

DPIA

Huisartsinzage in cliëntdossier VVT-instelling met gebruik van Nuts

Zorgaanbieder

Google	Kopie maken voor eigen gebruik
Microsoft	Kopie downloaden voor eigen gebruik

Documenteigenaar	Documenteigenaar vanuit zorgaanbieder
Versienummer	1.0
Versiedatum	28 april 2025
Vertrouwelijkheid	Intern gebruik

Inhoudsopgave

Inhoudsopgave	2
1 Inleiding	3
1.1 Over deze DPIA	3
1.1.1 Scope (toepassingsgebied) van deze DPIA	3
1.1.2 Doelgroep van deze DPIA	3
1.1.3 Toepassen van deze DPIA door een zorgaanbieder	4
1.1.4 Betrokkenen bij deze DPIA	4
1.1.5 Afkortingen	5
1.1.6 Versiebeheer	6
2 Uitwerking DPIA	7
2.1 Voorgenomen verwerking	7
2.1.1 Voorstel	7
2.1.2 Persoonsgegevens	8
2.1.2.1 Verwerkte persoonsgegevens in pilot-fase	8
2.1.2.2 Verwerkte persoonsgegevens voorzien op een later moment	9
2.1.2.3 Bijzondere en gevoelige persoonsgegevens	9
2.1.3 Gegevensverwerkingen	9
2.1.4 Verwerkingsdoeleinden	10
2.1.5 Betrokken partijen	10
2.1.6 Belangen bij de gegevensverwerkingen	10
2.1.7 Verwerkingslocaties	11
2.1.8 Technieken en methoden van de gegevensverwerkingen	12
2.1.8.1 Uitgangspunten Nuts-werkgroep	12
2.1.9 Juridisch en beleidsmatig kader	13
2.1.10 Bewaartermijnen	14
2.2 Rechtmatigheid verwerking	14
2.2.1 Rechtsgrond	14
2.2.2 Bijzondere persoonsgegevens	15
2.2.3 Doelbinding	15
2.2.4 Noodzaak en evenredigheid	15
2.2.4.1 Proportionaliteit	15
2.2.4.2 Subsidiariteit	15
2.2.5 Rechten van de betrokkenen	15
2.3 Risico's voor de betrokkenen	17
2.3.1 Proces en criteria	17
2.3.2 Bruto risico's	20
2.3.3 Voorgenomen maatregelen	28
2.3.3.1 Algemene maatregelen	28
2.3.3.2 Specifieke maatregelen	29
3 Beoordeling Functionaris gegevensbescherming zorgaanbieder	37
4 Acceptatie DPIA door directie zorgaanbieder	38

1 Inleiding

De kwaliteit van zorg in Nederland staat onder druk, aldus het Integraal Zorgakkoord uit 2022. Er is een veelvoud aan vraagstukken, en niet allemaal vragen deze om een medisch antwoord. Onderdeel van de problematiek is dat Nederland verschillende zorgstelsels kent, met verschillen in bekostiging en wetgevend kader. Dit heeft geleid tot versnippering en soms moeizame samenwerking in verschillende zorgdomeinen, en uit zich ook in verzuiling van informatie binnen de zorgdomeinen.

Er lopen - gelukkig - vele initiatieven om informatie-uitwisseling tussen de domeinen te harmoniseren, automatiseren en te vergemakkelijken. Eén van deze initiatieven is het inzetten van Nuts-toepassingen om communicatie tussen verschillende zorginformatiesystemen mogelijk te maken. Het (decentrale) Nuts-netwerk maakt gebruik van internationale standaarden om een vertrouwenslaag op het Internet te realiseren. Die standaarden zijn geïmplementeerd in "Nuts-nodes": Open Source software die zonder licentiekosten door elke IT leverancier gebruikt kan worden.

1.1 Over deze DPIA

Deze DPIA ziet toe op de Nuts-toepassing "Huisartsinzage in VVT-dossier", waarmee huisartsen vanuit het cliëntdossier in het gebruikte informatiesysteem rechtstreeks informatie kunnen opvragen uit het elektronisch cliëntdossier (ECD) van een aangesloten VVT-instelling. Dit kan zowel een traditioneel huisartsinformatiesysteem (HIS) zijn, als een tussenlaag zoals platformen voor regionale samenwerking. Randvoorwaardelijk is dat de betreffende zorgaanbieders allemaal deelnemen aan deze ontsluiting van informatie.

Meer informatie en ontwikkelingen rondom deze toepassing zijn hier te lezen:

- [Nuts Wiki: Samenwerken Huisarts en Thuiszorg](#)
- [Github: Toepassing Zorginzage HA VVT](#)

Dit document is opgesteld als een blauwdruk waarvan zorgaanbieders gebruik kunnen maken om binnen de eigen organisatie een DPIA op de voorgenomen toepassing uit te voeren. Het document is opgesteld in opdracht van ActiZ en InEen, onder leiding van een onafhankelijk derde partij.

1.1.1 Scope (toepassingsgebied) van deze DPIA

De Nuts-toepassing op het moment van schrijven betreft *read only*-inzage door de huisarts in het VVT-dossier, en dat is daarmee ook de scope van deze DPIA.

Opmerking: Binnen de Nuts-community bestaat de ambitie deze Nuts-toepassing in de toekomst uit te breiden: een wederzijdse uitwisseling van informatie waarin ook mutaties mogelijk zijn. Waar mogelijk wordt deze toekomstvisie binnen deze DPIA al zo veel als mogelijk meegenomen. Omdat in deze toekomstige situatie echter sprake is van andere verwerkingen en grondslagen is dat niet volledig mogelijk.

1.1.2 Doelgroep van deze DPIA

Het staat iedere organisatie vrij een DPIA uit te voeren op eigen (voorgenomen) verwerkingen. Onder bepaalde omstandigheden is het echter verplicht om een DPIA uit te voeren. Voorwaarden hiervoor zijn te lezen [in deze publicatie van de staatscourant](#). Het is aan de organisatie die deze DPIA beoogt in te vullen om te beoordelen of een DPIA verplicht is, of dat het anderszins wenselijk is om een DPIA uit te voeren.

1.1.3 Toepassen van deze DPIA door een zorgaanbieder

Deze DPIA is geschreven met als uitgangspunt betreffende zorgorganisaties zo veel als mogelijk het werk uit handen te nemen. Waar dingen aangevuld moeten worden is dit duidelijk gemarkeerd in het document.

Legenda

Zorgaanbieder	Te vervangen door de naam van de zorgaanbieder die deze DPIA invult.
XIS-applicatie	Te vervangen door de naam van de XIS-applicatie van de zorgaanbieder, zoals het gebruikte ECD of HIS.
XIS-leverancier	Te vervangen door de naam van leverancier van de XIS-applicatie van de zorgaanbieder.
Algemene tekst	Algemene tekst, aan te passen door de zorgaanbieder die deze DPIA invult naar de eigen situatie.

Let op: De blauwdruk DPIA beschrijft de situatie zoals deze is op **28 april 2025**. Zorgorganisaties zullen de blauwdruk moeten afstemmen op de situatie zoals deze is op het moment van invullen. In het bijzonder bij dreigingen, kwetsbaarheden en maatregelen kunnen en zullen zaken anders zijn. Stem dit af met jouw XIS-leverancier en regionale samenwerkingspartners.

1.1.4 Betrokkenen bij deze DPIA

Projectbegeleider en auteur blauwdruk-DPIA

Nick Zuiderwijk nick@zorgciso.nl 06 - 5354 2586	ZorgCISO	Adviseur informatiebeveiliging en privacy Fractioneel CISO voor zorginstellingen
--	----------	---

Interviewees blauwdruk-DPIA

Dennis Snippert	Ecare	Product owner
Maarten Botterhuis	Nedap Healthcare	Lead Netwerkgzorg
Daan Verbree	Topicus	Platform Integration Officer
Bart van den Heuvel	Wijtz	Partner / adviseur
Cornelis de Pee	ZorgCIO	CIO op afroep

Reviewers blauwdruk-DPIA

Dennis Snippert	Ecare	Product owner
Maarten Botterhuis	Nedap Healthcare	Lead Netwerkgzorg
Daan Verbree	Topicus	Platform Integration Officer
Bart van den Heuvel	Wijtz	Partner / adviseur
Cornelis de Pee	ZorgCIO	CIO op afroep

Djiby Macalou		Adviseur gegevensbescherming
Gerard van den Berg	Sensire / Yunio	Functionaris Gegevensbescherming
Steven Stolp	InEen	Beleidsadviescommissie informatiebeleid
Steven van der Vegt	Stichting Nuts	Bestuurssecretaris
Erik van den Beld	Audittrail	Principal Consultant Privacy Fractioneel FG voor zorginstellingen
Leon van der Zande	Topicus	Lead architect Healthcare
Charlotte de Jong	Sanday	Product Owner Shared Services & Data Sciences
Mireille Kamminga	Topicus	Product owner / analyst

Projectbegeleider interne uitwerking toepassing binnen zorgaanbieder

Naam	Organisatie	Functie / titel
------	-------------	-----------------

Betrokkenen interne uitwerking toepassing binnen zorgaanbieder

Naam	Organisatie	Functie / titel
Naam	Organisatie	Functie / titel
Naam	Organisatie	Functie / titel
Naam	Organisatie	Functie / titel

1.1.5 Afkortingen

Dit hoofdstuk bevat een toelichting op enkele veel gebruikte afkortingen binnen dit document.

