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP084 Applicatie	Versleutel gegevens in rust en transport	Versleutel alle gegevensdragers waarop niet-publieke informatie staat, inclusief smartphones en laptops, conform de laatst bekende en geldende richtlijnen. Dit reduceert het risico op een gegevenslek bij verlies van een dergelijk apparaat. Neem voor niet-publieke gegevens ook adequate beveiligingsmaatregelen om ze te beschermen in transit. Dit kan door de verbinding te beveiligen, danwel door encryptie van de informatie zelf. Dit laatste heeft de voorkeur.	Versleutel log-gegevens in rust en transport.
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.

IMP069 Netwerk	Hanteer het zero-trust model	Ga nooit uit van het impliciete vertrouwen dat wie op een bepaald netwerk of systeem komt daar ook hoort: * Controleer overal het netwerkverkeer. * Controleer toegang per sessie. * Hanteer dynamische policies en gebruik daarbij de geldigheidsduur van de laatste authenticatie. * Blijf continue monitoren. Verzamel zoveel mogelijk gegevens om de beveiliging te blijven verbeteren. Dit wordt ook wel het 'zero-trust' model genoemd.	Blijf continue monitoren. Verzamel zoveel mogelijk gegevens om de beveiliging te blijven verbeteren.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren Ontvanger van de loginformatie.

4.4.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Security & Privacy**
1	Onderdeel van het vertrouwensmodel is onder andere eenvoudige identificatie, authenticatie, autorisatie, logging, toestemming en behandelrelatie en de rollen en verantwoordelijkheden die daarbij horen	Logging zal ingeregeld worden 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 en 2. SIEM.
2	De komende jaren gaat specifieke aandacht uit naar het voldoen aan het NEN7510 normenkader en de NIB2 richtlijn.	Wordt opgenomen als daderstellingen per bouwblok.

4.4.3 Nictiz: API Requirements for Dutch Healthcare

Nictiz API Requirements for Dutch Healthcare - Security Monitoring		
nr	**Requirement**	**Hoofdstuk**
SC005	An API MUST provide audit logging conforming to NEN 7513	API security

4.4.4 Privacy

Kaderstelling Privacy		Security Monitoring
2.5.2.1	Rechtmatigheid, behoorlijkheid en transparantie	Auditlogging, systeemlogging.
2.5.2.1	Verantwoordingsplicht	
2.5.2.3	Recht op gegevenswissing	Aantoonbaar maken dat gegevens uit systeem verwijderd zijn na verzoek tot vergetelheid.
2.5.2.4	Beveiliging van de verwerking	Geautomatiseerde protocollen betreffende de elektronische toegang tot persoonsgegevens en regelmatige controles van deze protocollen door de interne toezichthoudende afdeling.
2.5.2.4	Monitoring en logging	Real time monitoring inregelen.
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.
2.5.2.5	Registers	Verwerkingsregister creëren die voldoet aan de wettelijke eisen (op basis van audit logging).
2.5.2.5	Mogelijkheid tot volgen van data	Mogelijk maken traceren van data uitwisselingen.

4.4.5 Besluit vaststelling bewaartermijn logging

Hierbij extra benadrukt:

De logging als bedoeld in het Besluit elektronische gegevensverwerking door zorgaanbieders, wordt ten minste 5 jaar bewaard vanaf het moment dat de logregel wordt geschreven.

4.5 Kaders Privacy Enhancing Technologies (PL3b)

4.5.1 Privacy

Kaderstelling Privacy		Privacy Enhancing Technologies
2.5.2.1	Beperking van de opslag	Mogelijkheid tot anonimiseren.
2.5.2.1	Integriteit en vertrouwelijkheid	Mogelijkheid tot pseudonimiseren en versleuteling persoonsgegevens.
2.5.2.4	Beveiliging van de verwerking	
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.
2.5.2.5	Data access governance	Het platform is in staat het gebruik van gegevens te controleren, te beschermen en te auditen om de privacy te handhaven en te waarborgen.

4.6 Kaders Data services (PL4a)

4.6.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Data Services
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	Er dient een dienstbeschrijving gemaakt te worden. Als input geldt hiervoor het op te stellen domein model. Aangezien deze samen met het RIVM wordt opgesteld, wordt overlap voorkomen en aangesloten op verwante diensten.
IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie	Verwerk als afnemer gegevens uit een bronsysteem met respect voor de classificatie van die gegevens. Geef het geen hogere classificatie voor beschikbaarheid en integriteit dan de bron, en geen lagere classificatie voor vertrouwelijkheid. Maak zonodig afspraken met de aanbieder om hun classificatie aan te passen en in hun dienst bijpassende maatregelen daarvoor te implementeren.	De Data Services zijn de gegevens van de GGD-en zelf en is dus zelf een bron. In het domeinmodel dient dus BIV-classificatie per gegeven te zijn opgenomen. Het domeinmodel wordt opgeleverd vanuit functionaliteit.
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	Het domeinmodel dient rekening te houden met grondslag, doelbinding en data-minimalisatie. Dient als metadata opgenomen te worden.

IMP030 Informatie	Scheiding van datasets	Verdeel de informatie in afgebakende datasets, die ook elk afzonderlijk getoetst kunnen worden op het voldoen aan de AVG.	Datasets worden logisch gescheiden op basis van metadata uit het domeinmodel. Indien nodig met aandacht voor pseudonimisatie/anonimisatie en overige benodigdheden voor (epidemiologisch) onderzoek, zoals b.v. een ID.
IMP087 Applicatie	Verwerk bericht-interactie persistent	Zorg dat een bericht dat een mutatie tot gevolg heeft, bijvoorbeeld een bericht dat een betalingsopdracht representeert, niet verloren kan gaan. Een dergelijk 'transactioneel' bericht moet een incident als uitwijk of storing kunnen overleven. Alle onderdelen van een verwerkingsketen nemen verantwoordelijkheid voor het bericht en zorgen ervoor dat het bericht niet verloren gaat. Correcte verwerking heeft prioriteit boven verwerkingssnelheid. Persistentie houdt in dat een (transport-)transactie pas is voltooid als het bericht is opgeslagen in een 'persistent store', zoals een bestand of database. Een opvragingsbericht daarentegen heeft geen mutatie tot gevolg. Responsetijd heeft hier meer prioriteit. Bij verlies van een opvragingsbericht (door bv. een storing) wordt de opvraging opnieuw gedaan. Verwerk een opvragingsbericht daarom niet-persistent verwerkt.	Data Services moet via koppelvlak services een bevestiging sturen dat het mutatiebericht is opgeslagen.
IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's	Gegevensuitwisseling tussen (web)applicaties gebeurt via Restful API's. De broneigenaar levert API's die voldoen aan de moderne RESTful standaarden. API's dienen centraal te worden beheerd in een API management systeem.	Data Services dient data API's op te leveren. T.b.v. (web) applicaties dienen dit Restful API's te zijn.
IMP038 Informatie	Gebruik gestandaardiseerde referentiedata	Gebruik gestandaardiseerde referentiedata. Zie ook CBS referentiedata, of domeinspecifieke bronnen voor referentiedata.	Referentie naar de bron van de data dient als metadata opgenomen te worden.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van Data Services componenten.
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing t.b.v. Data Services, waarbij wel gestuurd wordt op het maximaal in controle zijn over de data.

IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk Iaas.	Voorziening realiseren als PaaS of IaaS in eigen Cloud services om zo maximaal controle te houden op de data.
IMP026 Organisatorisch	Pas je eigen proces en organisatie aan aan de standaard oplossing	Pas je processen en organisatie aan de standaard oplossingen aan, in plaats van het omgekeerde. Zie ook EIF principle 4 "Reusability", aanbeveling 6+7.	N.v.t., betreft denkwijzen vanuit applicatie centrische gedachtegang.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.

IMP001 Informatie	Beschrijf informatieobjecten in een model	Voor een optimale dienstverlening aan burgers en bedrijven en voor effectieve en efficiënte samenwerking in het leveren van diensten tussen en binnen overheidsorganisaties, is het belangrijk om een gezamenlijk beeld te hebben van de informatie die hierbinnen worden gebruikt en nodig zijn. Dit is alleen mogelijk door informatieobjecten voor een dienst, systematisch te beschrijven met behulp van een informatiemodel dat de semantiek en syntax van de gegevens vastlegt. Zo kunnen de betrokken gebruikers de relevante informatieobjecten vinden, toepassen, (her)gebruiken en archiveren. Dit betekent dat een informatiemodel minimaal bevat: Informatietypen (entiteiten) (een ordening van informatieobjecten in zogenaamde informatietypen, ook wel de hoofdstructuur (entiteiten) van het informatiemodel met hun onderlinge relaties. Attributen (een ordening elementen die binnen de entiteiten zijn of worden opgenomen met de beschrijving daarvan). Regels (een opsomming van eisen waar de entiteiten en attributen aan moeten voldoen). Maak het informatiemodel bekend in een datacatalogus die inzicht geeft in de beschikbaarheid van data. En benut visualisatiemiddelen om het model en de samenhang/relaties tussen de objecten visueel inzichtelijk te maken.	Opgeleverd vanuit functionaliteit. Het informatiemodel dient daarnaast uitgebreid te worden met een domein model, waarin alle bedrijfslogica is opgenomen. Indien mogelijk zal de tooling het model kunnen executeren, zodat alle gegevens bij de data zijn en er zoveel mogelijk automatisch data API's worden aangemaakt.
IMP021 Organisatorisch Informatie Applicatie	Bevorder hergebruik van gegevens	Maak zo veel mogelijk gebruik van gegevens die reeds beschikbaar zijn in plaats van deze gegevens opnieuw te verzamelen of te creëren.	Hergebruik gegevens die reeds beschikbaar zijn. Vanuit functionaliteit dient hier rekening mee moeten worden gehouden.
IMP049 Informatie	Draag zorg voor juiste en actuele en volledige informatie	Een gebruiker kan er op vertrouwen dat een informatieobject, zoals deze in de bron is vastgelegd, juist, actueel en volledig is. Fouten kunnen worden gemeld en hersteld. Daarbij is het van belang dat herstelwijzigingen worden gelogd, zodat traceerbaar is hoe foutieve gegevens zijn verwerkt en wat het effect daarvan is. Dit betekent dat: De kwaliteit van de informatie transparant, verankerd en geborgd moet zijn binnen de processen van de verantwoordelijke en leverende organisatie (datamanagement). Er gebruik moet worden gemaakt van gestandaardiseerde gegevensmodellen, gegevenswoordenboeken en catalogussen ten behoeve van machinematige verwerking van gegevens. De informatie tijdens de gehele levenscyclus moet worden gemonitord, gecontroleerd, gevalideerd op basis van regels, kaders, normen en standaarden waarbij wijzigingen traceerbaar moeten worden gemaakt. De informatie tijdens de gehele levenscyclus regelmatig moet worden getoetst aan wet- en regelgeving en daar verantwoording over moet worden afgelegd. Er cyclisch gerapporteerd moet worden over de	De kwaliteit van de informatie transparant, verankerd en geborgd moet zijn binnen de processen van de verantwoordelijke en leverende organisatie (datamanagement). Er gebruik moet worden gemaakt van gestandaardiseerde gegevensmodellen, gegevenswoordenboeken en catalogussen ten behoeve van machinematige verwerking van gegevens. Er cyclisch gerapporteerd moet worden over de kwaliteit van de gegevens. Voor afwijkingen moeten de juiste maatregelen worden getroffen om de betrouwbaarheid en de

		kwaliteit van de gegevens. Voor afwijkingen moeten de juiste maatregelen worden getroffen om de betrouwbaarheid en de kwaliteit van de informatie te kunnen waarborgen. De informatie moet door de gehele lifecycle gevolgd kunnen worden vanaf de oorsprong tot aan het verwerken, opslaan, bewerken en beschikbaar stellen en/of vernietigen. (data-lineage). Er gebruik moet worden gemaakt van authentieke- en/of kwalitatieve bronnen.	kwaliteit van de informatie te kunnen waarborgen. De informatie moet door de gehele lifecycle gevolgd kunnen worden vanaf de oorsprong tot aan het verwerken, opslaan, bewerken en beschikbaar stellen en/of vernietigen. (data-lineage).
IMP044 Grond slagen	Hanteer bewaartermijn en voor informatie	Informatie wordt niet langer bewaard en niet eerder vernietigd dan wettelijk is toegestaan. Dit betekent dat: Er een selectielijst is, waarin opgenomen de te vernietigen informatieobjecten of onderdelen daarvan. Er vastgesteld in de organisatie verankerd beleid is met betrekking tot vernietigen. Bevoegdheden, rollen en verantwoordelijkheden en beleid rondom vernietigen zijn belegd. De organisatie inzicht heeft in informatieobjecten, bewaartermijnen, processen, informatiesystemen en hun onderlinge samenhang.	Bevoegdheden, rollen en verantwoordelijkheden en beleid rondom vernietigen zijn belegd. En proces: selectielijst
IMP051 Inform atie	Leg auditlogs vast bij de bronregistratie van het gegeven	Als eigenaar van de bron wil je inzicht hebben in de toegang en inzage (CRUD) van de gegevens die vanuit de bron worden gebruikt. Voorkom dat auditgegevens verspreid raken over afnemende applicaties.	Leg auditlogs vast bij de bronregistratie van het gegeven.
IMP048 Inform atie	Leg de context van een informatieobje ct vast in metadata	Informatie-objecten moeten goed worden beheerd. Onderdeel hiervan is dat de context van een informatieobject goed moet zijn vastgelegd in metadata. Informatie en gegevens moeten duidelijk binnen een bepaalde context te plaatsen zijn. Metadata is daar het passende instrument voor. Context (vastgelegd in metadata) is nodig om gegevens te begrijpen voor verwerking. Zie DUTO eisen (ISO 23081)	TiVi dient hier vanuit onderdeel van informatie/domein model rekening mee te houden.
IMP050 Inform atie	Maak gegevens herleidbaar tot de bron (herkomst)	Dit betekent dat inzichtelijk gemaakt moet worden hoe gegevens tot stand zijn gekomen, over de gehele verwerking in de keten heen. Dus van bronnen tot eindproduct. Van ieder gegeven zijn de herkomst en verwerkingen beschikbaar tot aan vernietiging	Dit betekent dat inzichtelijk gemaakt moet worden hoe gegevens tot stand zijn gekomen, over de gehele verwerking in de keten heen. Dus van bronnen tot eindproduct. Van ieder gegeven zijn de herkomst en verwerkingen beschikbaar tot aan vernietiging.