XIS	X-informatiesysteem - een overkoepelende, neutrale term voor zorginformatiesystemen binnen de verschillende zorgdomeinen.
HIS	Huisartsinformatiesysteem - het systeem waarbinnen een huisarts o.a. cliëntdossiers voert.
ECD EPD	Elektronisch cliëntendossier - het systeem waarbinnen een VVT-instelling o.a. cliëntdossiers voert. <i>Ook wel bekend als een elektronisch patiëntendossier.</i>
VVT	Verpleeg- en verzorgingshuizen en thuiszorg.
UZI	Unieke Zorgverlener Identificatie. Een uniek nummer ("UZI-nummer") om zorgprofessionals in Nederland te identificeren.
URA	UZI Registratie Abonneenummer. Een uniek nummer ("URA-nummer") die een zorgorganisatie aanduidt.
ANW	Avond, nacht en weekend, veelal gebruikt in het kader van ANW-diensten.

FHIR	Fast Healthcare Interoperability Resources. Internationaal formaat voor uitwisseling van zorginformatie op basis van internet standaarden
ZIB	Zorginformatiebouwsteen. Een implementatie van FHIR voor de Nederlandse zorgsector.

1.1.6 Versiebeheer

0.9	05-04-2025	Nick Zuiderwijk	Conceptversie blauwdruk ter review
1.0	28-04-2025	Nick Zuiderwijk	Initiële blauwdruk na review
1.1	datum	Auteur zorgaanbieder	Conceptversie versie zorgaanbieder voor interne review
1.2	datum	Auteur zorgaanbieder	Initiële versie zorgaanbieder
x.x	datum	Auteur zorgaanbieder	Toelichting
x.x	datum	Auteur zorgaanbieder	Toelichting
x.x	datum	Auteur zorgaanbieder	Toelichting

2 Uitwerking DPIA

2.1 Voorgenomen verwerking

2.1.1 Voorstel

Deze DPIA beoordeelt de voorgenomen inrichting van de Nuts-toepassing “Huisartsinzage in VVT-dossier” bij zorgaanbieder door het uitsluiten van XIS-applicatie tot het hiervoor bedoelde Nuts-netwerk.

Indien deze implementatie onderdeel is van een regionale implementatie van de Nuts-toepassing, kan dit project hier worden beschreven (betrokken deelnemende organisaties, XIS-applicaties, enzovoorts).

Het overkoepelende doel van de Nuts-toepassing “Huisartsinzage in VVT-dossier” is de uitwisseling van informatie tussen VVT-instellingen en huisartsenpraktijken over gezamenlijke cliënten/patiënten verbeteren. In de praktijk gebeurt dit nog vaak telefonisch of per e-mail, wat verschillende risico's met zich meebrengt, zowel op het gebied van informatiebeveiliging als de kwaliteit van zorg. Middels de beoogde implementatie kunnen aangesloten huisartsenpraktijken rechtstreeks inzage krijgen in het cliëntdossier bij aangesloten VVT-instellingen.

In de beoogde situatie kan een zorgprofessional van een VVT-instelling de voorgenomen uitwisseling van informatie tussen de VVT-instelling en een huisartspraktijk vastleggen, na toestemming van de betreffende cliënt / patiënt (*). Hierbij wordt het URA-nummer van de huisarts vastgelegd, zodat de uitwisseling alleen plaats kan vinden met de eigen huisarts.

(*) NB: waar in dit document gesproken wordt over toestemming betreft het toestemming in het kader van de Wgbo. Dit is niet te verwarren met toestemming in het kader van de AVG.

Binnen het HIS wordt functionaliteit toegevoegd op basis waarvan vooraf bepaalde delen van het cliëntdossier van de VVT-instelling in “read only”-modus worden getoond. De betreffende gegevens worden in het volgende hoofdstuk verder uitgelicht. Er worden geen gegevens buiten het bronsysteem opgeslagen.

De doelen van deze specifieke Nuts-toepassing zijn als volgt geformuleerd:

1. Het verbeteren van de informatievoorziening van de huisarts die behoefte heeft aan informatie over wat er in het VVT-domein met de cliënt / patiënt gebeurt;
2. Optimaliseren van het werkproces van een verpleegkundige die belast is met de taak om de huisarts waar nodig op de hoogte te houden.

Nuts wordt in algemene zin gekenmerkt als decentraal netwerk: tussen zorginformatiesystemen vindt directe uitwisseling plaats, zonder dat hier een server van een derde partij tussen zit. De betreffende zorginformatiesystemen installeren hiervoor een zogenaamde “Nuts-node”.

Uitzondering op het decentrale netwerk is een zogenaamde “discovery server” waarbinnen adressering plaatsvindt (“adresboek van zorgverleners”). Deze discovery server verwerkt geen persoonlijke informatie van een cliënt / patiënt, slechts algemene organisatorische informatie over aangesloten zorgorganisaties.

Vanuit het perspectief van de AVG betreft het een bestaande verwerking. Wel zijn de procesmatige en technologische veranderingen van dusdanige aard dat een nieuwe DPIA vereist is.

2.1.2 Persoonsgegevens

In dit hoofdstuk worden de categorieën van persoonsgegevens beschreven zoals verwerkt binnen de beoogde verwerking van gegevens. Deze categorieën komen voort uit persoonsgegevens die onderdeel zijn van geselecteerde zorginformatiebouwstenen (ZIBs), in lijn met uitwisselingen die al in het kader van ANW-diensten plaatsvinden. In de tabel wordt gelinkt naar de betreffende ZIBs en onderliggende FHIR-resources.

Hoewel er geen officiële informatiestandaard bestaat voor onderhavige uitwisseling, vallen de persoonsgegevens die onderdeel zijn van de geselecteerde ZIBs binnen de kader van “*Handreiking Gegevensuitwisseling huisarts en wijkverpleegkundige*” van V&VN en NHG.

Opmerking: de betreffende ZIBs hebben een cardinaliteit van 0-1. XIS-leveranciers hebben een mate van vrijheid om bepaalde sets (gedeeltelijk) niet open te stellen voor uitwisseling.

2.1.2.1 Verwerkte persoonsgegevens in pilot-fase

Concept	ZIB(s)	FHIR	Categorieën van persoonsgegevens
Patiënt/Cliënt Logistiek	[1] [2]	[1]	- Naamgegevens van cliënt/patiënt - Contactgegevens van cliënt/patiënt - Contextuele gegevens van cliënt/patiënt (zoals voorkeursapothek, geslacht, wilsbekwaamheid, taalvaardigheid en nationaliteit) - Persoonlijke gezondheidsgegevens van cliënt/patiënt - Naamgegevens van contactpersoon - Contactgegevens van contactpersoon - Naamgegevens van huisarts - Contactgegevens van huisarts
Tekst rapportages Zorginhoudelijk	n/b	[1]	- Rapportages over cliënt/patiënt
Alerts Zorginhoudelijk	[1]	[1]	- Alerts over cliënt/patiënt (bv. aandoening of conditie, waarschuwing, opmerking)
Wilsverklaring Zorginhoudelijk	[1]	[1]	- Wilsverklaring van cliënt/patiënt incl. aandoening
Woonsituatie Zorginhoudelijk	[1]	[1]	- Woningtype van cliënt/patiënt
Bloeddruk Zorginhoudelijk	[1]	[1]	- Bloeddrukmetingen van cliënt/patiënt
Lichaamsgewicht Zorginhoudelijk	[1]	[1]	- Lichaamsgewichtmetingen van cliënt/patiënt

Concept	ZIB(s)	FHIR	Categorieën van persoonsgegevens
Lichaamslengte Zorginhoudelijk	[1]	[1]	- Lichaamslengtemetingen van cliënt/patiënt
Pijnscore Zorginhoudelijk	[1]	[1]	- Pijnscoremetingen van cliënt/patiënt
Bloedglucose Zorginhoudelijk	[1]	[1]	- Bloedglucosemetingen van cliënt/patiënt
URA-nummer Identificatie	n/b	n/b	- UZI registratie abonneenummer

2.1.2.2 Verwerkte persoonsgegevens voorzien op een later moment

Concept	ZIB(s)	FHIR	Persoonsgegevens
Allergieën Zorginhoudelijk	[1]	[1]	- Allergiegegevens van cliënt/patiënt

2.1.2.3 Bijzondere en gevoelige persoonsgegevens

Binnen de uitwisseling worden verschillende bijzondere en gevoelige categorieën verwerkt, op hoofdlijnen:

- Het BSN ten behoeve van identificatie van een cliënt / patiënt;
- Persoonlijke gezondheidsgegevens ten behoeve van het ontvangen van zorg;
- Contextuele gegevens, zoals taalvaardigheid, nationaliteit en wilsbekwaamheid, ten behoeve van het ontvangen van zorg;

Deze persoonsgegevens worden, net als de reguliere persoonsgegevens, opgehaald bij één bronhouder (cliëntdossier bij de VVT-instelling) en real-time getoond. Deze gegevens worden onderhouden door zorgprofessionals van de betreffende VVT-instelling, en indien noodzakelijk voor het verlenen van kwalitatieve zorg, verwerkt door zorgprofessionals van een huisartspraktijk.

2.1.3 Gegevensverwerkingen

De volgende voorgenomen gegevensverwerkingen zijn in scope binnen deze DPIA:

Alleen voor VVT-instelling

- Openstellen van (geselecteerde delen van) cliëntdossiers vanuit XIS-applicatie tot het hiervoor bedoelde Nuts-netwerk middels inrichting en aansluiting van een Nuts-node.

Alleen voor huisarts

- Ophalen van (geselecteerde delen van) cliëntdossiers vanuit het tot hiervoor bedoelde Nuts-netwerk aangesloten ECDs naar XIS-applicatie middels inrichting en aansluiting van een Nuts-node.
- Het gebruik van de in XIS-applicatie getoonde gegevens uit het cliëntendossier van een VVT-instelling door zorgprofessionals van zorgaanbieder.

2.1.4 Verwerkingsdoeleinden

Het doel van de voornoemde verwerkingen is het efficiënter en effectiever uitwisselen van cliëntdossiers tussen aan het hiervoor bedoelde Nuts-netwerk deelnemende VVT-instellingen en huisartsenpraktijken om de kwaliteit van het zorgproces te verbeteren. Daarnaast worden verschillende positieve verbeteringen ten aanzien van privacy en informatiebeveiliging gerealiseerd, zoals het faciliteren van logging en monitoring, het delen van gestandaardiseerde datasets en het toevoegen van autorisatie- en authenticatie-mechanismen.

2.1.5 Betrokken partijen

Partij	Rol
Patiënt / cliënt	- Data-subject
Eerste contactpersoon en/of wettelijk vertegenwoordiger van patiënt / cliënt	- Data-subject (als onderdeel van contextuele dataset patiënt / cliënt)
Aangesloten VVT-instelling(en)	- Individueel verwerkingsverantwoordelijk voor cliënten binnen eigen XIS - Verstrekker
Zorgprofessionals VVT-instelling(en)	- Data-subject (als onderdeel van contextuele dataset patiënt / cliënt)
Aangesloten huisartspraktijk(en)	- Individueel verwerkingsverantwoordelijk voor cliënten binnen eigen XIS - Ontvanger
Zorgprofessionals huisartsenpraktijk(en)	- Data-subject (als onderdeel van contextuele dataset patiënt / cliënt)
Aangesloten XIS-leverancier(s)	- Verwerker
Leveranciers van aangesloten XIS-leverancier(s)	- Sub-verwerker
Technisch medewerkers XIS-leveranciers	- Ontvanger (in voorkomend geval)
Stichting Nuts	- Derde partij, geen verwerker van persoonsgegevens

2.1.6 Belangen bij de gegevensverwerkingen

Partij	Rol
Patiënt / cliënt	- Ontvangen van tijdige en kwalitatief goede zorg - Veilige, verantwoorde omgang met persoonlijke (gezondheids)gegevens
Eerste contactpersoon en/of wettelijk vertegenwoordiger van patiënt / cliënt	- Tijdig betrokken bij het zorgproces en/of geïnformeerd waar nodig
Aangesloten VVT-instelling(en)	- Efficiënte en effectieve overdracht van

Partij	Rol
	VVT-dossiers aan huisarts - Goede (mogelijkheden tot) inrichting van logging en monitoring binnen het cliëntdossier, inclusief uitwisseling van audittrail - Autoriseren van huisartsenpraktijk tot het cliëntdossier
Zorgprofessionals VVT-instelling(en)	- Tijdig betrokken bij het zorgproces waar nodig - Identificeerbaar bij uitgewisselde informatie in het geval van vragen
Aangesloten huisartspraktijk(en)	- Efficiënte en effectieve ontvangst van VVT-dossiers van VVT-instelling - Goede (mogelijkheden tot) inrichting van logging en monitoring binnen het cliëntdossier, inclusief uitwisseling van audittrail - Verhoging kwaliteit zorgproces t.o.v. huidige situatie
Zorgprofessionals huisartsenpraktijk(en)	- Tijdig betrokken bij het zorgproces waar nodig - Tijdig en compleet geïnformeerd
Aangesloten XIS-leverancier(s)	- Waarde toevoegen aan zorgproces van aangesloten zorgaanbieders - Economisch belang
Leveranciers van aangesloten XIS-leverancier(s)	- Economisch belang
Technisch medewerkers XIS-leveranciers	- Inrichten en onderhouden van Nuts-nodes - Support en ondersteuning kunnen bieden waar nodig
Stichting Nuts	- Baat bij goede implementatie t.b.v. acceptatie en ontwikkeling Nuts-toepassingen

2.1.7 Verwerkingslocaties

Zowel de technische verwerking van de cliëntdossiers als het gebruik van de cliëntdossiers door zorgprofessionals vindt plaats binnen de Europese Economische Ruimte (EER).

Systeem	Locatie van dataopslag
XIS-applicatie	Locatie
Overige betrokken XIS / onderaannemer	Locatie
Overige betrokken XIS / onderaannemer	Locatie
Overige betrokken XIS / onderaannemer	Locatie
Overige betrokken XIS / onderaannemer	Locatie

2.1.8 Technieken en methoden van de gegevensverwerkingen

Momenteel bevindt de Nuts-toepassing zich nog in een pilotfase. Er wordt toegewerkt naar een minimal viable product (MVP) door de betreffende Nuts-werkgroep. Op hoofdlijnen zijn de componenten:

Component	Doel
Nuts-node met inzagerol	XIS van een huisartsenpraktijk (of een regionaal tussenplatform) ontsluiten tot het hiervoor bedoelde Nuts-netwerk
Nuts-node met bronrol	XIS van een VVT-instelling ontsluiten tot het hiervoor bedoelde Nuts-netwerk
Discovery service	Adressering en aansluiting tot het netwerk mogelijk maken

Binnen de beoogde technische inrichting is geen sprake van aanvullende opslag van gegevens: deze blijven binnen het bronsysteem staan (het VVT-dossier). Het betreft een *real-time* doorgifte van informatie. Er vindt geen besluitvorming of profilering plaats in de techniek.

2.1.8.1 Uitgangspunten Nuts-werkgroep

Bij het inrichting van het minimal viable product (MVP) worden [de volgende uitgangspunten gehanteerd](#):

- De patiënt is reeds bekend/in zorg bij zowel de huisarts als bij de VVT instelling;
- De patiënt heeft toestemming gegeven om data te delen met de huisarts;
- Informatie kan opgehaald worden bij het bronsysteem en getoond in het doelsysteem.
- In de documentatie is vastgelegd welke informatie (ZIB's) er beschikbaar gemaakt kan worden via deze koppeling.
- Indien informatie opgehaald wordt, zal deze ook getoond worden in een vorm die passend is in het doelsysteem.
- De medewerkers blijven in hun eigen systeem werken. De leveranciers zijn zelf verantwoordelijk hoe zij de medewerkers het beste willen/kunnen ondersteunen.
- Er wordt gebruikgemaakt van bestaande zorginformatiebouwstenen die voor de leveranciers al bekend zijn. Hierbij wordt FHIR versie STU3 gebruikt.
- Het afhandelen van de toestemmingsvraag vindt plaats in het bronsysteem. Het systeem bepaalt zelf hoe dit vastgelegd wordt en hoe het gecontroleerd wordt
- Authenticatie vindt plaats op basis van een Verifiable Credential: het URA nummer van de organisatie waar de opvrager werkt en zoals vastgelegd in een UZI Servercertificaat.
- Het bronsysteem moet vastleggen en checken welke organisatie bij de informatie mag. Er kan niet op medewerker niveau of rol worden gecontroleerd. Verdere uitwerking in hoofdstuk autorisatie.
- Logging vindt in de gehele keten plaats.