IMP003 Grondslagen Informatie	Maak zoveel mogelijk data beschikbaar als open data [Definitie open data: Data is open als iedereen er gratis gebruik van kan maken, deze kan hergebruiken en kan verspreiden zonder juridische, sociale of technologische beperkingen.]	Stel overheidsdata actief beschikbaar voor hergebruik door derden, bijvoorbeeld in de vorm van open data. Beschouw dit aanbod als een dienst. De enige uitzondering zijn overheidsdata waarvoor wet- en regelgeving expliciet beperkingen oplegt, die stel je niet actief beschikbaar. Vanuit o.a. de WOO richt de overheid zich op transparantie. Daarbij hoort het actief beschikbaar stellen dan wel delen van data. Wel met inachtneming van de beperkingen die daarbij gelden (bijv. vanuit de AVG). Er zijn meerdere redenen om data actief beschikbaar te stellen. Zo kan het meer transparantie en inzicht geven in het overheidshandelen en zo de accountability vergroten. Bijvoorbeeld door begrotingen of inkoopgegevens als open data beschikbaar te stellen. Het kan ook economische en maatschappelijke innovatie stimuleren, zoals de ontwikkeling van apps en informatiediensten op basis van overheidsdata.	Daarbij hoort het actief beschikbaar stellen dan wel delen van data. Wel met inachtneming van de beperkingen die daarbij gelden (bijv. vanuit de AVG).
IMP047 Informatie	Pas de FAIR dataprincipes toe	Pas de implicaties van de FAIR dataprincipes toe. Zie ook go.fair.org FAIR-principes.	FAIR principes toepassen.
IMP052 Applicatie	Sla informatie op in een duurzaam toegankelijk bestandsformaat	Informatie moet toegankelijk zijn voor gebruikers, zowel mens als machine. Hiervoor moeten de gebruikers geen speciale toepassingen of hulpmiddelen nodig hebben. Daarbij moet het formaat waar de informatie in wordt opgeslagen toekomstbestendig zijn, zodat de informatie ook in de toekomst nog toegankelijk is. Dit betekent dat: Gebruik wordt gemaakt van een open standaard. Bij doorontwikkeling van de gebruikte formaten, het originele bronbestand opgeslagen blijft in zijn huidige formaat en het voorlaatste bestandformaat actief wordt gemigreerd naar het nieuwe formaat. Er voor het gebruik van het bestandsformaat geen afhankelijkheid is van één enkele leverancier en het onafhankelijk van hulpmiddelen of speciale toepassingen te gebruiken is. Het bestandsformaat goed is gedocumenteerd. Het formaat het eenvoudig uitwisselen met andere platforms en apparaten ondersteunt. Fouten in de bitopslag automatisch gedetecteerd kunnen worden en te herstellen zijn. Het formaat op grote schaal gebruikt wordt.	Gebruik wordt gemaakt van een open standaard. Bij doorontwikkeling van de gebruikte formaten, het originele bronbestand opgeslagen blijft in zijn huidige formaat en het voorlaatste bestandformaat actief wordt gemigreerd naar het nieuwe formaat. Er voor het gebruik van het bestandsformaat geen afhankelijkheid is van één enkele leverancier en het onafhankelijk van hulpmiddelen of speciale toepassingen te gebruiken is. Het bestandsformaat goed is gedocumenteerd. Het formaat het eenvoudig uitwisselen met andere platforms en apparaten ondersteunt. Het formaat op grote schaal gebruikt wordt.
IMP073 Informatie	Stel van ieder gegeven de kwaliteit vast	Stel voor ieder gegeven de kwaliteit vast volgens kenmerken van compleetheid, actualiteit en tijdigheid.	Functionaliteit dient voor ieder gegeven de kwaliteit vast te stellen volgens kenmerken van compleetheid, actualiteit en tijdigheid.
IMP058 Informatie	Stel voor ieder gegeven de unieke bron vast	Het niet hebben van een 'single point of truth (SPOT)' kan leiden tot divergerende data en mogelijk tot inconsistente beslissingen die op basis van de verschillende databronnen worden genomen.	Stel voor ieder gegeven de unieke bron vast.
IMP046 Organi	Stel één verantwoordeli	Voor ieder gegeven en voor iedere verwerking moet er een verantwoordelijke gegevenseigenaar zijn. Dat	Functionaliteit dient één verantwoordelijke vast te

satoris ch	jke vast voor ieder gegeven	vraagt een inventarisatie van alle relevante gegevensobjecten.	stellen voor ieder gegeven.
IMP060 Applic atie	Bepaal autorisaties met metadata	Autorisaties voor het verstrekken en gebruik van gegevens kan worden bepaald op basis van metadata. De beheerder die het gegeven beheert en het wil verstrekken voor verdere bewerking, voegt metadata toe aan de hand waarvan de beheerder en de afnemer een autorisatiebeslissing kan nemen.	Functionaliteit dient hier als onderdeel van informatie/domein model rekening mee te houden.
IMP055 Organi satoris ch	Gegevens eenmalig uitgevraagd, uniek opgeslagen, meervoudig gebruikt	Gegevens worden eenmalig uitgevraagd of verzameld, uniek opgeslagen, en vervolgens meervoudig gebruikt. Dit impliceert tevens dat de juistheid van de gebruikte informatie-objecten uit een bronregistratie niet voor gebruik opnieuw hoeft te worden gecontroleerd.	Indien gegevens van andere bronnen worden 'ingeladen' dient de bron bij die gegevens als metadata opgenomen te worden.
IMP056 Organi satoris ch Inform atie	Registreer gegevens bij de bron	Registreer gegevens (zo dicht mogelijk) bij de bron, daar waar de gegevens ontstaan. Dit verhoogt de volledigheid, kwaliteit en de actualiteit van de gegevens aanzienlijk en voorkomt fouten. De vastgelegde gegevens kunnen daarna voor verschillende doeleinden worden gebruikt. Een ander belangrijk voordeel is dat het achteraf registreren van gegevens die eerder zijn ontstaan wordt voorkomen hetgeen de registratielast vermindert. Waar mogelijk, leg gegevens geautomatiseerd vast.	Vanuit het domeinmodel (functionaliteit) zoveel mogelijk direct doorverwijzen naar de bron i.p.v. kopie 'inladen'.
IMP077 Organi satoris ch	Stel de juridische aansprakelijkh eid per gegevensobje ct vast	Stel per informatie-object de bron vast, en daarmee de juridische aansprakelijkheid voor de juistheid van het object.	In domeinmodel wordt aangegeven van welke informatie objecten GGD of RIVM zelf bronhouder is. Indien gegevens van andere bronnen worden 'ingeladen' dient de bron bij die gegevens als metadata opgenomen te worden.
IMP007 Inform atie	Verwijs naar de bron	Verwijzen naar de bron heeft voorkeur boven een kopie uit die bron. Inzage in de bron heeft de voorkeur boven zelf opslaan. Afspraken daarover worden vastgelegd en bekend gemaakt. Vanuit legitimiteitsperspectief kan het nodig zijn een kopie vast te leggen.	Vanuit het domeinmodel (functionaliteit) zoveel mogelijk direct doorverwijzen naar de bron i.p.v. kopie 'inladen'.
IMP057 Inform atie	Weet welke (bron)gegeven s in huis zijn	Weet welke gegevens de overheid of overheidsorganisatie al in huis heeft in de bronadministraties en op welke manier deze gegevens hergebruikt kunnen worden.	Maak gebruik van register van gegevens die bij de overheid of overheidsorganisaties in huis zijn en hoe deze hergebruikt kunnen worden.
IMP045 Grond slagen	Leg de doelbinding vast in de metadata van het gegevensobje ct	De verwerkingshistorie inclusief doel van verwerking wordt vastgelegd bij het gegevensobject als metadata. Dit betekent dat de historie van acties waarin een gegevensobject wordt verwerkt (opvragen / vastleggen / wijzigen / verwijderen) inclusief het doel van de actie vastgelegd wordt bij het gegevensobject.	Verwerkingen worden vastgelegd in Data Services.
IMP054 Inform atie	Leg de grondslag en het doel van de gegevensverw erking vast	Leg de grondslag en het doel vast, waarvoor informatie wordt uitgevraagd bij burgers en bedrijven. Aan het doel gekoppeld worden ook de eisen (kwaliteitscriteria) vastgelegd waaraan deze informatie moet voldoen. Houd er rekening mee dat het doel in de loop der tijd kan wijzigen.	Metadata waarin grondslag en doel worden opgenomen dienen gedefinieerd te worden in het domeinmodel.
IMP004 Grond slagen	Minimaliseer het gebruik van gegevens	Verzamel of vraag alleen die gegevens op die nodig zijn voor het strikte doel van de dienstverlening. En houd de gegevensverwerking die hierop volgt in proportie met het doel. Dit voorkomt dat	Access management - procesbouwblok is onderdeel van

Informatie		vertrouwelijke of privacygevoelige gegevens onnodig worden verwerkt.	domeinmodel onderdeel van de autorisatie.
IMP022 Grondslagen	Neem oorspronkelijke grondslag mee bij hergebruik diensten	Bij hergebruik van diensten kijken zowel aanbieder als afnemer opnieuw naar de oorspronkelijke grondslag en doelbinding. Als dat nodig blijkt passen zij pseudonimisering dan wel anonimisering van de data toe. Dit houdt in dat bij te ontwikkelen functionaliteit de oorspronkelijke grondslag bepalend is voor de hergebruikmogelijkheden.	Metadata waarin grondslag en doel worden opgenomen dienen gedefinieerd te worden in het domeinmodel.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. Data Services worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.
IMP080 Informatie	Controleer de verwerking van gegevens	Controleer de verwerking van gegevens: * Zijn de criteria voor juistheid, en tijdigheid vastgesteld? * Worden gegevens die vanuit een systeemvreemde omgeving ingevoerd zijn eerst gecontroleerd op juistheid, tijdigheid en volledigheid, voordat verdere verwerking plaatsvindt? * Worden te versturen gegevens gecontroleerd op juistheid, volledigheid en tijdigheid? * Worden ter verwerking aangeboden gegevens gecontroleerd op juiste, volledig en tijdige verwerking? * Worden kritieke gegevens die in verschillende gegevensverzamelingen voorkomen periodiek met elkaar vergeleken op consistentie? (Dit geldt alleen zolang de gegevens niet frequent en integraal worden gesynchroniseerd met de brongegevens)	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok. Wel moet het bouwblok in de rules services de criteria m.b.t. juistheid vanuit het domeinmodel kunnen afdwingen.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.

IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats.
IMP064 Applicatie	Stel onweerlegbaarheid vast	Stel vast voor welke berichtenstromen of transacties onweerlegbaarheid van gegevens vereist is, zodat daarvoor aanvullende maatregelen genomen kunnen worden.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP069 Netwerk	Hanteer het zero-trust model	Ga nooit uit van het impliciete vertrouwen dat wie op een bepaald netwerk of systeem komt daar ook hoort: * Controleer overal het netwerkverkeer. * Controleer toegang per sessie. * Hanteer dynamische policies en gebruik daarbij de geldigheidsduur van de laatste authenticatie. * Blijf continue monitoren. Verzamel zoveel mogelijk gegevens om de beveiliging te blijven verbeteren. Dit wordt ook wel het 'zero-trust' model genoemd.	Dynamische policies ook op basis van business rules gedefinieerd in het domein model.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.
IMP065 Informatie	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces	Controleer de kwaliteit van gegevens vanaf invoer en op ieder koppelvlak aan de hand van de vastgestelde kwaliteitseisen. Eenmaal geverifieerd hoeft een verificatie niet opnieuw plaats te vinden als de eerder uitgevoerde verificatie nog betrouwbaar is.	Controle van gegevens m.b.t. metagegevens uit domeinmodel (invoer en uitvoer regels).

4.6.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Data Services**
1	Gezondheidsdata die in informatiesystemen opgesloten zit, moet volgens de FAIR-principes beschikbaar worden voor primair en secundair gebruik.	Wordt afgehandeld via NORA principe.

2	Dit betekent onder andere het gebruik van (op inhoud gestandaardiseerde) API's Hierbij hoort ook een eenheid van taal (zib-) en API-strategie om de gestandaardiseerde toegang tot data te realiseren	Zie ook NORA, gebruik gestandaardiseerde API's.
3	In het IZA is afgesproken dat de gestandaardiseerde (open) API-strategie van Nictiz leidend wordt in de wijze van openstelling van systemen.	De API Requirements for Dutch Healthcare van Nictiz is opgenomen in de kaders.

4.6.3 Nictiz: API Requirements for Dutch Healthcare

Nictiz API Requirements for Dutch Healthcare - Data Services		
nr	**Requirement**	**Hoofdstuk**
SD001	API documentation MUST be publicly and freely available	API specification & documentation
SD002	API documentation MUST provide examples of how to use the API	API specification & documentation
SD003	API documentation SHOULD provide examples of input and output data	API specification & documentation
SD004	API documentation SHOULD include a FAQ page for API client developers	API specification & documentation
SD005	API documentation MAY specify cases in which API usage is not applicable	API specification & documentation
SD008	API specifications SHOULD be machine readable and allow for automated code generation	API specification & documentation
SD009	API documentation MUST be published in English	API specification & documentation
SD010	When documentation claims compliance to standards, specifications, guidelines and practices, policies or law, documentation MUST provide (references to) evidence to back up these claims	API specification & documentation
SD011	Content relationship MUST be described in API documentation	API specification & documentation
SD012	API documentation MUST describe the availability and usage of operations	API specification & documentation
SD013	API versioning policy MUST be documented	API specification & documentation
SD014	API specifications MUST cover the rationale behind the exchange paradigm used by the API	API specification & documentation
LM008	An API specification MUST comply with Semantic Versioning specification (SemVer) version 2.0.0	API Lifecycle management and versioning
AG003	Data Processing Policies MUST be openly and freely available	API agreements
DR001	Interfaces MUST be defined in English	API design rules
DR002	Developers MUST only apply standard HTTP methods	API design rules
DR003	Developers MUST adhere to HTTP safety and idempotency semantics for operations	API design rules
DR004	Server communication MUST remain stateless	API design rules
DR005	Content relationship MUST be predictably implemented	API design rules
DR006	Operations MUST be predictably implemented	API design rules
DR007	API version MUST be accessible through the API	API design rules
DR008	APIs MUST at least support the DEFLATE and gzip compression algorithms	API design rules
DR009	APIs MUST support the use of HTTP Accept-Encoding and Content-Encoding header fields for negotiating compression	API design rules
DR011	JSON formatted content SHOULD comply to RFC 8259 or its successor	API design rules
DR012	When describing an API where data is being transferred to another party, the NOTIFIED PULL exchange pattern SHOULD be used rather than the PUSH exchange pattern	API design rules
DR013	System APIs SHOULD be designed independent of specific use cases and types of client systems or users	API design rules
DR016	System APIs SHOULD be based on the operations, messaging, or resource paradigm rather than the document paradigm	API design rules
DR-S001	APIs MAY use MTOM/XOP for formatting binary data	API design rules - SOAP
DR-S002	API clients MUST support MTOM/XOP formatting of binary data	API design rules - SOAP