Verder worden met het oog op de toekomst [de volgende uitgangspunten](#) voorzien:

- We sluiten niet aan op Mitz (maar gaan toestemming lokaal oplossen).
- Er is geen goed authenticatiemiddel voor de gebruiker beschikbaar (Dezi) dus werken we met een VC waarbij de organisatie op basis van een UZI certificaat wordt geauthenticeerd.
- We implementeren niet alle mogelijke ZIB's want die zijn niet beschikbaar in bronsystemen, maar hanteren een subset.

- dPOP wordt pas in een later stadium toegevoegd, voor nu maakt dit geen onderdeel uit van de usecase.
- We verrijken / corrigeren de informatie uit de UZI credentials niet (human readable namen), dit moet bij de bron opgelost worden.
- Bij gebrek aan een generieke lokalisatiedienst wordt er een workaround toegepast waarbij handmatig wordt vastgelegd waar de patiënt in zorg is en waar dus informatie opgehaald kan worden.

2.1.9 Juridisch en beleidsmatig kader

Kader	Versie	Reden insluiting
Handreiking Gegevensuitwisseling huisarts en wijkverpleegkundige	7-2-2025	Beschrijft de tussen V&VN en NHG afgesproken kaders (dataset) voor het onderling uitwisselen van informatie
NEN 7510	2024	Minimale eisen aan de systematische inrichting van informatiebeveiliging bij zorgorganisaties en haar ketenpartners
NEN 7512	2022	Verbijzondering van een aantal maatregelen uit NEN 7510-1 bijlage A, waarin eisen aan gestructureerde gegevensuitwisseling in de zorg worden gesteld
NEN 7513	2024	Verbijzondering van een aantal maatregelen uit NEN 7510-1 bijlage A, waarin eisen aan logging en monitoring in zorginformatiesystemen worden gesteld
Algemene verordening gegevensbescherming (AVG) incl. uitvoeringswet (uAVG)		Relevante eisen aan verwerkingsverantwoordelijken en verwerkers ten behoeve van (de beveiliging van) verwerking van persoonsgegevens, en het borgen van rechten van betrokkenen.
Integraal Zorgakkoord (IZA)	2022	Bevat afspraken tussen de overheid en een groot aantal zorgorganisaties, waaronder brancheverenigingen, betreffende onder andere gegevensuitwisseling in de zorg.
Regeling gebruik BSN in de zorg		Kader ten behoeve van het registreren en gebruiken van het BSN gedurende het zorgproces ten behoeve van het identificeren van een cliënt / patiënt.
Besluit elektronische gegevensverwerking door zorgaanbieders		Wettelijke verankering van de verplichting tot het inrichten van NEN 7510, NEN 7512 en NEN 7513 door zorgaanbieders.
Wet op de geneeskundige behandelingsovereenkomst / Wgbo (BW:7, titel 7, afdeling 5)		Regelt de relatie tussen cliënt en zorgverlener.

Kader	Versie	Reden insluiting
De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)		Stelt eisen aan waarborgen voor cliënten / patiënten rondom elektronische gegevensuitwisseling van persoonsgegevens in de zorg.
Wegiz en het EGIZ-stelsel <i>in ontwikkeling</i>		Stellen eisen aan de inrichting van elektronische gegevensuitwisseling in de zorg, onderverdeeld en specifieke gegevensuitwisselingen en generieke functies.
eIDAS-verordeningen inclusief uitvoeringswetten Wet Diaz en het Dezi-stelsel <i>in ontwikkeling</i>		Stellen randvoorwaardelijke eisen aan de inrichting van identificatie en authenticatie van zorgprofessionals en cliënten / patiënten.
Wet op de beroepen in de individuele gezondheidszorg (BIG)		Stelt randvoorwaardelijke eisen aan het (doorbreken van) het medisch beroepsgeheim.

2.1.10 Bewaartermijnen

De beoogde gegevenskoppelingen leiden niet tot (aanvullende) opslag van informatie. Informatie blijft behouden in het bronsysteem (ECD) en wordt niet opgeslagen in het inzagesysteem (HIS of tussenplatform), tenzij zaken handmatig worden overgenomen in het kader van dossiervoering van de huisarts. Reguliere wet- en regelgeving ten aanzien van bewaartermijnen rondom cliëntdossiers zijn en blijven van toepassing.

Werk hier uit hoe de eigen organisatie (omgang met) bewaartermijnen heeft ingericht.

2.2 Rechtmatigheid verwerking

2.2.1 Rechtsgrond

De beoogde gegevensverwerking van persoonsgegevens vindt reeds plaats. Er is geen sprake van nieuwe of gewijzigde grondslagen, al worden verwerkingen in de beoogde situatie wel op een fundamenteel andere wijze ingericht.

De grondslagen voor bestaande en beoogde gegevensverwerkingen zijn:

- AVG artikel 6, lid 1 c) (wettelijke verplichting tot verlenen zorg en het voeren van een dossier)
- In voorkomend geval AVG artikel 6, lid 1 d) (in medische noodsituaties)
- AVG artikel 9, lid 2 h) (opheffing van het verbod tot het verwerken van bijzondere categorieën van persoonsgegevens)
- BW Artikel 7:450 (toestemming voor behandeling)
- BW Artikel 7:457 (voorwaarden voor het verstrekken cliëntgegevens aan derden)
- BW Artikel 7:465 (toestemming voor behandeling bij wilsonbekwaamheid)
- BW Artikel 7:466 (eisen aan veronderstelde toestemming)
- Wet BIG Artikel 88 (ten behoeve van het medisch beroepsgeheim)

Registratie van toestemming (in het kader van de Wgbo) voor het uitwisselen van informatie in het kader van deze Nuts-toepassing, gegeven door cliënt of wettelijk vertegenwoordiger, kan worden vastgelegd in het cliëntdossier van de cliënt / patiënt bij een VVT-instelling. Afspraak tussen de deelnemende leveranciers aan deze Nuts-toepassing is dat toestemming altijd actief wordt vastgelegd, zelfs als het veronderstelde toestemming betreft.

Het vastleggen van de toestemming, in combinatie met registratie van het URA-nummer van de huisarts, zorgt voor technische ontsluiting van het cliëntdossier.

Er is op dit moment geen landelijke informatiestandaard beschikbaar rondom de inzage van het thuiszorgdossier. Wel is er een handreiking gegevensuitwisseling tussen huisarts en wijkverpleegkundige beschikbaar. Deze handreiking wordt opgesteld onder begeleiding van V&VN en NHG. De in hoofdstuk 2.1.2 beschreven set met uitgewisselde persoonsgegevens valt binnen de kaders van de handreiking.

2.2.2 Bijzondere persoonsgegevens

Er is sprake van het verwerken van bijzondere persoonsgegevens. Voor een overzicht van deze gegevens, zie hoofdstuk 2.1.2. In het kader van het verlenen van zorg is er sprake van een uitzonderingsgrond op basis van AVG artikel 9, lid 2 h) en BW Artikel 7:457.

2.2.3 Doelbinding

De persoonsgegevens van de cliënt zijn en blijven alleen gebruikt worden in het kader van het oorspronkelijke doel: verlenen van zorg / uitvoering van de behandelovereenkomst.

2.2.4 Noodzaak en evenredigheid

2.2.4.1 Proportionaliteit

De (technologische) aanpassingen binnen de bestaande verwerkingen veranderen weinig aan de proportionaliteit van de verwerkingen. Hoewel deze nieuwe vorm van uitwisseling ook nieuwe risico's meebrengt - zie hiervoor hoofdstuk 2.3 - brengt het ook significante voordelen mee. Informatie wordt effectiever en efficiënter uitgewisseld, wat de kwaliteit van het zorgproces en de beveiliging van persoonlijke (gezondheids)gegevens ten goede komt.

2.2.4.2 Subsidiariteit

De aanpassingen binnen de verwerkingen brengen significante voordelen met zich mee. De privacy-vriendelijke insteek van Nuts-toepassingen draagt bij aan een hoog niveau van waarborging van privacyrechten van cliënten / patiënten. Dit geldt ook voor de specifieke aanpak, met werken vanuit bronsystemen en (huidige) read-only inzage door zorgprofessionals van een huisartspraktijk.

2.2.5 Rechten van de betrokkenen

Op zorgaanbieders rust vanuit de AVG de plicht om verschillende waarborgen voor betrokkenen in te richten. Bijvoorbeeld een privacyverklaring, verwerkingsregister en het aanstellen van een Functionaris Gegevensbescherming. De wijze waarop dit is ingericht, alsmede de wijze waarop betrokkenen hun rechten kunnen uitoefenen, veranderen door de aanpassingen van de verwerkingen niet. Wel zal **zorgaanbieder** moeten zorgdragen dat de procesmatige en technische aanpassingen voldoende

verwerkt zijn binnen relevante documentatie, zoals de privacyverklaring, het verwerkingsregister, datalekprocedures en het proces rondom (het uitvoering geven aan) privacyrechten van betrokkenen.

Werk hier uit hoe de eigen organisatie (omgang met) privacyrechten van betrokkenen heeft ingericht.

2.3 Risico's voor de betrokkenen

2.3.1 Proces en criteria

Hoofdstuk 2.3 gaat in op geïdentificeerde dreigingen ten aanzien van gegevensbescherming / rechten van betrokkenen rondom de beoogde verwerkingen, en mitigerende maatregelen ter beheersing van deze dreigingen. In het proces (conform ISO 31000 en ISO 27005) komen onderstaande onderdelen aan bod:

ID	Unieke identificatie van de dreiging.
Dreiging	Beschrijving van de dreiging.
Risico-houder	Gedelegeerde houder van het risico.
Kwetsbaarheden	Bekende zwaktes in bijvoorbeeld organisatie, techniek of architectuur, die zouden kunnen leiden tot het manifesteren van een dreiging.
Impact voor betrokkenen	Waarschijnlijke impact voor betrokkenen wanneer de dreiging zich zou manifesteren.
Bruto-risico	Score van kans, impact en risiconiveau vóór het toepassen van maatregelen (inherent risico).
Maatregelen	Specifieke maatregelen ter beheersing van de dreiging.
Netto-risico	Score van kans, impact en risiconiveau ná het toepassen van maatregelen, vandaag de dag.
Risico-acceptatie	Uitspraak of de dreiging adequaat is gemitigeerd, binnen passende kosten-batenverhouding.

Voor het scoren van de bruto en netto risico's wordt gebruikgemaakt van criteria voorgeschreven uit NEN 7512:2022. Dit normenkader ziet toe op de beheersing van risico's rondom het koppelen van applicaties in de zorg. De relevante tabellen zijn hieronder overgenomen.

Let op:

- Het risiconiveau wordt niet geautomatiseerd aangepast op basis van de scores van kans en impact. Deze dient handmatig afgestemd te worden op onderstaande tabel 3.
- Deze DPIA is niet te verwarren met de risicobeoordeling die in het kader van de NEN 7512 uitgevoerd moet worden. Waar deze DPIA toeziet op risico's voor

betrokken, ziet de risicobeoordeling uit NEN 7512 toe op organisatorische risico's. Beide beoordelingen dienen verplicht uitgevoerd te worden.

Tabel 1a NEN 7512:2022 – Gevolgklasse (patiënten en betrokkenen)

Gevolgen voor:		
patiënten in de zin van de Wgbo 5)	betrokkenen in de zin van de AVG	Gevolgklasse
<u>Enkele patiënt</u> : verwonding waarvan herstel op korte termijn mag worden verwacht; psychologisch ongemak.	In beginsel algemeen bekende informatie wordt onthuld.	Zeer klein
<u>Enkele patiënt</u> : verwonding waarvan herstel op korte termijn niet mag worden verwacht; aanzienlijk psychologisch trauma. <u>Meerdere patiënten</u> : verwonding waarvan herstel op korte termijn mag worden verwacht; psychologisch ongemak.	Informatie wordt onthuld waarmee financiële en/of identiteitsfraude kan worden gepleegd.	Klein
<u>Enkele patiënt</u> : ernstige verwonding of ernstige invaliditeit waarvan herstel op korte termijn mag worden verwacht; ernstig psychologisch trauma. <u>Meerdere patiënten</u> : verwonding waarvan herstel op korte termijn niet mag worden verwacht; aanzienlijk psychologisch trauma.	Informatie wordt onthuld die, wanneer gecombineerd met informatie uit openbare bronnen, kan leiden tot een inbreuk op de rechten of vrijheden van betrokkene(n).	Matig
<u>Enkele patiënt</u> : permanente, levens-veranderende invaliditeit en elke andere conditie waarvan de prognose hetzelfde luidt; ernstige verwonding of ernstige invaliditeit waarvan herstel op korte termijn niet mag worden verwacht. <u>Meerdere patiënten</u> : ernstige verwonding of ernstige invaliditeit waarvan herstel op korte termijn mag worden verwacht; ernstig psychologisch trauma.	Informatie wordt onthuld die, wanneer gecombineerd met informatie uit niet-openbare bronnen, kan leiden tot een inbreuk op de rechten of vrijheden van betrokkene(n).	Groot
<u>Enkele patiënt</u> : overlijden. <u>Meerdere patiënten</u> : permanente, levensveranderende invaliditeit en elke andere conditie waarvan de prognose hetzelfde luidt; ernstige verwonding of ernstige invaliditeit waarvan herstel op korte termijn niet mag worden verwacht.	Informatie wordt onthuld die kan leiden tot een inbreuk op de rechten of vrijheden van betrokkene(n).	Zeer groot

Tabel 2 NEN 7512:2022 – Kansklasse

Omschrijving	Gevolgklasse
Verwaarloosbare mogelijkheid van optreden. Een kans van minder dan 0,5 % dat het binnen 1 jaar optreedt; een kans van minder dan één keer in de komende 200 jaar.	Ze er laag
Zou kunnen optreden, maar zal vrijwel nooit optreden. Een kans van 5 % dat het binnen 1 jaar optreedt; een kans van eens in de komende 20 jaar.	La ag
Mogelijk; optreden niet onwaarschijnlijk. Een kans van 10 % dat het binnen 1 jaar optreedt; een kans van eens in de 10 jaar; een kans van tweemaal in de komende 20 jaar.	B escheiden
Zeer goed mogelijk; zal in een groot deel van de gevallen optreden. Een kans van 20 % dat het binnen 1 jaar optreedt; een kans van eens in de 5 jaar; een kans van viermaal in de komende 20 jaar.	Ho og
Zal zeker of vrijwel zeker optreden. Een kans van 50 % dat het binnen 1 jaar optreedt; een kans van eens in de 2 jaar; een kans van tienmaal in de komende 20 jaar.	Ze er hoog

Tabel 3 NEN 7512:2022 – Risicoklasse

Kansklasse	Privacy- resp. gevolgklasse				
	Zeer klein	Klein	Matig	Groot	Zeer groot
Ze er hoog	C	B	B	A	A
Ho og	C	C	B	B	A
B escheiden	D	D	C	B	B
La ag	E	D	D	C	B
Ze er laag	E	E	D	C	C

Let op:

- Er is geen sprake van een minimaal acceptabele risicoklasse. Het is aan zorgaanbieder om te bepalen of netto-risicoscores acceptabel zijn. Dit is in lijn met de aanpak en visie van NEN 7512:2022.

2.3.2 Bruto risico's

Onderstaande dreigingen en kwetsbaarheden zijn opgehaald vanuit interviews met verschillende betrokkenen ("expert-interviews"), zoals beschreven in hoofdstuk 1.1.4.

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
1	Cliëntgegevens niet beschikbaar of niet integer door problemen in techniek of architectuur	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Nuts v6 is een nog onbewezen versie, die nog in bèta versie verkeert. Er zijn vooralsnog bekende compatibiliteitsproblemen met versie v5. - Er wordt gebruikgemaakt van een centrale discovery-server (adresboek) waarvan governance en afspraken nog niet volledig zijn ingericht. Voor nu is dit bij leverancier Topicus belegd, maar nog onduidelijk is onder andere hoe dit op de lange termijn georganiseerd wordt en door wie. - Er kan bij betrokken ECD- en HIS-leveranciers sprake zijn van verschillen in toepassing FHIR / ZIB architectuur. Bijvoorbeeld: als onderdeel van deelname aan eOverdracht gebruiken de meeste ECD-leveranciers oudere ZIBs. HIS-leveranciers gebruiken over het algemeen de meest recente versies. Hierdoor kunnen integriteitsproblemen ontstaan. Ook zijn er nog geen afspraken gemaakt over governance op dit gebied voor de lange termijn (hoe om te gaan met updates, enzovoorts). Verder is duidelijk dat over deze	- Zorg wordt niet tijdig of niet passend verleend omdat gegevens ontbreken, verminkt zijn of tijdelijk niet beschikbaar zijn (performance).	Gevolgs Kans Score	Klein Zeer hoog B