DR-R001	APIs MUST use nouns to name resources	API design rules - RESTful
DR-R002	APIs MUST use singular nouns to name collection resources	API design rules - RESTful
DR-R003	APIs MUST hide irrelevant implementation details	API design rules - RESTful
DR-R004	APIs MUST support both JSON and XML formatting	API design rules - RESTful
DR-R005	API clients MUST at least support JSON or XML formatting	API design rules - RESTful
DR-R006	APIs MAY support BSON formatting	API design rules - RESTful
DR-R007	APIs MUST use the Accept header for content negotiation	API design rules - RESTful
DR-R008	APIs MUST use the Content-Type header for content negotiation	API design rules - RESTful
SC001	API specifications MUST comply with Dutch NCSC guidelines for web applications	API security
SC002	API implementations MUST comply with Dutch NCSC guidelines for web applications	API security
SC003	API deployments MUST comply with Dutch NCSC guidelines for web applications	API security
SC004	API deployments MUST comply with Dutch NCSC guidelines for Transport Layer Security	API security
SC005	An API MUST provide audit logging conforming to NEN 7513	API security
SC006	Specifications for 'System APIs' MUST use authentication and authorization models that are not specific to a use case or (type of) client or user	API security
SC007	APIs MUST use fully standardized models for identification and authentication	API security
SC-S001	APIs SHOULD use WS-Security to ensure message confidentiality and integrity for adding security tokens	API security - SOAP
SC-S002	APIs SHOULD use the SAML Token Security Model	API security - SOAP
SC-R001	APIs MUST comply with RFC 7523 or its successor for client authentication and for requesting OAuth 2 access tokens	API security - RESTful
SC-R002	APIs SHOULD use OpenID Connect to achieve Single-Sign-On when requesting OAuth access tokens	API security - RESTful
SC-R003	JWT tokens used for client authentication and authorization grants MUST comply with RFC 7515 and RFC 7518, or its successors	API security - RESTful

4.6.4 Privacy

Kaderstelling Privacy		Data Services
2.5.2.1	Rechtmatigheid, behoorlijkheid en transparantie	Metadata domeinmodel met gegevens grondslag en velden t.b.v. auditlogging.
2.5.2.1	Doelbinding	Metadata domeinmodel met gegevens doelbinding.
2.5.2.3	Recht van inzage	
2.5.2.5	Privacy by design & Privacy by default	
2.5.2.1	Juistheid van gegevens	Bij ingebruikname domeinmodel afdwingen dat bepaalde velden verplicht een waarde moeten hebben.
2.5.2.1	Juistheid van gegevens	Mogelijkheid bedrijfsregels.
2.5.2.1	Beperking van de opslag	Metadata domeinmodel met gegevens bewaartermijn en wat er moet gebeuren na verstrijken bewaartermijn.
2.5.2.3	Recht van inzage	
2.5.2.5	Privacy by design & Privacy by default	
2.5.2.5	Bewaartermijnen	
2.5.2.2	Verwerken van bijzondere persoonsgegevens	Metadata domeinmodel met gegevens onderscheidt gewone en bijzondere persoonsgegevens, en mogelijke uitzonderingsgrond.
2.5.2.3	Recht van inzage	
2.5.2.3	Recht van inzage	Metadata domeinmodel met gegevens van ontvangers aan wie persoonsgegevens worden verstrekt.
2.5.2.3	Recht van inzage	Metadata domeinmodel met gegevens van bron van die gegevens.
2.5.2.3	Recht van inzage	Indien er gebruik wordt gemaakt van automatische besluitvorming, moet uitgelegd kunnen worden hoe dat tot stand komt.
2.5.2.3	Recht van inzage	Metadata domeinmodel met gegevens over identificeerbaarheid van gegevens.
2.5.2.3	Recht op rectificatie	Metadata domeinmodel met gegevens van classificatie.
2.5.2.5	Privacy by design & Privacy by default	Metadata domeinmodel met gegevens over de toegankelijkheid van gegevens .
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

2.5.2.5	Kennisgeving bij een inbreuk in verband met persoonsgegevens	Het moet mogelijk zijn om op korte termijn (binnen 24 uur) alle informatie te verzamelen zodra er een inbreuk optreedt.
2.5.2.5	Registers	Metadata domeinmodel met gegevens benodigd voor verwerkingsregister.
2.5.2.6	Eisen bij EPD	Voor het platform betekent dit dat wanneer er sprake is van een Elektronisch Patiënten Dossier (EPD), er de mogelijkheid moet zijn om het gehele dossier of delen daarvan te verwijderen.

4.7 Kaders Opslag services (PL4b)

4.7.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Opslag Services
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	N.v.t. Betreft een 'basisvoorziening' dienst. Deze dient wel als dienst beschreven te worden.
IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie	Verwerk als afnemer gegevens uit een bronsysteem met respect voor de classificatie van die gegevens. Geef het geen hogere classificatie voor beschikbaarheid en integriteit dan de bron, en geen lagere classificatie voor vertrouwelijkheid. Maak zonodig afspraken met de aanbieder om hun classificatie aan te passen en in hun dienst bijpassende maatregelen daarvoor te implementeren.	Maatregelen implementeren op basis van BIV-classificatie bron. Hier gaat het dus met name om de eigen Data Services.
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	N.v.t. Betreft een 'basisvoorziening' dienst.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van Opslag services componenten.

IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing t.b.v. Opslag Services.
IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk Iaas.	Betreft PaaS of IaaS op Cloud Services.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.

IMP052 Applicatie	Sla informatie op in een duurzaam toegankelijk bestandsformaat	Informatie moet toegankelijk zijn voor gebruikers, zowel mens als machine. Hiervoor moeten de gebruikers geen speciale toepassingen of hulpmiddelen nodig hebben. Daarbij moet het formaat waar de informatie in wordt opgeslagen toekomstbestendig zijn, zodat de informatie ook in de toekomst nog toegankelijk is. Dit betekent dat: Gebruik wordt gemaakt van een open standaard. Bij doorontwikkeling van de gebruikte formaten, het originele bronbestand opgeslagen blijft in zijn huidige formaat en het voorlaatste bestandformaat actief wordt gemigreerd naar het nieuwe formaat. Er voor het gebruik van het bestandsformaat geen afhankelijkheid is van één enkele leverancier en het onafhankelijk van hulpmiddelen of speciale toepassingen te gebruiken is. Het bestandsformaat goed is gedocumenteerd. Het formaat het eenvoudig uitwisselen met andere platforms en apparaten ondersteunt. Fouten in de bitopslag automatisch gedetecteerd kunnen worden en te herstellen zijn. Het formaat op grote schaal gebruikt wordt.	Fouten in de bitopslag automatisch gedetecteerd kunnen worden en te herstellen zijn.
IMP002 Informatie	Voorkom verlies van informatie	Veranderingen in techniek, organisatie of gebruikerswensen mogen niet van negatieve invloed zijn op de duurzame toegankelijkheid van informatie. Hetzelfde geldt voor bitrot (verlies van informatie door verval van opslagmedia). Neem vooraf maatregelen om informatie toekomstbestendig te maken, zodat deze toegankelijk blijft voor de van toepassing zijnde vormen van (her)gebruik. Dit betekent dat: Leveranciersafhankelijkheid wordt voorkomen. Analyse wordt gemaakt van welke gevolgen veranderingen (in techniek, organisatie, of gebruikerswensen) hebben voor de duurzame toegankelijkheid van informatie. Bij het ontwerpen van informatiesystemen na wordt gedacht over de te gebruiken technologie voor het beheren van informatie.	De Opslag Services en de onderliggende opslagmedia dienen bitrot te voorkomen.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheids eisen t.a.v. deze dienst worden volledig bepaald door de beschikbaarheids eisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheids eisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot	Scheiding van systeemfuncties, controle op communicatiege

		gegevens en systeemfuncties en door versleuteling van gegevens.	drag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats.
IMP084 Applicatie	Versleutel gegevens in rust en transport	Versleutel alle gegevensdragers waarop niet-publieke informatie staat, inclusief smartphones en laptops, conform de laatst bekende en geldende richtlijnen. Dit reduceert het risico op een gegevenslek bij verlies van een dergelijk apparaat. Neem voor niet-publieke gegevens ook adequate beveiligingsmaatregelen om ze te beschermen in transit. Dit kan door de verbinding te beveiligen, danwel door encryptie van de informatie zelf. Dit laatste heeft de voorkeur.	Versleutel gegevens in rust.
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden.	Systeemlogging aanleveren.

		Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	

4.7.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Opslag Services**
1	Er wordt gebruik gemaakt van internationale standaarden voor eenheid van taal, opslag en transport van data.	Internationale standaarden voor opslag dienen gebruikt te worden.

4.7.3 Privacy

Kaderstelling Privacy		Opslag Services
2.5.2.1	Beperking van de opslag	Automatisch verwijderen of anonimiseren op basis van bewaartermijn.
2.5.2.5	Bewaartermijnen	
2.5.2.1	Integriteit en vertrouwelijkheid	Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
2.5.2.4	Beveiliging van de verwerking	
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

4.8 Kaders Koppel Services (PL5)

4.8.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Koppel Services
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	Er dient een dienstbeschrijving gemaakt te worden. Tevens is dit de plek hoe data aangeleverd kan worden. Verschillende technieken zoals web API's, messaging en SFTP dienen beschreven te worden inclusief hoe deze gebruikt kunnen worden.
IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie	Verwerk als afnemer gegevens uit een bronsysteem met respect voor de classificatie van die gegevens. Geef het geen hogere classificatie voor beschikbaarheid en integriteit dan de bron, en geen lagere classificatie voor vertrouwelijkheid. Maak zonodig afspraken met de aanbieder om hun classificatie aan te passen en in hun dienst bijpassende maatregelen daarvoor te implementeren.	Het ontsluiten van de eigen data, gecombineerd met de Data Intelligence Services en de plek waar andere bronnen hun data aanleveren. Per subonderdeel zal de BIV vastgesteld moeten worden, maar in ieder geval dient deze technisch aangepast te kunnen worden indien hogere waardes van toepassing zijn.

IMP087 Applicatie	Verwerk bericht-interactie persistent	Zorg dat een bericht dat een mutatie tot gevolg heeft, bijvoorbeeld een bericht dat een betalingsopdracht representeert, niet verloren kan gaan. Een dergelijk 'transactioneel' bericht moet een incident als uitwijk of storing kunnen overleven. Alle onderdelen van een verwerkingsketen nemen verantwoordelijkheid voor het bericht en zorgen ervoor dat het bericht niet verloren gaat. Correcte verwerking heeft prioriteit boven verwerkingssnelheid. Persistentie houdt in dat een (transport-)transactie pas is voltooid als het bericht is opgeslagen in een 'persistent store', zoals een bestand of database. Een opvragingsbericht daarentegen heeft geen mutatie tot gevolg. Responsetijd heeft hier meer prioriteit. Bij verlies van een opvragingsbericht (door bv. een storing) wordt de opvraging opnieuw gedaan. Verwerk een opvragingsbericht daarom niet-persistent verwerkt.	In te richten technieken zoals API Gateway en Messaging service dienen dermate ingericht te worden dat mutatieberichten niet verloren kunnen gaan.
IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's	Gegevensuitwisseling tussen (web)applicaties gebeurt via Restful API's. De broneigenaar levert API's die voldoen aan de moderne RESTful standaarden. API's dienen centraal te worden beheerd in een API management systeem.	De data API's worden beschikbaar gesteld via de Koppel Services, waar dus ook een API-management systeem ingericht moet worden.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Eisen aan organisatie GGD GHOR NL: Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van Koppel services componenten.
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing(en) t.b.v. Koppel Services.

IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk Iaas.	Voorziening afnemen als SaaS, indien PaaS of IaaS laten landen op Cloud Services.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.

IMP003 Grondslagen Informatie	Maak zoveel mogelijk data beschikbaar als open data [Definitie open data: Data is open als iedereen er gratis gebruik van kan maken, deze kan hergebruiken en kan verspreiden zonder juridische, sociale of technologische beperkingen.]	Stel overheidsdata actief beschikbaar voor hergebruik door derden, bijvoorbeeld in de vorm van open data. Beschouw dit aanbod als een dienst. De enige uitzondering zijn overheidsdata waarvoor wet- en regelgeving expliciet beperkingen oplegt, die stel je niet actief beschikbaar. Vanuit o.a. de WOO richt de overheid zich op transparantie. Daarbij hoort het actief beschikbaar stellen dan wel delen van data. Wel met inachtneming van de beperkingen die daarbij gelden (bijv. vanuit de AVG). Er zijn meerdere redenen om data actief beschikbaar te stellen. Zo kan het meer transparantie en inzicht geven in het overheidshandelen en zo de accountability vergroten. Bijvoorbeeld door begrotingen of inkoopgegevens als open data beschikbaar te stellen. Het kan ook economische en maatschappelijke innovatie stimuleren, zoals de ontwikkeling van apps en informatiediensten op basis van overheidsdata.	Daarbij hoort het actief beschikbaar stellen dan wel delen van data. Wel met inachtneming van de beperkingen die daarbij gelden (bijv. vanuit de AVG). Dus API's om data te benaderen evt. beschikbaar stellen voor anonieme toegang.
IMP059 Informatie	Geef de voorkeur aan halen i.p.v. brengen van gegevens	Geef de voorkeur aan het halen (pull) i.p.v. het brengen van gegevens (push).	Te realiseren: API Gateway, API Management & SFTP koppelservices. Messaging (push) zal nodig zijn, maar de afweging dient hiervoor gemaakt en geborgd te worden.
IMP056 Organisatorisch Informatie	Registreer gegevens bij de bron	Registreer gegevens (zo dicht mogelijk) bij de bron, daar waar de gegevens ontstaan. Dit verhoogt de volledigheid, kwaliteit en de actualiteit van de gegevens aanzienlijk en voorkomt fouten. De vastgelegde gegevens kunnen daarna voor verschillende doeleinden worden gebruikt. Een ander belangrijk voordeel is dat het achteraf registreren van gegevens die eerder zijn ontstaan wordt voorkomen hetgeen de registratielast vermindert. Waar mogelijk, leg gegevens geautomatiseerd vast.	Via de Koppel Services moet het mogelijk zijn te registreren in bronnen van externe partijen.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. deze dienst worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang

			en versleuteling van gegevens.
IMP080 Informatie	Controleer de verwerking van gegevens	Controleer de verwerking van gegevens: * Zijn de criteria voor juistheid, en tijdigheid vastgesteld? * Worden gegevens die vanuit een systeemvreemde omgeving ingevoerd zijn eerst gecontroleerd op juistheid, tijdigheid en volledigheid, voordat verdere verwerking plaatsvindt? * Worden te versturen gegevens gecontroleerd op juistheid, volledigheid en tijdigheid? * Worden ter verwerking aangeboden gegevens gecontroleerd op juiste, volledig en tijdige verwerking? * Worden kritieke gegevens die in verschillende gegevensverzamelingen voorkomen periodiek met elkaar vergeleken op consistentie? (Dit geldt alleen zolang de gegevens niet frequent en integraal worden gesynchroniseerd met de brongegevens)	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok. Koppel Services moeten wel voorzien in de mechanismen om juiste en volledige levering van data te controleren en waar mogelijk te garanderen.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP064 Applicatie	Stel onweerlegbaarheid vast	Stel vast voor welke berichtenstromen of transacties onweerlegbaarheid van gegevens vereist is, zodat daarvoor aanvullende maatregelen genomen kunnen worden.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP084 Applicatie	Versleutel gegevens in rust en transport	Versleutel alle gegevensdragers waarop niet-publieke informatie staat, inclusief smartphones en laptops, conform de laatst bekende en geldende richtlijnen. Dit reduceert het risico op een gegevenslek bij verlies van een dergelijk apparaat. Neem voor niet-publieke gegevens ook adequate beveiligingsmaatregelen om ze te beschermen in transit. Dit kan door de verbinding te beveiligen, danwel door encryptie van de informatie zelf. Dit laatste heeft de voorkeur.	Versleutel gegevens in transport.
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.

IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.
IMP065 Informatie	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces	Controleer de kwaliteit van gegevens vanaf invoer en op ieder koppelvlak aan de hand van de vastgestelde kwaliteitseisen. Eenmaal geverifieerd hoeft een verificatie niet opnieuw plaats te vinden als de eerder uitgevoerde verificatie nog betrouwbaar is.	Controle van geautomatiseerde invoer.

4.8.2 MedMij

Bron: MedMij		
Zie hiervoor Actuele gegevensdiensten - MedMij Catalogus - MedMij Afsprakenstelsel		
1.	Via de Koppel Services moet het mogelijk zijn gegevens aan te leveren aan PGO-omgevingen volgens de MedMij informatiestandaarden die met name gebruik maken van het communicatieprotocol FHIR.	Eis aan informatiestandaard en communicatieprotocol.

4.8.3 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Koppel Services**
1	Effectieve uitwisseling vraagt om eenheid van taal en techniek, zodat data begrepen wordt en bruikbaar is. Daarom is de Wegiz ook een belangrijke aanjager die er mede voor zorgt dat data beschikbaar komt.	Eenheid van techniek dient toegepast te worden.
2	Door drempelvrije, eenvoudige controle voor burgers en zorgverlener op de navolging van afspraken en richtlijnen.	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
3	Alle betrokkenen in het netwerk van een persoon moeten de mogelijkheid hebben de data in die dossiers te kunnen raadplegen en gebruiken. Maar alleen als zij daartoe geautoriseerd zijn en die gegevens nodig hebben voor het leveren van passende hybride zorg met waarborgen voor patiëntveiligheid.	Aansluiting LSP dient gerealiseerd te worden.
4	De burger zelf heeft recht op inzage in én gebruik van alle over hem geregistreerde en uitgewisselde gegevens	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
5	Deelnemers in het zorgnetwerk worden door hun systemen gefaciliteerd in het vastleggen van data en gebruik van eigen en andermans data door een gebruiksvriendelijke inrichting, een vertaalslag naar relevante, begrijpelijke informatie en het bieden van de juiste functionaliteit om hun rol in het netwerk te kunnen vervullen	Kunnen gebruiken van andermans data. Vertaalslag (translatie) dient dit te realiseren.
6	Partijen in het zorgnetwerk zijn aangesloten op de landelijk dekkende en nationaal vastgestelde infrastructuren. Dit zodat zij elkaar eenvoudig kunnen bereiken, gegevens kunnen delen en ondersteund worden in de samenwerking	Aansluiting LSP dient gerealiseerd te worden.
7	Bij eenmalige registratie leg je data op een gestandaardiseerde manier vast (eenheid van taal) en wordt deze vervolgens op een standaard manier ontsloten (Eenheid van Techniek) voor secundair gebruik.	Eenheid van techniek dient toegepast te worden.
8	Beschikbaar stellen van data ten behoeve van anderen in het zorgnetwerk wordt verplicht. Niet alleen voor betrokkenen in het netwerk, maar ook ten behoeve van het algemeen maatschappelijk belang. Dit heeft gevolgen voor besluiten over toestemming en bezwaren. Alleen als de persoon	Aansluiting LSP dient gerealiseerd te worden.

	expliciet de toegang tot zorg- en gezondheidsdata weigert, komen data niet beschikbaar	
9	Onderdeel van het vertrouwensmodel is onder andere eenvoudige identificatie, authenticatie, autorisatie, logging, toestemming en behandelrelatie en de rollen en verantwoordelijkheden die daarbij horen	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
10	Er wordt gebruik gemaakt van internationale standaarden voor eenheid van taal, opslag en transport van data	Internationale standaarden voor eenheid van taal en transport van data.
11	Dit betekent onder andere het gebruik van (op inhoud gestandaardiseerde) API's Hierbij hoort ook een eenheid van taal (zib-) en API-strategie om de gestandaardiseerde toegang tot data te realiseren	Zie ook NORA, gebruik gestandaardiseerde API's.
12	Daarbij horen ook afspraken over landelijk dekkende infrastructuren. Er loopt momenteel een onderzoek naar scenario's om gegevensuitwisseling versneld te faciliteren met een landelijk dekkend netwerk	Afspraken koppelingen netwerken dienen gemaakt of gevolgd te worden.
13	(Inter)nationaal vastgestelde gestandaardiseerde koppelingen (API's)	Er dienen (inter)nationaal vastgestelde gestandaardiseerde koppelingen (API's) opgeleverd te worden.
14	Een (inter)nationaal vastgesteld stelsel van onderling verbonden infrastructuren	Er dient een (inter)nationaal vastgesteld stelsel van onderling verbonden infrastructuren gerealiseerd te worden waarop wordt aangesloten.
15	In het IZA is afgesproken dat de gestandaardiseerde (open) API-strategie van Nictiz leidend wordt in de wijze van openstelling van systemen.	De API Requirements for Dutch Healthcare van Nictiz is opgenomen in de kaders.
16	Persoonlijke gezondheidsomgevingen (PGO's) kunnen voorzien in deze behoefte.	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
17	Door een expliciete scheiding te maken tussen de standaarden voor de inhoud (Eenheid van taal) en de standaarden voor datatransport (Eenheid van Techniek) ontstaat er meer stabiliteit in het ecosysteem en kan de betekenis van de data voor een langere tijd worden gegarandeerd.	Eenheid van techniek dient toegepast te worden.
18	ZORG-AB voor adressering (en de verbinding met Lrza)	Verbinding met Lrza dient gerealiseerd te worden.
19	1 lokalisatievoorziening om te kunnen achterhalen waar patiëntgegevens terug te vinden zijn (vergelijkbaar met mijnpensioenoverzicht.nl)	Registerfunctionaliteit dient gerealiseerd/gebruikt te worden.

4.8.4 Nictiz: Medicatieproces 9

Bron: Nictiz – Medicatieproces 9		
Zie hiervoor https://informatiestakndaarden.nictiz.nl/wiki/Mappingarchitectuur#Mappings_en_transacties		
1.	Via de Koppel Services moet het mogelijk zijn om informatie van de ene (technische) in de andere (technische) vorm over te zetten. De kunst van mappen is ervoor te zorgen dat er geen informatiewaarde verloren gaat en dat de mapping bij voorkeur twee kanten op werkt. Mapping is een optie als de bronsystemen niet (op de gewenste termijn) zelf de informatie in de juiste vorm aan kunnen bieden, maar wel een stabiel alternatief formaat ondersteunen. Om een mapping twee kanten op te laten werken, ben je afhankelijk van de mogelijkheden en beperkingen van beide kanten.	Koppel Services dienen translatie uit te kunnen voeren, zoals opgenomen in https://informatiestandaarden.nictiz.nl/wiki/mp:Mappingarchitectuur

4.8.5 Nictiz: API Requirements for Dutch Healthcare

Nictiz API Requirements for Dutch Healthcare - Koppel Services		
nr	**Requirement**	**Hoofdstuk**
SD001	API documentation MUST be publicly and freely available	API specification & documentation
SD002	API documentation MUST provide examples of how to use the API	API specification & documentation

SD003	API documentation SHOULD provide examples of input and output data	API specification & documentation
SD004	API documentation SHOULD include a FAQ page for API client developers	API specification & documentation
SD005	API documentation MAY specify cases in which API usage is not applicable	API specification & documentation
SD008	API specifications SHOULD be machine readable and allow for automated code generation	API specification & documentation
SD009	API documentation MUST be published in English	API specification & documentation
SD010	When documentation claims compliance to standards, specifications, guidelines and practices, policies or law, documentation MUST provide (references to) evidence to back up these claims	API specification & documentation
SD011	Content relationship MUST be described in API documentation	API specification & documentation
SD012	API documentation MUST describe the availability and usage of operations	API specification & documentation
SD013	API versioning policy MUST be documented	API specification & documentation
SD014	API specifications MUST cover the rationale behind the exchange paradigm used by the API	API specification & documentation
TS001	Public test tooling MUST be freely available for test purposes	API testability
DI001	API specifications SHOULD be published in the Dutch API library for healthcare	API discoverability
DI002	API implementations SHOULD be published in the Dutch API library for healthcare	API discoverability
DI003	API deployments SHOULD be published in the Dutch API library for healthcare	API discoverability
OB001	All API onboarding policies, criteria and procedures MUST be documented	API onboarding
OB002	API onboarding SHOULD be an online self-service process	API onboarding
OB003	API onboarding MAY require a review of the client system and API client developer organization	API onboarding
OB004	When API onboarding requires the API client developer to provide information on the client system and/or client developer organization, the API server deployer MUST provide an Information Disclosure Statement	API onboarding
OB005	The API server deployer MUST provide a procedure for offboarding an API client and/or organization responsible for developing and/or deploying an API client	API onboarding
OB006	All API offboarding policies, criteria and procedures MUST be documented	API onboarding
LM001	API specifications MUST be marked deprecated when they are no longer recommended for use	API Lifecycle management and versioning
LM002	API specifications MUST be marked retired when they are no longer supported	API Lifecycle management and versioning
LM003	API implementations MUST be marked deprecated when they are no longer recommended for use	API Lifecycle management and versioning
LM004	API implementations MUST be marked retired when they are no longer supported	API Lifecycle management and versioning
LM005	API deployments MUST be marked deprecated when they are no longer recommended for use	API Lifecycle management and versioning
LM006	API deployments MUST be marked retired when they are no longer supported	API Lifecycle management and versioning
LM007	An API client MUST be designed to handle non-breaking changes	API Lifecycle management and versioning
LM008	An API specification MUST comply with Semantic Versioning specification (SemVer) version 2.0.0	API Lifecycle management and versioning
AG001	API Service Levels MUST be openly and freely available	API agreements
AG002	API Access Restriction Policies MUST be openly and freely available	API agreements
AG003	Data Processing Policies MUST be openly and freely available	API agreements
AG004	When an API server deployer charges API client developers and/or API client deployers for using the API in a	API agreements

	production environment, any fees MUST be predictable and openly and freely available	
DR001	Interfaces MUST be defined in English	API design rules
DR002	Developers MUST only apply standard HTTP methods	API design rules
DR003	Developers MUST adhere to HTTP safety and idempotency semantics for operations	API design rules
DR004	Server communication MUST remain stateless	API design rules
DR005	Content relationship MUST be predictably implemented	API design rules
DR006	Operations MUST be predictably implemented	API design rules
DR007	API version MUST be accessible through the API	API design rules
DR008	APIs MUST at least support the DEFLATE and gzip compression algorithms	API design rules
DR009	APIs MUST support the use of HTTP Accept-Encoding and Content-Encoding header fields for negotiating compression	API design rules
DR011	JSON formatted content SHOULD comply to RFC 8259 or its successor	API design rules
DR012	When describing an API where data is being transferred to another party, the NOTIFIED PULL exchange pattern SHOULD be used rather than the PUSH exchange pattern	API design rules
DR014	Process APIs SHOULD be designed to reuse System APIs	API design rules
DR-S001	APIs MAY use MTOM/XOP for formatting binary data	API design rules - SOAP
DR-S002	API clients MUST support MTOM/XOP formatting of binary data	API design rules - SOAP
DR-R001	APIs MUST use nouns to name resources	API design rules - RESTful
DR-R002	APIs MUST use singular nouns to name collection resources	API design rules - RESTful
DR-R003	APIs MUST hide irrelevant implementation details	API design rules - RESTful
DR-R004	APIs MUST support both JSON and XML formatting	API design rules - RESTful
DR-R005	API clients MUST at least support JSON or XML formatting	API design rules - RESTful
DR-R006	APIs MAY support BSON formatting	API design rules - RESTful
DR-R007	APIs MUST use the Accept header for content negotiation	API design rules - RESTful
DR-R008	APIs MUST use the Content-Type header for content negotiation	API design rules - RESTful
SC001	API specifications MUST comply with Dutch NCSC guidelines for web applications	API security
SC002	API implementations MUST comply with Dutch NCSC guidelines for web applications	API security
SC003	API deployments MUST comply with Dutch NCSC guidelines for web applications	API security
SC004	API deployments MUST comply with Dutch NCSC guidelines for Transport Layer Security	API security
SC005	An API MUST provide audit logging conforming to NEN 7513	API security
SC007	APIs MUST use fully standardized models for identification and authentication	API security
SC009	When generic services/functions are nationally prescribed for use, APIs MUST use these generic services/functions	API security
SC-S001	APIs SHOULD use WS-Security to ensure message confidentiality and integrity for adding security tokens	API security - SOAP
SC-S002	APIs SHOULD use the SAML Token Security Model	API security - SOAP
SC-R001	APIs MUST comply with RFC 7523 or its successor for client authentication and for requesting OAuth 2 access tokens	API security - RESTful
SC-R002	APIs SHOULD use OpenID Connect to achieve Single-Sign-On when requesting OAuth access tokens	API security - RESTful
SC-R003	JWT tokens used for client authentication and authorization grants MUST comply with RFC 7515 and RFC 7518, or its successors	API security - RESTful

4.8.6 Privacy

Kaderstelling Privacy		Koppel Services
2.5.2.1	Integriteit en vertrouwelijkheid	Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
2.5.2.4	Beveiliging van de verwerking	
2.5.2.3	Koppeling met het Landelijk Schakel Punt (LSP)	Koppeling LSP realiseren.