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			problematiek niet te licht gedacht moet worden: onder andere het LSP kampt al jaren met deze uitdaging. Voorkomen moet worden dat dit "pleisters plakken" wordt: dit is op de lange termijn niet houdbaar. - Informatie wordt uitgewisseld na authenticatie met 'verifiable credentials'. In de praktijk is dit het omzetten van een UZI-certificaat naar een bruikbaar format. Hiervoor is een specifieke tool nodig die niet gebruiksvriendelijk is, waardoor HIS en ECD software dit zelf moeten implementeren binnen de eigen software. Dit is nog niet in alle software gereed. - De naar een 'verifiable credential' om te zetten UZI-certificaten worden niet altijd tijdig gedeeld door betrokken IT-leveranciers. Dit kan leiden tot tragere implementaties en problemen bij het vernieuwen van het certificaat (en heeft daarmee invloed op beschikbaarheid van cliëntgegevens). - Niet alle door huisartsenpraktijken gebruikte informatiesystemen zijn huisartsinformatiesystemen. Soms zit er een communicatieplatform / broker tussen, met eigen systeemcertificaten en Nuts-nodes. Dit kan leiden tot technische problemen in de implementatie met onder andere de werking van systeemcertificaten. - Binnen de keten van de uitwisseling van informatie tussen VVT-instelling en huisartsenpraktijk zijn verschillende partijen			

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			betrokken die niet allemaal een overeenkomst met elkaar hebben. Bijvoorbeeld heeft de huisartsenpraktijk geen overeenkomst met de betreffende ECD-leverancier. Bij toekomstige technische of functionele problemen is niet vastgelegd in welke mate men daarop aan kan spreken. Dit geldt in het bijzonder ook voor de discovery service. - Hoewel er testdagen bij leveranciers plaatsvinden, zijn dit momenteel alleen fictieve situaties. Nog onduidelijk is of binnen deze testdagen alle mogelijke scenario's getest worden, en of men niet te veel met alleen "happy flows" test. Wanneer zaken over het hoofd worden gezien geeft dit met de implementatie mogelijk op een later moment problemen.			
2	Cliëntgegevens niet beschikbaar of niet integer door onjuist gebruik HIS/ECD	Zorgaanbieder	- Er kan sprake zijn van verschillen in inrichting en gebruik van het HIS / ECD, waardoor informatie zich bevindt in onjuiste ZIBs. Dit risico lijkt groter te zijn bij huisartsenpraktijken, omdat VVT-instellingen vanuit de inrichting van ANW / eOverdacht al het nodige werk verzet hebben.	- Zorg wordt niet tijdig of niet passend verleend omdat gegevens ontbreken of verminkt zijn	Gevolg Kans Score	Klein ▾ Bescheid... ▾ D ▾
3	Gegevens worden onbevoegd ingezien en gebruikt	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Zowel voor huisartsenpraktijken als VVT-instelling geldt dat autorisatie en authenticatie passend moet zijn ingericht. Dit zijn in algemene zin kwetsbare processen. - Authenticatie-eisen vanuit wet- en regelgeving niet op een gewenste manier zijn ingericht. De implementatie van de eIDAS (1.0) verordening is nooit een volledig succes geweest, mede doordat	- Persoonlijke (gezondheids)gegevens worden op onrechtmatige wijze gebruikt door potentieel onbevoegde personen (zoals een zorgprofessional zonder BIG-registratie, of een zorgprofessional zonder	Gevolg Kans Score	Matig ▾ Zeer hoog ▾ B ▾

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			UZI-passen in de thuis- en wijkzorg niet werkbaar bleken te zijn. Het nieuwe Dezi-stelsel en de NEN 7518 zijn nog niet van kracht, waardoor er nog geen definitieve oplossing is. Hierdoor is authenticatie in HIS en ECD software naar beste kunnen ingericht, maar niet op lange termijn houdbaar en nu een kwetsbaar proces. - Er kan sprake zijn van het delen van accounts en/of UZI-passen, ook bijvoorbeeld van huisartsen door de administratieve ondersteuning. - Van de toekomstige inrichting van het Dezi-stelsel is nog onduidelijk hoe dit ingericht gaat worden. Er wordt gespeculeerd dat dit mogelijk op basis van een DigiD-app gaat gebeuren. Hierbij is gebruikersongemak te voorzien, wat kan leiden tot olifantenpaadjes. Daarnaast is de toekomstige inrichting vooralsnog gericht op uitwisseling tussen BIG-geregistreerde zorgprofessionals. In de wijkverpleging is hier veelal geen sprake van. - In de praktijk zijn er implementatieverschillen in de toepassing van multifactor authenticatie. Verschillende organisaties gebruiken bijvoorbeeld een IP-adres ("fysieke locatie") of e-mailcode als tweede factor, waarvan te betwijfelen valt of de Autoriteit Persoonsgegevens dit als een adequate inrichting ziet. - De raadplegende zorgverlener wordt niet	directe behandelrelatie) - Registraties in logging en monitoring zijn onbetrouwbaar, waardoor acties van zorgprofessionals niet herleidbaar zijn		

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			(opnieuw) geauthenticeerd bij aanvang van de informatie-uitwisseling. Er wordt vertrouwd op het authenticatiemechanisme van het gebruikte zorginformatiesysteem. Deze informatie wordt identificerend meegestuurd in de uitwisseling. - Rol(code)gebaseerd autoriseren is (nog) niet mogelijk binnen de implementatie van deze Nuts-toepassing, waardoor het aanbod van informatie aan de lezer "alles of niets" is. Hiernaast zijn er ook verschillen in wat de verschillende betrokken organisaties bijvoorbeeld als een "zorgteam" ziet, waarvan nog onduidelijk is hoe dit op de lange termijn gaat uitpakken. - Nog onduidelijk is hoe het proces er uit gaat zien van het identificeren van een cliënt / patiënt door een zorgprofessional van een huisartsenpraktijk. Is alleen het BSN voldoende? Of worden ook aanvullende zaken gecontroleerd? Wat dan, en wat is voldoende? - NEN 7513:2024 is nog relatief jong en fundamenteel veranderd, waarmee mogelijk nog niet alle XIS-leveranciers voldoen aan de meest recente vereisten binnen hun software.			
4	Gegevens worden onbevoegd uitgewisseld	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Vanuit zowel de Wgbo als AVG wordt (waar van toepassing) geïnformeerde toestemming door een betrokkene vereist. De doelgroep van deze gegevensuitwisseling (ouderen) is kwetsbaar door verhoogd risico op psychogeriatrische aandoeningen. De drempel om "het vinkje" te zetten binnen het ECD ter accordering voor de	- Persoonlijke (gezondheids)gegevens worden op onrechtmatige wijze uitgewisseld, potentieel met ongewenste individuen	Gevolg Kans Score	Matig Hoog B

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			uitwisseling is daarnaast laag. - Initiatieven rondom toestemmingsprofielen zijn nog maar in beperkte mate geïmplementeerd in zorginformatiesystemen, waardoor mogelijk onvoldoende rekening wordt gehouden met gegeven toestemming. - De geselecteerde set aan gegevens wordt 'as is' overgedragen via de koppeling. Er is maar in beperkte mate sprake van dataminimalisatie of selectieve uitvraag/delen van gegevens, als inherent onderdeel van de inrichting van deze Nuts-toepassing. De bandbreedte zit in tijdigheid (alleen gegevens over periode X ophalen) en implementatie van ZIBs per leverancier. - Bij het tot stand brengen van een koppeling tussen een ECD en HIS, zijn er technisch gezien geen waarborgen voor tijdigheid. Bij onvoldoende inrichting van compenserende organisatorische maatregelen, zullen koppelingen oneindig blijven bestaan, zelfs wanneer hier geen wettelijke basis meer voor is.	- Er wordt meer informatie uitgewisseld dan strikt noodzakelijk voor de zorgvraag		
5	Ongewenst of onjuist gebruik VVT-dossier door medewerker huisartspraktijk	Zorgaanbieder	- VVT-dossiers worden in de basis als 'read only'-tekst gedeeld. Deze tekst kan echter geknipt/geplakt worden, geprint worden, of er kan een screenshot van gemaakt worden. Hier zitten geen extra waarborgen op.	- Persoonlijke (gezondheids)gegevens worden op onrechtmatige wijze gebruikt	Gevolg Kans Score	Zeer klein ▾ Bescheid... ▾ D ▾
6	Niet passend kunnen voldoen aan uitoefening privacyrechten betrokkene	Zorgaanbieder	- Functionaliteit met betrekking tot logging en monitoring moet zichzelf nog bewijzen, onder andere vanwege de problematiek met autorisatie	- Cliënt / patiënt kan privacyrechten niet uitoefenen	Gevolg Kans Score	Zeer klein ▾ Bescheid... ▾ D ▾

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			en authenticatie. - Binnen de keten van de uitwisseling van informatie tussen VVT-instelling en huisartsenpraktijk zijn verschillende partijen betrokken die niet allemaal een overeenkomst met elkaar hebben. Bijvoorbeeld heeft een huisartsenpraktijk geen overeenkomst met de betreffende ECD-leverancier. Bij toekomstige technische of functionele problemen is niet vastgelegd in welke mate men daarop aan kan spreken. Dit geldt in het bijzonder voor de discovery service.			
7	Digitale inbraak cliëntdossier	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- De ontsluiting van het VVT-dossier tot het HIS vormt een extra aanvalsvector, zowel tijdens de overdracht als via het HIS. Omdat deze beoogde verwerking inzet van nieuwe technologie betreft (zie de verschillende punten hierboven) brengt dit verhoogde dreigingsniveaus met zich mee.	- Serieuze inbreuk op privacyrechten cliënt / patiënt, potentieel leidend tot bijvoorbeeld identiteitsfraude of discriminatie.	Gevolg Kans Score	Zeer groot Zeer laag C
8	Lastig werkbaar of onveilig systeem door onbalans in inrichting Nuts-toepassing	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- De balans vinden tussen een werkbaar systeem en een veilig systeem is lastig. Aan de ene kant zijn er veel eisen vanuit wet- en regelgeving ten aanzien van beveiliging. Aan de andere kant moeten zorgprofessionals “gewoon” hun werk kunnen doen. - Deze Nuts-toepassing wordt ontwikkeld ‘voor en door’ leveranciers van HIS en ECD-software. Binnen het project zijn niet direct zorgorganisaties of zorgprofessionals betrokken. Hierdoor is er mogelijk een mismatch in vraag en aanbod van informatie en functionaliteit.	- Zorg wordt trager of met minder context verleend omdat gegevens ontbreken of niet tijdig inzichtelijk zijn; er wordt teruggevallen op oude processen (telefoon, e-mail)	Gevolg Kans Score	Matig Hoog B

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			- Een alternatief voor deze Nuts-toepassing is 1-op-1 koppelingen. Hoewel er momenteel consensus lijkt dat 1-op-1 koppelingen op lange termijn niet rendabel en wenselijk zijn, kunnen implementatieproblemen van deze Nuts-toepassing ertoe leiden dat regio's gaan terugvallen op dergelijke koppelingen. Dit kan adoptie en ontwikkeling van de Nuts-toepassing verstoren.			
9	Gedeelde informatie wordt niet optimaal benut binnen het zorgproces	Zorgaanbieder	- De context van het uitwisselen van informatie wijzigt. Waar voorheen zaken in persoon of telefonisch werden besproken, moeten zorgprofessionals van een huisartspraktijk het nu sneller doen met een stuk tekst. Hierdoor gaan mogelijk nuances verloren, wat afbreuk kan doen aan de kwaliteit van het zorgproces. - Er wordt in de voorziene implementatie van de Nuts-toepassing breder en meer informatie gedeeld. Echter heeft dit pas toegevoegde waarde als deze informatie ook daadwerkelijk gebruikt wordt. Wanneer zorgprofessionals "toch liever een eigen meting doen", of bijvoorbeeld een rapportage van een specialist ouderengeneeskunde of verpleegkundige van een VVT-instelling onvoldoende serieus wordt genomen, doet dit afbreuk aan de toegevoegde waarde van de Nuts-toepassing. - De inrichting van deze Nuts-toepassing binnen het HIS betekent nieuwe functionaliteit op een nieuwe plek. De kans is aanwezig dat deze	- Zorgverlening is inefficiënt, duurt onnodig lang, of kan tot conflicterende diagnoses leiden. - Zorg wordt niet tijdig of niet passend verleend omdat gegevens ontbreken of niet tijdig inzichtelijk zijn	Gevolgs Kans Score	Klein Hoog C

ID	Dreiging	Risico-houder	Kwetsbaarheden	Impact voor betrokkenen	Bruto-risico	
			nieuwe functionaliteit niet begrepen, gekend of gevonden wordt.			

2.3.3 Voorgenomen maatregelen

2.3.3.1 Algemene maatregelen

ID	Maatregel	Opmerkingen en observaties
1	Invullen ▾ Zorgaanbieder heeft NEN 7510-1 aantoonbaar ingericht	Invullen indien van toepassing
2	Invullen ▾ Zorgaanbieder heeft eisen uit de voor deze Nuts-toepassing relevante wet- en regelgeving aantoonbaar ingericht. Zie voor een volledig overzicht het kader uit hoofdstuk 2.1.9.	Invullen indien van toepassing
3	Invullen ▾ Zorgaanbieder en XIS-leverancier hebben NEN 7512 aantoonbaar ingericht (voor de onderdelen die op de eigen organisatie van toepassing zijn)	Invullen indien van toepassing
4	Invullen ▾ Zorgaanbieder en XIS-leverancier hebben NEN 7513 aantoonbaar ingericht (voor de onderdelen die op de eigen organisatie van toepassing zijn)	Invullen indien van toepassing
5	Invullen ▾ Relevante overeenkomsten zijn afgesloten tussen Zorgaanbieder en XIS-leverancier en deze doen voldoende recht aan zaken voortvloeiend uit deze Nuts-toepassing	Invullen indien van toepassing

2.3.3.2 Specifieke maatregelen

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
1	Cliëntgegevens niet beschikbaar of niet integer door problemen in techniek of architectuur	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Invullen - Betrokken leveranciers binnen de Nuts-toepassing werken op transparante wijze (proces, architectuur) conform afspraken in de Nuts-community. - Invullen - Er vinden tussen de betrokken leveranciers binnen de Nuts-toepassing regelmatig testdagen plaats om de techniek te testen. Bij deze testdagen dragen leveranciers voldoende zorg om niet alleen met 'happy flows' te testen. - Invullen - Betrokken leveranciers binnen de Nuts-toepassing maken onderling passende afspraken rondom governance (zoals wijzigingsbeheer, inrichting discovery server, hoe om te gaan met communicatieplatformen / brokers). - Invullen - De Nuts-community maakt passende afspraken met Nictiz over de governance rondom architectuurstandaarden (ZIBs, FHIR, enz.) in relatie tot Nuts-toepassingen. - Invullen - De Nuts-community stelt aangesloten zorgorganisaties op de hoogte van belangrijke updates aan de architectuur. - Invullen - Zorgaanbieder instrueert de toeleverancier van UZI-certificaten om deze op verzoek te delen met XIS-leverancier. - Invullen - Aanvullen met eigen maatregelen indien van toepassing	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
2	Cliëntgegevens niet beschikbaar of niet integer door onjuist gebruik HIS/ECD	Zorgaanbieder	- Invullen - XIS-leverancier geeft voldoende instructies en training aan Zorgaanbieder over hoe de informatievoorziening binnen het gebruikte zorginformatiesysteem in te richten. - Invullen - Zorgaanbieder geeft voldoende training aan haar team over hoe de informatievoorziening binnen het gebruikte zorginformatiesysteem in te richten. - Invullen - Aanvullen met eigen maatregelen indien van toepassing	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen
3	Gegevens worden onbevoegd ingezien	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Invullen - Zorgaanbieder heeft het proces rond autorisaties (rollen en rechten) en authenticatie (gebruikersnaam en wachtwoord, MFA, wettelijke identificatiemiddelen) als volgt ingericht: aanvullen - Invullen - Zorgaanbieder heeft gedragsregels opgesteld over het delen van accounts en authenticatiemiddelen. Medewerkers van Zorgaanbieder ontvangen hierover voldoende training. - Invullen - XIS-leverancier heeft mogelijkheden tot autoriseren en authenticeren in de techniek ingericht conform huidige wet- en regelgeving, rekening houdend met alle beperkingen. De wijze waarop MFA en identificatiemiddelen zijn ingericht voldoen aan alle huidige standpunten van de Autoriteit Persoonsgegevens. - Invullen - XIS-leverancier draagt zorg dat ontwikkelingen in wet- en regelgeving conform autoriseren en authenticeren zo snel mogelijk worden doorgevoerd na publicatie (o.a. Dezi-stelsel, relevante EGIZ-normen).	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
			- Invullen - Waar verbeterpunten worden geïdentificeerd in autorisatiemodellen (zoals het toepassen van rol-code gebaseerd autoriseren) of het meer selectief delen van informatie, voert XIS-leverancier deze op verzoek van Zorgaanbieder zo spoedig mogelijk door. - Invullen - XIS-leverancier draagt zorg dat zorgprofessionals van Zorgaanbieder voldoende middelen hebben om cliënten / patiënten conform wet- en regelgeving te kunnen identificeren. Zorgaanbieder richt hiervoor passende training in voor haar medewerkers. - Invullen - Bovenstaande maatregelen zijn voldoende vastgelegd in de overeenkomsten tussen Zorgaanbieder en XIS-leverancier. - Invullen - XIS-leverancier heeft NEN 7513:2024 aantoonbaar geïmplementeerd. - Invullen - Aanvullen met eigen maatregelen indien van toepassing			
4	Gegevens worden onbevoegd uitgewisseld	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Invullen - Zorgaanbieder heeft het proces rond het verkrijgen en vastleggen van toestemming voor het uitwisselen van informatie passend ingericht conform Factsheet Toestemmingen van VWS. Medewerkers van Zorgaanbieder ontvangen over de inrichting en toepassing hiervan voldoende training. - Invullen - Zorgaanbieder heeft het proces rond het toepassen van toestemmingsprofielen ingericht conform relevante wet- en regelgeving. Medewerkers van	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
			Zorgaanbieder ontvangen over de inrichting en toepassing hiervan voldoende training. - Invullen - XIS-leverancier heeft het proces rond het toepassen van toestemmingsprofielen op voor Zorgaanbieder passende wijze ingericht in de techniek. Waar door Zorgaanbieder gewenst wordt aangesloten op voorzieningen als het LSP. Medewerkers van Zorgaanbieder ontvangen over de inrichting en toepassing hiervan voldoende training. - Invullen - Waar verbeterpunten worden geïdentificeerd in autorisatiemodellen (zoals het toepassen van rol-code gebaseerd autoriseren) of het meer selectief delen van informatie, voert XIS-leverancier deze op verzoek van Zorgaanbieder zo spoedig mogelijk door. - Invullen - Zorgaanbieder houdt binnen het proces van het koppelen van het VVT-dossier aan het huisartsdossier voldoende rekening met tijdigheid. De koppeling wordt ongedaan gemaakt wanneer deze geen wettelijke basis meer heeft. XIS-leverancier voorziet hier in de techniek voldoende in. Er worden geen gegevens opgeslagen binnen een informatiesysteem van een huisarts. Daarnaast wordt de context van een cliënt / patiënt meegewogen in autorisaties (zoals of de persoon nog in zorg is). Medewerkers van Zorgaanbieder ontvangen over de inrichting en toepassing hiervan voldoende training. - Invullen - Aanvullen met eigen maatregelen indien van toepassing			
5	Ongewenst of onjuist gebruik VVT-dossier door medewerker	Zorgaanbieder	- Invullen - Zorgaanbieder heeft gedragsregels opgesteld over hoe haar medewerkers gebruik mogen maken van	Gevolg Kans	Invullen -	Invullen -