2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

4.9 Kaders Data Intelligence Services (PL6)

4.9.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Data Intelligence Services
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	Huidige HCI-omgeving dient volgens de nog vast te stellen manier van beschrijven van de dienst gedaan te worden. Afhankelijk van de SOLL (wordt er ontwikkeld, of wordt het onderdeel van Data Services en koppel services) dient deze aangepast te worden.
IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie	Verwerk als afnemer gegevens uit een bronsysteem met respect voor de classificatie van die gegevens. Geef het geen hogere classificatie voor beschikbaarheid en integriteit dan de bron, en geen lagere classificatie voor vertrouwelijkheid. Maak zonodig afspraken met de aanbieder om hun classificatie aan te passen en in hun dienst bijpassende maatregelen daarvoor te implementeren.	Maatregelen implementeren op basis van BIV-classificatie bron(nen). De classificatie van de gecombineerde data is een resultante van de classificaties van de verschillende bronnen. Aandachtspunt is dat de overgang van applicatie-centrische naar data-centrische inrichting een grote impact heeft op de manier waarop Security Operations haar processen ondersteunt.
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	Bij het maken van dataproducten wordt rekening gehouden met doelbinding, data-minimalisatie en oorspronkelijke grondslag. Voor het onttrekken van gegevens om deze dataproducten te kunnen maken dient Data Intelligence Services alle data die onder controle staat van de GGD GHOR NL te kunnen benaderen.

IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's	Gegevensuitwisseling tussen (web)applicaties gebeurt via Restful API's. De broneigenaar levert API's die voldoen aan de moderne RESTful standaarden. API's dienen centraal te worden beheerd in een API management systeem.	Data Intelligence Services communiceren via API's van Koppel Services.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste toolkeuze om invulling te geven aan Data intelligence platform componenten.
IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk IaaS.	Betreft PaaS of IaaS op Cloud Services.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP021 Organisatorisch Informatie Applicatie	Bevorder hergebruik van gegevens	Maak zo veel mogelijk gebruik van gegevens die reeds beschikbaar zijn in plaats van deze gegevens opnieuw te verzamelen of te creëren.	Hergebruik gegevens die reeds beschikbaar zijn.

IMP049 Informatie	Draag zorg voor juiste en actuele en volledige informatie	Een gebruiker kan er op vertrouwen dat een informatieobject, zoals deze in de bron is vastgelegd, juist, actueel en volledig is. Fouten kunnen worden gemeld en hersteld. Daarbij is het van belang dat herstelwijzigingen worden gelogd, zodat traceerbaar is hoe foutieve gegevens zijn verwerkt en wat het effect daarvan is. Dit betekent dat: De kwaliteit van de informatie transparant, verankerd en geborgd moet zijn binnen de processen van de verantwoordelijke en leverende organisatie (datamanagement). Er gebruik moet worden gemaakt van gestandaardiseerde gegevensmodellen, gegevenswoordenboeken en catalogussen ten behoeve van machinematige verwerking van gegevens. De informatie tijdens de gehele levenscyclus moet worden gemonitord, gecontroleerd, gevalideerd op basis van regels, kaders, normen en standaarden waarbij wijzigingen traceerbaar moeten worden gemaakt. De informatie tijdens de gehele levenscyclus regelmatig moet worden getoetst aan wet- en regelgeving en daar verantwoording over moet worden afgelegd. Er cyclisch gerapporteerd moet worden over de kwaliteit van de gegevens. Voor afwijkingen moeten de juiste maatregelen worden getroffen om de betrouwbaarheid en de kwaliteit van de informatie te kunnen waarborgen. De informatie moet door de gehele lifecycle gevolgd kunnen worden vanaf de oorsprong tot aan het verwerken, opslaan, bewerken en beschikbaar stellen en/of vernietigen. (data-lineage). Er gebruik moet worden gemaakt van authentieke- en/of kwalitatieve bronnen.	Data Intelligence Services draagt zorg voor correcte aansluiting bij de bronnen (procesvalidatie). Informatie in dataproducten moet gelijk zijn als in de bron. Overige punten zijn met name van toepassing op Data Services.
IMP050 Informatie	Maak gegevens herleidbaar tot de bron (herkomst)	Dit betekent dat inzichtelijk gemaakt moet worden hoe gegevens tot stand zijn gekomen, over de gehele verwerking in de keten heen. Dus van bronnen tot eindproduct. Van ieder gegeven zijn de herkomst en verwerkingen beschikbaar tot aan vernietiging	Dit betekent dat inzichtelijk gemaakt moet worden hoe gegevens tot stand zijn gekomen, over de gehele verwerking in de keten heen. Dus van bronnen tot eindproduct. Van ieder gegeven zijn de herkomst en verwerkingen beschikbaar tot aan vernietiging.
IMP007 Informatie	Verwijs naar de bron	Verwijzen naar de bron heeft voorkeur boven een kopie uit die bron. Inzage in de bron heeft de voorkeur boven zelf opslaan. Afspraken daarover worden vastgelegd en bekend gemaakt. Vanuit legitimiteitsperspectief kan het nodig zijn een kopie vast te leggen.	Zoveel mogelijk verwijzen naar de bron i.p.v. kopie opslaan, comply or explain.
IMP057 Informatie	Weet welke (bron)gegevens in huis zijn	Weet welke gegevens de overheid of overheidsorganisatie al in huis heeft in de bronadministraties en op welke manier deze gegevens hergebruikt kunnen worden.	Maak gebruik van register van gegevens die bij de overheid of overheidsorganisaties in huis zijn en hoe deze hergebruikt kunnen worden.
IMP045 Grondslagen	Leg de doelbinding vast in de metadata van het	De verwerkingshistorie inclusief doel van verwerking wordt vastgelegd bij het gegevensobject als metadata. Dit betekent dat de historie van acties waarin een gegevensobject wordt verwerkt (opvragen / vastleggen / wijzigen / verwijderen)	Samengestelde gegevensobjecten worden ook opgeslagen in het domeinmodel inclusief alle bijhorende metadata. Uitgangspunt is dat dit

	gegevensobject	inclusief het doel van de actie vastgelegd wordt bij het gegevensobject.	secundair gebruik is van gegevens uit de Data Services.
IMP004 Grondslagen Informatie	Minimaliseer het gebruik van gegevens	Verzamel of vraag alleen die gegevens op die nodig zijn voor het strikte doel van de dienstverlening. En houd de gegevensverwerking die hierop volgt in proportie met het doel. Dit voorkomt dat vertrouwelijke of privacygevoelige gegevens onnodig worden verwerkt.	Voor vertrouwelijke of (privacy-) gevoelige gegevens geldt: vraag alleen die gegevens op die strikt noodzakelijk zijn voor het vastgestelde doel.
IMP022 Grondslagen	Neem oorspronkelijke grondslag mee bij hergebruik diensten	Bij hergebruik van diensten kijken zowel aanbieder als afnemer opnieuw naar de oorspronkelijke grondslag en doelbinding. Als dat nodig blijkt passen zij pseudonimisering dan wel anonimisering van de data toe. Dit houdt in dat bij te ontwikkelen functionaliteit de oorspronkelijke grondslag bepalend is voor de hergebruikmogelijkheden.	Bij hergebruik van (primaire) gegevens wordt opnieuw gekeken naar de oorspronkelijke grondslag en doelbinding. Als dat nodig blijkt wordt pseudonimisering dan wel anonimisering van de data toegepast.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen moeten nog worden vastgesteld door de LFI.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.
IMP080 Informatie	Controleer de verwerking van gegevens	Controleer de verwerking van gegevens: * Zijn de criteria voor juistheid, en tijdigheid vastgesteld? * Worden gegevens die vanuit een systeemvreemde omgeving ingevoerd zijn eerst gecontroleerd op juistheid, tijdigheid en volledigheid, voordat verdere verwerking plaatsvindt? * Worden te versturen gegevens gecontroleerd op juistheid, volledigheid en tijdigheid? * Worden ter verwerking aangeboden gegevens gecontroleerd op juiste, volledig en tijdige verwerking? * Worden kritieke gegevens die in verschillende gegevensverzamelingen voorkomen periodiek met elkaar vergeleken op consistentie? (Dit geldt alleen zolang de gegevens niet frequent en integraal worden gesynchroniseerd met de brongegevens)	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok. De criteria voor juistheid en tijdigheid gelden zowel voor de te ontvangen als de te leveren gegevens.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.

IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats.
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.

4.9.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Data Intelligence Services**
1	Door ontwikkeling van goede faciliteiten voor het anonimiseren en pseudonimiseren van data, komt data uit primaire processen op de juiste manier beschikbaar voor secundair gebruik.	Functioneel dienen er goede faciliteiten voor anonimiseren en pseudonimiseren ontwikkeld te worden.
2	De opgeslagen informatie moet direct beschikbaar zijn voor burgers, zorgverleners, beleidsmakers en onderzoekers. Ongeacht de context waarin zij deze data willen hergebruiken (met waarborgen voor privacy)	Privacy by design dient toegepast te worden.

4.9.3 Nictiz: API Requirements for Dutch Healthcare

Nictiz API Requirements for Dutch Healthcare - Data Intelligence Services		
nr	**Requirement**	**Hoofdstuk**
SD001	API documentation MUST be publicly and freely available	API specification & documentation
SD002	API documentation MUST provide examples of how to use the API	API specification & documentation
SD003	API documentation SHOULD provide examples of input and output data	API specification & documentation
SD004	API documentation SHOULD include a FAQ page for API client developers	API specification & documentation
SD005	API documentation MAY specify cases in which API usage is not applicable	API specification & documentation

SD008	API specifications SHOULD be machine readable and allow for automated code generation	API specification & documentation
SD009	API documentation MUST be published in English	API specification & documentation
SD010	When documentation claims compliance to standards, specifications, guidelines and practices, policies or law, documentation MUST provide (references to) evidence to back up these claims	API specification & documentation
SD011	Content relationship MUST be described in API documentation	API specification & documentation
SD012	API documentation MUST describe the availability and usage of operations	API specification & documentation
SD013	API versioning policy MUST be documented	API specification & documentation
SD014	API specifications MUST cover the rationale behind the exchange paradigm used by the API	API specification & documentation
LM008	An API specification MUST comply with Semantic Versioning specification (SemVer) version 2.0.0	API Lifecycle management and versioning
DR001	Interfaces MUST be defined in English	API design rules
DR002	Developers MUST only apply standard HTTP methods	API design rules
DR003	Developers MUST adhere to HTTP safety and idempotency semantics for operations	API design rules
DR004	Server communication MUST remain stateless	API design rules
DR005	Content relationship MUST be predictably implemented	API design rules
DR006	Operations MUST be predictably implemented	API design rules
DR007	API version MUST be accessible through the API	API design rules
DR008	APIs MUST at least support the DEFLATE and gzip compression algorithms	API design rules
DR009	APIs MUST support the use of HTTP Accept-Encoding and Content-Encoding header fields for negotiating compression	API design rules
DR011	JSON formatted content SHOULD comply to RFC 8259 or its successor	API design rules
DR012	When describing an API where data is being transferred to another party, the NOTIFIED PULL exchange pattern SHOULD be used rather than the PUSH exchange pattern	API design rules
DR014	Process APIs SHOULD be designed to reuse System APIs	API design rules
DR-S001	APIs MAY use MTOM/XOP for formatting binary data	API design rules - SOAP
DR-S002	API clients MUST support MTOM/XOP formatting of binary data	API design rules - SOAP
DR-R001	APIs MUST use nouns to name resources	API design rules - RESTful
DR-R002	APIs MUST use singular nouns to name collection resources	API design rules - RESTful
DR-R003	APIs MUST hide irrelevant implementation details	API design rules - RESTful
DR-R004	APIs MUST support both JSON and XML formatting	API design rules - RESTful
DR-R005	API clients MUST at least support JSON or XML formatting	API design rules - RESTful
DR-R006	APIs MAY support BSON formatting	API design rules - RESTful
DR-R007	APIs MUST use the Accept header for content negotiation	API design rules - RESTful
DR-R008	APIs MUST use the Content-Type header for content negotiation	API design rules - RESTful
SC001	API specifications MUST comply with Dutch NCSC guidelines for web applications	API security
SC002	API implementations MUST comply with Dutch NCSC guidelines for web applications	API security
SC003	API deployments MUST comply with Dutch NCSC guidelines for web applications	API security
SC004	API deployments MUST comply with Dutch NCSC guidelines for Transport Layer Security	API security
SC005	An API MUST provide audit logging conforming to NEN 7513	API security
SC007	APIs MUST use fully standardized models for identification and authentication	API security
SC-S001	APIs SHOULD use WS-Security to ensure message confidentiality and integrity for adding security tokens	API security - SOAP
SC-S002	APIs SHOULD use the SAML Token Security Model	API security - SOAP
SC-R001	APIs MUST comply with RFC 7523 or its successor for client authentication and for requesting OAuth 2 access tokens	API security - RESTful
SC-R002	APIs SHOULD use OpenID Connect to achieve Single-Sign-On when requesting OAuth access tokens	API security - RESTful

SC-R003	JWT tokens used for client authentication and authorization grants MUST comply with RFC 7515 and RFC 7518, or its successors	API security - RESTful

4.9.4 Privacy

Kaderstelling Privacy		Data Intelligence Services
2.5.2.3	Recht op gegevensportabiliteit	Het platform voorziet in een methode om binnen een maand medische dossiers van een betrokkene in een gestructureerd, veelgebruikt en machineleesbaar formaat aan betrokkene te verstrekken. (dataset provisioning).
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.
2.5.2.8	Wetenschappelijk onderzoek	Het platform beschikt over middelen om instanties toegang te geven tot specifieke gegevens van de database ten behoeve van wetenschappelijk onderzoek. Toegang wordt enkel verleend na toestemming van de verwerkingsverantwoordelijke(n). De gegevens die inzichtelijk zijn voor onderzoek zijn altijd gepseudonimiseerd of geanonimiseerd.

4.10 Kaders Multi-Channel Presentatie Services (PL7a)

4.10.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Multi-Channel Presentatie Services
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	N.v.t. Betreft een 'basisvoorziening' dienst. Deze dient wel als dienst beschreven te worden.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Eis aan organisatie GGD GHOR Nederland: Met behulp van Gartner, Critical Friends en marktverkenningen wordt het beste standaardpatroon voor Multi-Channel Presentatie Services bepaald.
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing	Standaardoplossing t.b.v. Multi-Channel Presentatie Services.

	zonder maatwerk	je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	
IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk IaaS.	Betreft PaaS of IaaS op Cloud Services.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP053 Organisatorisch	Stel betrokkenen op de hoogte van het doel waarvoor gegevens verzameld worden	Stel bij het verzamelen en opvragen van persoonsgegevens de betrokkenen op de hoogte van het doel waarvoor de gegevens worden verzameld en van de rechten die zij mogen uitoefenen.	Cookie toestemming.

IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. deze dienst worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens. Specifiek voor data "in Use" en het tegengaan van externe dataopslag.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats.

IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.
IMP065 Informatie	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces	Controleer de kwaliteit van gegevens vanaf invoer en op ieder koppelvlak aan de hand van de vastgestelde kwaliteitseisen. Eenmaal geverifieerd hoeft een verificatie niet opnieuw plaats te vinden als de eerder uitgevoerde verificatie nog betrouwbaar is.	Controle van handmatige invoer.