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
	huisartspraktijk		informatie gedeeld vanuit het VVT-dossier. Medewerkers van Zorgaanbieder ontvangen over de inrichting en toepassing hiervan voldoende training. - Invullen - Aanvullen met eigen maatregelen indien van toepassing	Score	Invullen - Invullen -	Toelichting: invullen
6	Niet passend kunnen voldoen aan inzageverzoek betrokkene	Zorgaanbieder	- Invullen - Zorgaanbieder heeft het proces rond autorisaties (rollen en rechten) en authenticatie (gebruikersnaam en wachtwoord, MFA, wettelijke identificatiemiddelen) ingericht zoals beschreven onder dreiging #3. - Invullen - Zorgaanbieder heeft gedragsregels opgesteld over het delen van accounts en authenticatiemiddelen. Medewerkers van Zorgaanbieder ontvangen hierover voldoende training. - Invullen - XIS-leverancier heeft mogelijkheden tot autoriseren en authenticeren in de techniek ingericht conform huidige wet- en regelgeving, rekening houdend met alle beperkingen. De wijze waarop MFA en identificatiemiddelen zijn ingericht voldoen aan alle huidige standpunten van de Autoriteit Persoonsgegevens. - Invullen - Zorgaanbieder heeft een passende organisatorische inrichting voor het afhandelen van privacy-verzoeken van cliënten / patiënten. Met XIS-leverancier zijn hierover passende afspraken gemaakt, inclusief toepassing hiervan in de keten. Deze afspraken zijn gedocumenteerd in relevante overeenkomsten. Medewerkers van Zorgaanbieder ontvangen hierover voldoende training.	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
			- Invullen - Logging en monitoring in XIS-applicatie is ingericht conform eisen uit NEN 7513. Zorgaanbieder heeft de procesmatige toepassing hiervan voldoende ingericht. XIS-leverancier voorziet in de techniek voldoende in de toepassing van relevante eisen uit NEN 7513. - Invullen - Aanvullen met eigen maatregelen indien van toepassing			
7	Digitale inbraak cliëntdossier	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Invullen - De betreffende Nuts-toepassing is open source en ingericht conform best practices. Hierdoor kan een ieder gemakkelijk bijdragen aan het verbeteren van gebruikte code. - Invullen - XIS-leverancier is gecertificeerd tegen de volgende normenkaders (onder accreditatie): invullen, bijvoorbeeld NEN 7510-1, ISO 27001, ISO 27017, ISO 27018 of ISO 27701 - Invullen - XIS-leverancier kan de volgende assurance verklaringen overleggen: invullen, bijvoorbeeld ISAE 3000 type 1 of 2, of ISAE 3402 type 1 of 2 - Invullen - Aanvullen met eigen maatregelen indien van toepassing	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen
8	Lastig werkbaar of onveilig systeem door onbalans in inrichting Nuts-toepassing	Zorgaanbieder Organisatorisch XIS-leverancier Techniek	- Invullen - Er vindt in voldoende mate overleg plaats tussen de leveranciers betrokken bij de Nuts-toepassing en zorgprofessionals (gebruikers) om de balans tussen veilig en werkbaar te bewaken. Ook is er sprake van een uitgebreide pilot. - Invullen - Binnen de werkgroep van de Nuts-toepassing	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
			is voldoende kennis aanwezig over relevante wet- en regelgeving, en deze kennis wordt voldoende toegepast. - Invullen - Er is voldoende aandacht voor implementatieplannen en acceptatietesten. De acceptatietesten voldoen minimaal aan de eisen gesteld vanuit de Algemene Inkoopvoorwaarden Gezondheidszorg (AIVG) - module ICT. - Invullen - Er zijn contractuele afspraken gemaakt tussen Zorgaanbieder en XIS-leverancier over het melden en afhandelen van gebruikersmeldingen ná implementatie. Bijvoorbeeld bij performance problemen, gebruikersongemak of andere functionele problemen. Deze meldingen worden tijdig en naar tevredenheid opgepakt. - Invullen - Aanvullen met eigen maatregelen indien van toepassing			
9	Gedeelde informatie wordt niet optimaal benut binnen het zorgproces	Zorgaanbieder	- Invullen - Zorgaanbieder heeft passende organisatorische maatregelen ingericht om verlies van context in de uitwisseling op te vangen, te weten: aanvullen - Invullen - Zorgaanbieder heeft gedragsregels opgesteld over hoe om te gaan met informatie uit cliëntdossiers verkregen van andere instellingen, ten behoeve van het borgen van kwaliteit en efficiëntie van het zorgproces. Medewerkers van Zorgaanbieder ontvangen hierover passende training. - Invullen - Zorgaanbieder geeft haar medewerkers passende training over de nieuwe functionaliteit binnen zorginformatiesystemen, voortvloeiend uit deze	Gevolg Kans Score	Invullen - Invullen - Invullen -	Invullen - Toelichting: invullen

ID	Dreiging	Risico-houder	Maatregelen	Netto-risico		Risico-acceptatie
			Nuts-toepassing. - Invullen ▼ Aanvullen met eigen maatregelen indien van toepassing			

3 Beoordeling Functionaris gegevensbescherming zorgaanbieder

Deze pagina is gereserveerd voor de FG van de zorgaanbieder die de blauwdruk afrondt. Op deze pagina kan de FG zijn of haar bevindingen en oordeel over de volledig uitgewerkte DPIA invoegen.

4 Acceptatie DPIA door directie zorgaanbieder

De directie van zorgaanbieder onderschrijft de werkwijze en uitkomsten van deze DPIA, inclusief acceptatie van restrisico's, geïdentificeerde benodigde maatregelen en de eindverantwoordelijkheid die hiermee gepaard gaat. Wij zullen ons inspannen om deze verbeteracties zo goed als mogelijk te faciliteren middels het beschikbaar stellen van voldoende middelen.

Namens de directie van zorgaanbieder,

Naam

Functie

Handtekening

.....

Plaats, Datum