4.10.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Multi-Channel Presentatie Services**
1	Deelnemers in het zorgnetwerk worden door hun systemen gefaciliteerd in het vastleggen van data en gebruik van eigen en andermans data door een gebruiksvriendelijke inrichting, een vertaalslag naar relevante, begrijpelijke informatie en het bieden van de juiste functionaliteit om hun rol in het netwerk te kunnen vervullen	Zie ook business requirements LFI; gebruikersvriendelijke inrichting.

4.10.3 Nictiz: API Requirements for Dutch Healthcare

Nictiz API Requirements for Dutch Healthcare - Multichannel Presentatie Services		
nr	**Requirement**	**Hoofdstuk**
SD001	API documentation MUST be publicly and freely available	API specification & documentation
SD002	API documentation MUST provide examples of how to use the API	API specification & documentation
SD003	API documentation SHOULD provide examples of input and output data	API specification & documentation
SD004	API documentation SHOULD include a FAQ page for API client developers	API specification & documentation
SD005	API documentation MAY specify cases in which API usage is not applicable	API specification & documentation
SD008	API specifications SHOULD be machine readable and allow for automated code generation	API specification & documentation
SD009	API documentation MUST be published in English	API specification & documentation
SD010	When documentation claims compliance to standards, specifications, guidelines and practices, policies or law, documentation MUST provide (references to) evidence to back up these claims	API specification & documentation
SD011	Content relationship MUST be described in API documentation	API specification & documentation
SD012	API documentation MUST describe the availability and usage of operations	API specification & documentation

SD013	API versioning policy MUST be documented	API specification & documentation
SD014	API specifications MUST cover the rationale behind the exchange paradigm used by the API	API specification & documentation
LM008	An API specification MUST comply with Semantic Versioning specification (SemVer) version 2.0.0	API Lifecycle management and versioning
DR001	Interfaces MUST be defined in English	API design rules
DR002	Developers MUST only apply standard HTTP methods	API design rules
DR003	Developers MUST adhere to HTTP safety and idempotency semantics for operations	API design rules
DR004	Server communication MUST remain stateless	API design rules
DR005	Content relationship MUST be predictably implemented	API design rules
DR006	Operations MUST be predictably implemented	API design rules
DR007	API version MUST be accessible through the API	API design rules
DR008	APIs MUST at least support the DEFLATE and gzip compression algorithms	API design rules
DR009	APIs MUST support the use of HTTP Accept-Encoding and Content-Encoding header fields for negotiating compression	API design rules
DR011	JSON formatted content SHOULD comply to RFC 8259 or its successor	API design rules
DR012	When describing an API where data is being transferred to another party, the NOTIFIED PULL exchange pattern SHOULD be used rather than the PUSH exchange pattern	API design rules
DR015	Experience APIs SHOULD be based on Process APIs	API design rules
DR-S001	APIs MAY use MTOM/XOP for formatting binary data	API design rules - SOAP
DR-S002	API clients MUST support MTOM/XOP formatting of binary data	API design rules - SOAP
DR-R001	APIs MUST use nouns to name resources	API design rules - RESTful
DR-R002	APIs MUST use singular nouns to name collection resources	API design rules - RESTful
DR-R003	APIs MUST hide irrelevant implementation details	API design rules - RESTful
DR-R004	APIs MUST support both JSON and XML formatting	API design rules - RESTful
DR-R005	API clients MUST at least support JSON or XML formatting	API design rules - RESTful
DR-R006	APIs MAY support BSON formatting	API design rules - RESTful
DR-R007	APIs MUST use the Accept header for content negotiation	API design rules - RESTful
DR-R008	APIs MUST use the Content-Type header for content negotiation	API design rules - RESTful
SC001	API specifications MUST comply with Dutch NCSC guidelines for web applications	API security
SC002	API implementations MUST comply with Dutch NCSC guidelines for web applications	API security
SC003	API deployments MUST comply with Dutch NCSC guidelines for web applications	API security
SC004	API deployments MUST comply with Dutch NCSC guidelines for Transport Layer Security	API security
SC005	An API MUST provide audit logging conforming to NEN 7513	API security
SC007	APIs MUST use fully standardized models for identification and authentication	API security
SC-S001	APIs SHOULD use WS-Security to ensure message confidentiality and integrity for adding security tokens	API security - SOAP
SC-S002	APIs SHOULD use the SAML Token Security Model	API security - SOAP
SC-R001	APIs MUST comply with RFC 7523 or its successor for client authentication and for requesting OAuth 2 access tokens	API security - RESTful
SC-R002	APIs SHOULD use OpenID Connect to achieve Single-Sign-On when requesting OAuth access tokens	API security - RESTful
SC-R003	JWT tokens used for client authentication and authorization grants MUST comply with RFC 7515 and RFC 7518, or its successors	API security - RESTful

4.10.4 Privacy

Kaderstelling Privacy		Multichannel Presentatie Services
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

4.11 Kaders Applicatie Services (PL7b)

4.11.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Applicatie Services
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	Eis aan organisatie GGD GHOR Nederland: Dit is de dienst die de GGD'en en burgers daadwerkelijk afnemen op basis van de Data Services wellicht aangevuld met andere bronnen. Dit is de belangrijkste te beschrijven dienst.
IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's	Gegevensuitwisseling tussen (web)applicaties gebeurt via Restful API's. De broneigenaar levert API's die voldoen aan de moderne RESTful standaarden. API's dienen centraal te worden beheerd in een API management systeem.	Applicatie services communiceren via API's van koppel services.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Eis aan organisatie GGDGHOR Nederland: Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van componenten om applicaties low code/no code geautomatiseerd te realiseren vanuit het domeinmodel.
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing t.b.v. applicatieontwikkeling en -compositie.

IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS boven IaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk IaaS.	Betreft PaaS of IaaS op Cloud Services.
IMP026 Organisatorisch	Pas je eigen proces en organisatie aan aan de standaard oplossing	Pas je processen en organisatie aan de standaard oplossingen aan, in plaats van het omgekeerde. Zie ook EIF principle 4 "Reusability", aanbeveling 6+7.	Eis aan organisatie GGDGHOR Nederland: N.v.t., betreft denkwijzen vanuit applicatie centrische gedachtegang.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP051 Informatie	Leg auditlogs vast bij de bronregistratie van het gegeven	Als eigenaar van de bron wil je inzicht hebben in de toegang en inzage (CRUD) van de gegevens die vanuit de bron worden gebruikt. Voorkom dat auditgegevens verspreid raken over afnemende applicaties.	Voorkom dat auditgegevens verspreid raken over afnemende applicaties.

IMP056 Organisatorisch Informatie	Registreer gegevens bij de bron	Registreer gegevens (zo dicht mogelijk) bij de bron, daar waar de gegevens ontstaan. Dit verhoogt de volledigheid, kwaliteit en de actualiteit van de gegevens aanzienlijk en voorkomt fouten. De vastgelegde gegevens kunnen daarna voor verschillende doeleinden worden gebruikt. Een ander belangrijk voordeel is dat het achteraf registreren van gegevens die eerder zijn ontstaan wordt voorkomen hetgeen de registratielast vermindert. Waar mogelijk, leg gegevens geautomatiseerd vast.	Zoveel mogelijk verwijzen naar de bron i.p.v. kopie opslaan, pas toe of leg uit.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. deze dienst worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een	Binnen het bouwblok vindt microsegmentatie plaats.

		maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.

4.11.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Applicatie Services**
1	Meer inzet van digitale zorg- en gezondheidstoepassingen is alleen effectief als zowel zorgverleners als burgers/patiënten/cliënten hier goed mee om kunnen gaan.	Zie ook LFI BRQ, LMS-inrichting dient gerealiseerd te worden.

4.11.3 Nictiz: API Requirements for Dutch Healthcare

Nictiz API Requirements for Dutch Healthcare - Applicatie Services		
nr	**Requirement**	**Hoofdstuk**
SD001	API documentation MUST be publicly and freely available	API specification & documentation
SD002	API documentation MUST provide examples of how to use the API	API specification & documentation
SD003	API documentation SHOULD provide examples of input and output data	API specification & documentation
SD004	API documentation SHOULD include a FAQ page for API client developers	API specification & documentation
SD005	API documentation MAY specify cases in which API usage is not applicable	API specification & documentation
SD008	API specifications SHOULD be machine readable and allow for automated code generation	API specification & documentation
SD009	API documentation MUST be published in English	API specification & documentation
SD010	When documentation claims compliance to standards, specifications, guidelines and practices, policies or law, documentation MUST provide (references to) evidence to back up these claims	API specification & documentation
SD011	Content relationship MUST be described in API documentation	API specification & documentation
SD012	API documentation MUST describe the availability and usage of operations	API specification & documentation
SD013	API versioning policy MUST be documented	API specification & documentation
SD014	API specifications MUST cover the rationale behind the exchange paradigm used by the API	API specification & documentation

LM008	An API specification MUST comply with Semantic Versioning specification (SemVer) version 2.0.0	API Lifecycle management and versioning
DR001	Interfaces MUST be defined in English	API design rules
DR002	Developers MUST only apply standard HTTP methods	API design rules
DR003	Developers MUST adhere to HTTP safety and idempotency semantics for operations	API design rules
DR004	Server communication MUST remain stateless	API design rules
DR005	Content relationship MUST be predictably implemented	API design rules
DR006	Operations MUST be predictably implemented	API design rules
DR007	API version MUST be accessible through the API	API design rules
DR008	APIs MUST at least support the DEFLATE and gzip compression algorithms	API design rules
DR009	APIs MUST support the use of HTTP Accept-Encoding and Content-Encoding header fields for negotiating compression	API design rules
DR011	JSON formatted content SHOULD comply to RFC 8259 or its successor	API design rules
DR012	When describing an API where data is being transferred to another party, the NOTIFIED PULL exchange pattern SHOULD be used rather than the PUSH exchange pattern	API design rules
DR014	Process APIs SHOULD be designed to reuse System APIs	API design rules
DR-S001	APIs MAY use MTOM/XOP for formatting binary data	API design rules - SOAP
DR-S002	API clients MUST support MTOM/XOP formatting of binary data	API design rules - SOAP
DR-R001	APIs MUST use nouns to name resources	API design rules - RESTful
DR-R002	APIs MUST use singular nouns to name collection resources	API design rules - RESTful
DR-R003	APIs MUST hide irrelevant implementation details	API design rules - RESTful
DR-R004	APIs MUST support both JSON and XML formatting	API design rules - RESTful
DR-R005	API clients MUST at least support JSON or XML formatting	API design rules - RESTful
DR-R006	APIs MAY support BSON formatting	API design rules - RESTful
DR-R007	APIs MUST use the Accept header for content negotiation	API design rules - RESTful
DR-R008	APIs MUST use the Content-Type header for content negotiation	API design rules - RESTful
SC001	API specifications MUST comply with Dutch NCSC guidelines for web applications	API security
SC002	API implementations MUST comply with Dutch NCSC guidelines for web applications	API security
SC003	API deployments MUST comply with Dutch NCSC guidelines for web applications	API security
SC004	API deployments MUST comply with Dutch NCSC guidelines for Transport Layer Security	API security
SC005	An API MUST provide audit logging conforming to NEN 7513	API security
SC007	APIs MUST use fully standardized models for identification and authentication	API security
SC-S001	APIs SHOULD use WS-Security to ensure message confidentiality and integrity for adding security tokens	API security - SOAP
SC-S002	APIs SHOULD use the SAML Token Security Model	API security - SOAP
SC-R001	APIs MUST comply with RFC 7523 or its successor for client authentication and for requesting OAuth 2 access tokens	API security - RESTful
SC-R002	APIs SHOULD use OpenID Connect to achieve Single-Sign-On when requesting OAuth access tokens	API security - RESTful
SC-R003	JWT tokens used for client authentication and authorization grants MUST comply with RFC 7515 and RFC 7518, or its successors	API security - RESTful

4.11.4 Privacy

Kaderstelling Privacy		Applicatie Services
2.5.2.3	Recht op beperking van de verwerking	Te realiseren applicatie die voorziet in een methode om een verwerking stil te leggen en de ontvangers informeert aan wie de persoonsgegevens openbaar gemaakt zijn van deze beperking.
2.5.2.3	Burgerportaal	Te realiseren applicatie burgerportaal met inzicht welke gegevens er worden verwerkt en doeleinden. Tevens functie t.b.v. verzoek tot rectificatie of vergetelheid.
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.
2.5.2.6	Eisen bij EPD	Voor het platform betekent dit dat wanneer er sprake is van een Elektronisch Patiënten Dossier (EPD), er de mogelijkheid moet zijn om het gehele dossier of delen daarvan te verwijderen.

4.12 Applicatie Layering (PL7c)

4.12.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Applicatie Layering
IMP033 Applicatie	Koppel bronsystemen op basis van een passende classificatie	Verwerk als afnemer gegevens uit een bronsysteem met respect voor de classificatie van die gegevens. Geef het geen hogere classificatie voor beschikbaarheid en integriteit dan de bron, en geen lagere classificatie voor vertrouwelijkheid. Maak zonodig afspraken met de aanbieder om hun classificatie aan te passen en in hun dienst bijpassende maatregelen daarvoor te implementeren.	Het ontsluiten van de eigen data, gecombineerd met de Data Intelligence Services en de plek waar andere bronnen hun data aanleveren. Per subonderdeel zal de BIV vastgesteld moeten worden, maar in ieder geval dient deze technisch aangepast te kunnen worden indien hogere waardes van toepassing zijn.
IMP087 Applicatie	Verwerk bericht-interactie persistent	Zorg dat een bericht dat een mutatie tot gevolg heeft, bijvoorbeeld een bericht dat een betalingsopdracht representeert, niet verloren kan gaan. Een dergelijk 'transactioneel' bericht moet een incident als uitwijk of storing kunnen overleven. Alle onderdelen van een verwerkingsketen nemen verantwoordelijkheid voor het bericht en zorgen ervoor dat het bericht niet verloren gaat. Correcte verwerking heeft prioriteit boven verwerkingssnelheid. Persistentie houdt in dat een (transport-)transactie pas is voltooid als het bericht is opgeslagen in een 'persistent store', zoals een bestand of database. Een opvragingsbericht daarentegen heeft geen mutatie tot gevolg. Responsetijd heeft hier meer prioriteit. Bij verlies van een opvragingsbericht (door bv. een storing) wordt de opvraging opnieuw gedaan. Verwerk een opvragingsbericht daarom niet-persistent verwerkt.	Mutaties vinden plaats in de Data Services. De API's die hiertoe toegang bieden worden gemanaged en gemonitored in de Applicatie Layering voorziening. De technieken hiervoor dienen dermate ingericht te worden dat mutatieberichten niet verloren kunnen gaan.
IMP083 Applicatie	Wissel gegevens tussen (web)applicaties uit met API's	Gegevensuitwisseling tussen (web)applicaties gebeurt via Restful API's. De broneigenaar levert API's die voldoen aan de moderne RESTful standaarden. API's dienen centraal te worden beheerd in een API management systeem.	De data API's worden beschikbaar gesteld via de Applicatie Layering, waar dus ook een API-management systeem ingericht moet worden.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Eisen aan organisatie GGD GHOR NL: Met behulp van Gartner, Critical Friends en marktverkenningen zal gezocht worden naar de beste standaard invulling van Applicatie Layering componenten.

IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing(en) t.b.v. Applicatie Layering.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. deze dienst worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP064 Applicatie	Stel onweerlegbaarheid vast	Stel vast voor welke berichtenstromen of transacties onweerlegbaarheid van gegevens vereist is, zodat daarvoor aanvullende maatregelen genomen kunnen worden.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP084 Applicatie	Versleutel gegevens in rust en transport	Versleutel alle gegevensdragers waarop niet-publieke informatie staat, inclusief smartphones en laptops, conform de laatst bekende en geldende richtlijnen. Dit reduceert het risico op een gegevenslek bij verlies van een dergelijk apparaat. Neem voor niet-publieke gegevens ook adequate beveiligingsmaatregelen om ze te beschermen in transit. Dit kan door de verbinding te beveiligen,	Versleutel gegevens in transport.

		danwel door encryptie van de informatie zelf. Dit laatste heeft de voorkeur.	
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.
IMP065 Informatie	Verifieer de kwaliteit van gegevens van het begin tot het einde van het proces	Controleer de kwaliteit van gegevens vanaf invoer en op ieder koppelvlak aan de hand van de vastgestelde kwaliteitseisen. Eenmaal geverifieerd hoeft een verificatie niet opnieuw plaats te vinden als de eerder uitgevoerde verificatie nog betrouwbaar is.	Controle op kwaliteit van gegevens gebeurt binnen Data Services

4.12.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Applicatie Layering**
1	Effectieve uitwisseling vraagt om eenheid van taal en techniek, zodat data begrepen wordt en bruikbaar is. Daarom is de Wegiz ook een belangrijke aanjager die er mede voor zorgt dat data beschikbaar komt.	Eenheid van techniek dient toegepast te worden.
2	Door drempelvrije, eenvoudige controle voor burgers en zorgverlener op de navolging van afspraken en richtlijnen.	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
3	Alle betrokkenen in het netwerk van een persoon moeten de mogelijkheid hebben de data in die dossiers te kunnen raadplegen en gebruiken. Maar alleen als zij daartoe geautoriseerd zijn en die gegevens nodig hebben voor het leveren van passende hybride zorg met waarborgen voor patiëntveiligheid.	Aansluiting LSP dient gerealiseerd te worden.
4	De burger zelf heeft recht op inzage in én gebruik van alle over hem geregistreerde en uitgewisselde gegevens	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
5	Deelnemers in het zorgnetwerk worden door hun systemen gefaciliteerd in het vastleggen van data en gebruik van eigen en andermans data door een gebruiksvriendelijke inrichting, een vertaalslag naar relevante, begrijpelijke informatie en het bieden van de juiste functionaliteit om hun rol in het netwerk te kunnen vervullen	Kunnen gebruiken van andermans data. Vertaalslag (translatie) dient dit te realiseren.
6	Partijen in het zorgnetwerk zijn aangesloten op de landelijk dekkende en nationaal vastgestelde infrastructuren. Dit zodat zij elkaar eenvoudig kunnen bereiken, gegevens kunnen delen en ondersteund worden in de samenwerking	Aansluiting LSP dient gerealiseerd te worden.
7	Bij eenmalige registratie leg je data op een gestandaardiseerde manier vast (eenheid van taal) en wordt deze vervolgens op een standaard manier ontsloten (Eenheid van Techniek) voor secundair gebruik.	Eenheid van techniek dient toegepast te worden.
8	Beschikbaar stellen van data ten behoeve van anderen in het zorgnetwerk wordt verplicht. Niet alleen voor betrokkenen in het netwerk, maar ook ten behoeve van het algemeen maatschappelijk belang. Dit heeft gevolgen voor besluiten over toestemming en bezwaren. Alleen als de persoon expliciet de toegang tot zorg- en gezondheidsdata weigert, komen data niet beschikbaar	Aansluiting LSP dient gerealiseerd te worden.

9	Burgers en zorgverleners kunnen de applicatie kiezen die de door hen gewenste/benodigde functionaliteit biedt	Scheiding van data en koppel services. Koppel services biedt data API's aan, welke gebruikt kunnen worden door te kiezen applicaties.
10	Onderdeel van het vertrouwensmodel is onder andere eenvoudige identificatie, authenticatie, autorisatie, logging, toestemming en behandelrelatie en de rollen en verantwoordelijkheden die daarbij horen	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
11	Er wordt gebruik gemaakt van internationale standaarden voor eenheid van taal, opslag en transport van data	Internationale standaarden voor eenheid van taal en transport van data.
12	Dit betekent onder andere het gebruik van (op inhoud gestandaardiseerde) API's Hierbij hoort ook een eenheid van taal (zib-) en API-strategie om de gestandaardiseerde toegang tot data te realiseren	Zie ook NORA, gebruik gestandaardiseerde API's.
13	Daarbij horen ook afspraken over landelijk dekkende infrastructuren. Er loopt momenteel een onderzoek naar scenario's om gegevensuitwisseling versneld te faciliteren met een landelijk dekkend netwerk	Afspraken koppelingen netwerken dienen gemaakt of gevolgd te worden.
14	(Inter)nationaal vastgestelde gestandaardiseerde koppelingen (API's)	Er dienen (inter)nationaal vastgestelde gestandaardiseerde koppelingen (API's) opgeleverd te worden.
15	Een (inter)nationaal vastgesteld stelsel van onderling verbonden infrastructuren	Er dient een (inter)nationaal vastgesteld stelsel van onderling verbonden infrastructuren gerealiseerd te worden waarop wordt aangesloten.
16	In het IZA is afgesproken dat de gestandaardiseerde (open) API-strategie van Nictiz leidend wordt in de wijze van openstelling van systemen.	De API Requirements for Dutch Healthcare van Nictiz is opgenomen in de kaders.
17	Persoonlijke gezondheidsomgevingen (PGO's) kunnen voorzien in deze behoefte.	Zie ook kaders MedMij, kunnen ontsluiten naar PGO-omgevingen.
18	Door een expliciete scheiding te maken tussen de standaarden voor de inhoud (Eenheid van taal) en de standaarden voor datatransport (Eenheid van Techniek) ontstaat er meer stabiliteit in het ecosysteem en kan de betekenis van de data voor een langere tijd worden gegarandeerd.	Eenheid van techniek dient toegepast te worden.
19	ZORG-AB voor adressering (en de verbinding met Lrza)	Verbinding met Lrza dient gerealiseerd te worden.
20	1 lokalisatievoorziening om te kunnen achterhalen waar patiëntgegevens terug te vinden zijn (vergelijkbaar met mijnpensioenoverzicht.nl)	Registerfunctionaliteit dient gerealiseerd/gebruikt te worden.

4.12.3 Nictiz: Medicatieproces 9

Bron: Nictiz – Medicatieproces 9		
Zie hiervoor https://informatiestakndaarden.nictiz.nl/wiki/Mappingarchitectuur#Mappings_en_transacties		
1.	Via de Koppel Services moet het mogelijk zijn om informatie van de ene (technische) in de andere (technische) vorm over te zetten. De kunst van mappen is ervoor te zorgen dat er geen informatiewaarde verloren gaat en dat de mapping bij voorkeur twee kanten op werkt. Mapping is een optie als de bronsystemen niet (op de gewenste termijn) zelf de informatie in de juiste vorm aan kunnen bieden, maar wel een stabiel alternatief formaat ondersteunen. Om een mapping twee kanten op te laten werken, ben je afhankelijk van de mogelijkheden en beperkingen van beide kanten.	Koppel Services dienen translatie uit te kunnen voeren, zoals opgenomen in https://informatiestandaarden.nictiz.nl/wiki/mp:Mappingarchitectuur

4.12.4 Nictiz: API Requirements for Dutch Healthcare

Nictiz API Requirements for Dutch Healthcare - Koppel Services		
nr	**Requirement**	**Hoofdstuk**
SD001	API documentation MUST be publicly and freely available	API specification & documentation

SD002	API documentation MUST provide examples of how to use the API	API specification & documentation
SD003	API documentation SHOULD provide examples of input and output data	API specification & documentation
SD004	API documentation SHOULD include a FAQ page for API client developers	API specification & documentation
SD005	API documentation MAY specify cases in which API usage is not applicable	API specification & documentation
SD008	API specifications SHOULD be machine readable and allow for automated code generation	API specification & documentation
SD009	API documentation MUST be published in English	API specification & documentation
SD010	When documentation claims compliance to standards, specifications, guidelines and practices, policies or law, documentation MUST provide (references to) evidence to back up these claims	API specification & documentation
SD011	Content relationship MUST be described in API documentation	API specification & documentation
SD012	API documentation MUST describe the availability and usage of operations	API specification & documentation
SD013	API versioning policy MUST be documented	API specification & documentation
SD014	API specifications MUST cover the rationale behind the exchange paradigm used by the API	API specification & documentation
TS001	Public test tooling MUST be freely available for test purposes	API testability
DI001	API specifications SHOULD be published in the Dutch API library for healthcare	API discoverability
DI002	API implementations SHOULD be published in the Dutch API library for healthcare	API discoverability
DI003	API deployments SHOULD be published in the Dutch API library for healthcare	API discoverability
OB001	All API onboarding policies, criteria and procedures MUST be documented	API onboarding
OB002	API onboarding SHOULD be an online self-service process	API onboarding
OB003	API onboarding MAY require a review of the client system and API client developer organization	API onboarding
OB004	When API onboarding requires the API client developer to provide information on the client system and/or client developer organization, the API server deployer MUST provide an Information Disclosure Statement	API onboarding
OB005	The API server deployer MUST provide a procedure for offboarding an API client and/or organization responsible for developing and/or deploying an API client	API onboarding
OB006	All API offboarding policies, criteria and procedures MUST be documented	API onboarding
LM001	API specifications MUST be marked deprecated when they are no longer recommended for use	API Lifecycle management and versioning
LM002	API specifications MUST be marked retired when they are no longer supported	API Lifecycle management and versioning
LM003	API implementations MUST be marked deprecated when they are no longer recommended for use	API Lifecycle management and versioning
LM004	API implementations MUST be marked retired when they are no longer supported	API Lifecycle management and versioning
LM005	API deployments MUST be marked deprecated when they are no longer recommended for use	API Lifecycle management and versioning
LM006	API deployments MUST be marked retired when they are no longer supported	API Lifecycle management and versioning
LM007	An API client MUST be designed to handle non-breaking changes	API Lifecycle management and versioning
LM008	An API specification MUST comply with Semantic Versioning specification (SemVer) version 2.0.0	API Lifecycle management and versioning
AG001	API Service Levels MUST be openly and freely available	API agreements
AG002	API Access Restriction Policies MUST be openly and freely available	API agreements
AG003	Data Processing Policies MUST be openly and freely available	API agreements

AG004	When an API server deployer charges API client developers and/or API client deployers for using the API in a production environment, any fees MUST be predictable and openly and freely available	API agreements
DR001	Interfaces MUST be defined in English	API design rules
DR002	Developers MUST only apply standard HTTP methods	API design rules
DR003	Developers MUST adhere to HTTP safety and idempotency semantics for operations	API design rules
DR004	Server communication MUST remain stateless	API design rules
DR005	Content relationship MUST be predictably implemented	API design rules
DR006	Operations MUST be predictably implemented	API design rules
DR007	API version MUST be accessible through the API	API design rules
DR008	APIs MUST at least support the DEFLATE and gzip compression algorithms	API design rules
DR009	APIs MUST support the use of HTTP Accept-Encoding and Content-Encoding header fields for negotiating compression	API design rules
DR011	JSON formatted content SHOULD comply to RFC 8259 or its successor	API design rules
DR012	When describing an API where data is being transferred to another party, the NOTIFIED PULL exchange pattern SHOULD be used rather than the PUSH exchange pattern	API design rules
DR014	Process APIs SHOULD be designed to reuse System APIs	API design rules
DR-S001	APIs MAY use MTOM/XOP for formatting binary data	API design rules - SOAP
DR-S002	API clients MUST support MTOM/XOP formatting of binary data	API design rules - SOAP
DR-R001	APIs MUST use nouns to name resources	API design rules - RESTful
DR-R002	APIs MUST use singular nouns to name collection resources	API design rules - RESTful
DR-R003	APIs MUST hide irrelevant implementation details	API design rules - RESTful
DR-R004	APIs MUST support both JSON and XML formatting	API design rules - RESTful
DR-R005	API clients MUST at least support JSON or XML formatting	API design rules - RESTful
DR-R006	APIs MAY support BSON formatting	API design rules - RESTful
DR-R007	APIs MUST use the Accept header for content negotiation	API design rules - RESTful
DR-R008	APIs MUST use the Content-Type header for content negotiation	API design rules - RESTful
SC001	API specifications MUST comply with Dutch NCSC guidelines for web applications	API security
SC002	API implementations MUST comply with Dutch NCSC guidelines for web applications	API security
SC003	API deployments MUST comply with Dutch NCSC guidelines for web applications	API security
SC004	API deployments MUST comply with Dutch NCSC guidelines for Transport Layer Security	API security
SC005	An API MUST provide audit logging conforming to NEN 7513	API security
SC007	APIs MUST use fully standardized models for identification and authentication	API security
SC009	When generic services/functions are nationally prescribed for use, APIs MUST use these generic services/functions	API security
SC-S001	APIs SHOULD use WS-Security to ensure message confidentiality and integrity for adding security tokens	API security - SOAP
SC-S002	APIs SHOULD use the SAML Token Security Model	API security - SOAP
SC-R001	APIs MUST comply with RFC 7523 or its successor for client authentication and for requesting OAuth 2 access tokens	API security - RESTful
SC-R002	APIs SHOULD use OpenID Connect to achieve Single-Sign-On when requesting OAuth access tokens	API security - RESTful
SC-R003	JWT tokens used for client authentication and authorization grants MUST comply with RFC 7515 and RFC 7518, or its successors	API security - RESTful

4.12.5 Privacy

Kaderstelling Privacy		Applicatie Layering
2.5.2.1	Integriteit en vertrouwelijkheid	Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
2.5.2.4	Beveiliging van de verwerking	

2.5.2.3	Koppeling met het Landelijk Schakel Punt (LSP)	Koppeling LSP realiseren.
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

4.13 Kaders Veilige Applicatie- en Datatoegang (PL8a)

4.13.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Veilige Applicatie- en Datatoegang
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten. De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	N.v.t. Betreft een 'basisvoorziening' dienst. Deze dient wel als dienst beschreven te worden.
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	N.v.t. Betreft een 'basisvoorziening' dienst.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Met behulp van Gartner, Critical Friends en marktverkenningen wordt het beste standaardpatroon voor Veilige Applicatie- en Datatoegang bepaald.
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing(en) t.b.v. Veilige Applicatie- en Datatoegang.
IMP085 Organisatorisch Informatie Applicatie Netwerk	Kies bij cloudoplossingen SaaS boven PaaS	Bij het kiezen voor een cloud oplossing, geef de voorkeur aan SaaS boven PaaS boven IaaS. Houd hierbij rekening met het definiëren van een goede exit strategie en interoperabiliteit standaarden om de vendor lock-in zo beperkt mogelijk te houden. Een cloud oplossing vergt bovendien een gedegen strategie en plan van aanpak vanuit de eigen organisatie hoe met (publieke, community	Betreft PaaS of IaaS op Cloud Services.

	boven IaaS	of private) cloud diensten om te gaan. Het SaaS (Software as a Service) model richt zich primair op eindgebruikers. Deze zijn (vaak) te prefereren voor oplossingen die niet uniek of onderscheidend zijn voor de organisatie of het werkdomein. Voorbeelden hiervan zijn Customer Relations Management, e-mail & Instant Messaging, Financiën, HRM en Project Management. PaaS (Platform as a Service) richt zich vooral op ontwikkelaars waarmee ze een ontwikkelplatform ter beschikking krijgen waarbij de cloud dienstverlener zorgdraagt voor de infrastructurele aspecten. Bij IaaS (Infrastructure as a Service) neem je infrastructuur componenten uit de cloud af zoals servers, opslag, en netwerken. Opmerking: deze implicatie daagt uit om tot een zo hoog mogelijk niveau ontzorgd te worden. Bij Cloud oplossingen ga je eerst kijken of de functionele eisen met SaaS kunnen worden ingevuld. Als specifiek aan een applicatie-ontwikkelomgeving of infra de behoefte is, dan kies je uiteraard voor PaaS respectievelijk Iaas.	
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. deze dienst worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens. Specifiek

			voor data "in Use" en het tegengaan van externe dataopslag.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP015 Applicatie	Maak beveiligingsmaatregelen zo gebruiksvriendelijk mogelijk	Maak beveiligingsmaatregelen transparant voor de gebruiker en richt deze zo gebruiksvriendelijk mogelijk in. Verleid de gebruiker zo veel mogelijk om veilig te werken: zo leidt het afdwingen van gebruikersonvriendelijke beveiligingsmaatregelen vaak tot onveilige workarounds en ander onveilig gedrag.	VDI moet functioneel gebruikersvriendelijk zijn, dus voorzien in alle functionaliteiten benodigd om een bepaalde taak uit te voeren.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Binnen het bouwblok vindt microsegmentatie plaats.
IMP084 Applicatie	Versleutel gegevens in rust en transport	Versleutel alle gegevensdragers waarop niet-publieke informatie staat, inclusief smartphones en laptops, conform de laatst bekende en geldende richtlijnen. Dit reduceert het risico op een gegevenslek bij verlies van een dergelijk apparaat. Neem voor niet-publieke gegevens ook adequate beveiligingsmaatregelen om ze te beschermen in transit. Dit kan door de verbinding te beveiligen, danwel door encryptie van de informatie zelf. Dit laatste heeft de voorkeur.	Versleutel gegevens in transport. En in rust op elk client device (MAM en MDM).
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP069 Netwerk	Hanteer het zero-trust model	Ga nooit uit van het impliciete vertrouwen dat wie op een bepaald netwerk of systeem komt daar ook hoort: * Controleer overal het netwerkverkeer. * Controleer toegang per sessie. * Hanteer dynamische policies en gebruik daarbij de geldigheidsduur van de laatste authenticatie. * Blijf continue monitoren. Verzamel zoveel mogelijk	ZTNA client op managed (virtuele) werkplek.

		gegevens om de beveiliging te blijven verbeteren. Dit wordt ook wel het 'zero-trust' model genoemd.	
IMP019 Organisatorisch	Maak stelselafspraken over identificatie en authenticatie	Maak stelselafspraken om te komen tot één generiek digitaal stelsel voor identificatie en authenticatie of sluit aan bij een bestaand kanaaloverstijgend stelsel met afspraken over betrouwbaarheidsniveau's.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.

4.13.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Veilige Applicatie- en Datatoegang**
1	Beschikbaar stellen van data ten behoeve van anderen in het zorgnetwerk wordt verplicht. Niet alleen voor betrokkenen in het netwerk, maar ook ten behoeve van het algemeen maatschappelijk belang. Dit heeft gevolgen voor besluiten over toestemming en bezwaren. Alleen als de persoon expliciet de toegang tot zorg- en gezondheidsdata weigert, komen data niet beschikbaar	Mitz gebruiken.

4.13.3 Privacy

Kaderstelling Privacy		Veilige toegang
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

4.14 Kaders Veilige Netwerktoegang (PL8b)

4.14.1 NORA

NORA			Bouwblok
Implicatie nr	Implicatie	Beschrijving	Veilige Netwerktoegang
NAP07.01 Organisatorisch	Diensten vullen elkaar aan	Zorg er voor dat diensten elkaar aanvullen en niet overlappen: Geef een heldere beschrijving van je dienst Stem de opzet van de dienst af met aanbieders van verwante diensten Sluit aan op die verwante diensten Burgers en bedrijven moeten de dienst en de meerwaarde er van kunnen herkennen: de dienst moet uniek zijn en niet overlappen met andere diensten. Dat voorkomt verwarring en zorgt dat de beoogde gebruiker de dienst weet te vinden. Daarvoor moeten individuele organisaties zelf de verantwoordelijkheid nemen om hun dienstverlening naast elkaar te leggen en op elkaar af te stemmen. Dit voorkomt dubbel werk en overlappende diensten.	N.v.t. Betreft een 'basisvoorziening' dienst. Deze dient wel als dienst beschreven te worden.

		De overheid als geheel kan zo efficiënter werken. En bij individuele dienstverleners komt capaciteit en focus vrij om zich te concentreren op de kwaliteit van de unieke dienst die ze aanbieden.	
IMP032 Informatie	Ontwerp diensten met oog voor doelbinding en grondslag	Ontwerp en implementeer diensten met oog voor doelbinding, data-minimalisatie en oorspronkelijke grondslag.	N.v.t. Betreft een 'basisvoorziening' dienst.
IMP089 Organisatorisch	Gebruik standaard oplossingen	Ontwikkel geen eigen processen, systemen en technieken wanneer deze ergens anders al beschikbaar zijn. Stel je actief op de hoogte van beschikbare en geplande standaardoplossingen, om daar bij het maken van plannen rekening mee te houden. De bruikbare elementen van beschikbare standaardoplossingen zullen moeten worden ingepast in de eigen organisatie. Geen enkele standaardoplossing past altijd voor de volle honderd procent. Daarom zal de bereidheid tot het sluiten van compromissen aanwezig moeten zijn.	Met behulp van Gartner, Critical Friends en marktverkenningen wordt het beste standaardpatroon voor Veilige Netwerktoegang bepaald.
IMP025 Organisatorisch Applicatie	Gebruik standaard oplossingen zonder maatwerk	Gebruik een standaardoplossing (zoals bijvoorbeeld een pakketoplossing) zoveel mogelijk ongewijzigd, dus zonder maatwerkaanpassingen. Pas bij de toepassing van een standaardoplossing je werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar het kan de inrichtingsfilosofie van leveranciers.	Standaardoplossing(en) t.b.v. Veilige Netwerktoegang.
IMP036 Organisatorisch Informatie Applicatie Netwerk	Pas open standaarden toe	Verwerf producten die aan de standaard(en) voldoen. Hierbij geldt: Open standaarden tenzij. Implementaties maken gebruik van de beschrijvingen uit de open standaarden om leveranciersonafhankelijkheid te behouden. Maak met afnemers afspraken over de te gebruiken open standaarden. Anticipeer hierbij op de ontwikkeling van de open standaarden, bijvoorbeeld door nieuws over standaarden te volgen via noraonline.nl of www.forumstandaardisatie.nl/	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP037 Organisatorisch	Pleeg onderhoud op de toegepaste standaarden	Zorg via lifecyclemanagement voor toepassing van voldoende actuele versies van standaarden. Inventariseer de relevante standaarden en neem dat mee in het ontwerp van de dienst/voorziening.	Gebruik open standaarden, neem deze op in de dienstbeschrijving, incl. afspraken omtrent versies en richt een proces in om ontwikkelingen te volgen.
IMP063 Organisatorisch	Bepaal de continuïteitseisen	Continuïteitseisen vormen de input voor het maken van een calamiteitenplan. Voorbeelden van continuïteitseisen zijn Maximum Tolerable Outage (MTO), Recovery Time Objective (RTO), Recovery Point Objective (RPO).	Beschikbaarheidseisen t.a.v. deze dienst worden volledig bepaald door de beschikbaarheidseisen van de (primaire) processen die gebruik maken van het platform. Voor de primaire IZB-processen zijn er beschikbaarheidseisen gesteld van 24x7 99.9% uptime waarbij RTO en

			RPO moeten worden vastgesteld.
IMP081 Applicatie	Borg de vertrouwelijkheid van gegevens in maatregelen	De vertrouwelijkheid van gegevens wordt gegarandeerd door scheiding van systeemfuncties, door controle op communicatiegedrag en gegevensuitwisseling, door validatie op toegang tot gegevens en systeemfuncties en door versleuteling van gegevens.	Scheiding van systeemfuncties, controle op communicatiegedrag, controle op gegevensuitwisseling, validatie op toegang en versleuteling van gegevens. Specifiek voor data "in Use" en het tegengaan van externe dataopslag.
IMP062 Organisatorisch	Evalueer de risicoanalyse bij veranderingen	Een verandering in het dreigingsprofiel, of in een bedrijfsproces of in de onderliggende voorzieningen kan een mogelijke kwetsbaarheid introduceren of gevolgen hebben voor de veiligheidsbelangen van stakeholders. Een verandering kan de kans of de impact van een dreiging veranderen.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP079 Informatie Applicatie Netwerk	Garandeer de beschikbaarheid van systemen	ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. De beschikbaarheid van gegevens en systeemfuncties wordt gegarandeerd door: * Vermeervoudiging van systeemfuncties. * Herstelbaarheid en beheersing van verwerkingen. * Voorspelling van discontinuïteit. * Handhaving van functionaliteit.	Het bouwblok wordt ingericht met ten minste de minimale benodigde specificaties voor het voldoen aan de beschikbaarheidseisen.
IMP061 Organisatorisch	Reduceer rest-risico's	Besteed speciale aandacht aan de rest-risico's die overblijven na toepassen van de standaard maatregelen die op basis van de BIO of vanuit de AVG zijn ingericht en weeg de consequenties van de maatregelen af tegen het accepteren van het rest-risico. De verantwoordelijke voor het bedrijfsmiddel moet de rest-risico's accepteren.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP070 Netwerk	Segmenteer het netwerk	Het segmenteren van het netwerk beperkt de gevolgen van een aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld, waartussen een inspectiepunt ontstaat. Netwerksegmentatie voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt.	Alle bouwblokken zijn d.m.v. netwerksegmentatie gescheiden. Binnen het bouwblok vindt microsegmentatie plaats.
IMP086 Applicatie Netwerk	Zorg dat software up-to-date is	Houd alle gebruikte software en software-componenten, van applicatief tot infrastructureel, actueel. Volg de update-cyclus van leveranciers strikt: voer updates, patches en beveiligingsupdates zo snel mogelijk door op alle relevante systemen.	LCM toepassen op bouwblok.
IMP069 Netwerk	Hanteer het zero-trust model	Ga nooit uit van het impliciete vertrouwen dat wie op een bepaald netwerk of systeem komt daar ook hoort: * Controleer overal het netwerkverkeer. * Controleer toegang per sessie. * Hanteer dynamische policies en gebruik daarbij de geldigheidsduur van de laatste authenticatie. * Blijf continue monitoren. Verzamel zoveel mogelijk gegevens om de beveiliging te blijven verbeteren. Dit wordt ook wel het 'zero-trust' model genoemd.	ZTNA: * Controleer overal het netwerkverkeer.

IMP019 Organisatorisch	Maak stelselafspraken over identificatie en authenticatie	Maak stelselafspraken om te komen tot één generiek digitaal stelsel voor identificatie en authenticatie of sluit aan bij een bestaand kanaaloverstijgend stelsel met afspraken over betrouwbaarheidsniveau's.	N.v.t., wel randvoorwaardelijk voor de juiste werking van dit bouwblok.
IMP066 Applicatie	Richt een sterke logging en audit-trail in	Logging is fundamenteel in applicaties. Richt een sterke logging en audit-trail in, voor elke applicatie en elk systeem. Logbestanden en audit-trails spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Logberichten moeten zo veel mogelijk informatie bevatten over hetgeen er gebeurd is (wie, wat, waar, wanneer) en moeten op het juiste niveau gelogd worden. Let er op dat logberichten geen persoonlijke kenmerken (AVG) of security kenmerken (zoals wachtwoorden) mogen bevatten.	Systeemlogging aanleveren.

4.14.2 Nationale visie en strategie op het gezondheidsinformatiestelsel

Bron: Nationale visie en strategie op het gezondheidsinformatiestelsel		
Nr.	**Tekst**	**Implicatie Veilige Netwerktoegang**
1	Beschikbaar stellen van data ten behoeve van anderen in het zorgnetwerk wordt verplicht. Niet alleen voor betrokkenen in het netwerk, maar ook ten behoeve van het algemeen maatschappelijk belang. Dit heeft gevolgen voor besluiten over toestemming en bezwaren. Alleen als de persoon expliciet de toegang tot zorg- en gezondheidsdata weigert, komen data niet beschikbaar	Mitz gebruiken.
2	Daarbij horen ook afspraken over landelijk dekkende infrastructuren. Er loopt momenteel een onderzoek naar scenario's om gegevensuitwisseling versneld te faciliteren met een landelijk dekkend netwerk	Afspraken koppelingen netwerken dienen gemaakt/gevolgd te worden.
3	Een (inter)nationaal vastgesteld stelsel van onderling verbonden infrastructuren	Een (inter)nationaal vastgesteld stelsel van onderling verbonden infrastructuren dient op te worden aangesloten.

4.14.3 Privacy

Kaderstelling Privacy		Veilige toegang
2.5.2.5	Uitvoeren van DPIA's	Op elk bouwblok wordt een DPIA uitgevoerd.

Zwarte Woud 2
3524 SJ Utrecht
ggdghor.nl