Data Privacy Impact Assessment (DPIA) eOverdracht

RSO Trijn

Versie 0.3
15 juli 2025

Documentbeheer

Documentnaam	Data Privacy Impact Assessment (DPIA) eOverdracht
Versienummer definitief document	
Datum definitief document	
In opdracht van	
Auteurs	Daymian Vos Dick van Mourik Evelien Kruisselbrink Mbalia Hovius Sanne van Delft

Versiebeheer

Versie	Datum	Auteur/review	Samenvatting van de wijzigingen

Distributielijst

Versie	Datum	Naam	Functie	Organisatie

Gewenste planning
Op welke termijn is het de bedoeling dat het project begint, eindigt, en wanneer de DPIA afgerond moet zijn? In het opmerkingenveld mogen alle betrokkenen aanvullingen plaatsen.

Fase	Gewenste datum	Opmerkingen
Begin project		Voorbereidende acties
Eindconclusie DPIA		
Einde project		
Evaluatie DPIA		In te vullen door de Privacy Officer

Inhoudsopgave

ACHTERGRONDINFORMATIE

Met dit template stelt u een Data Protection Impact Assessment (DPIA) op voorafgaand aan de start van een nieuw project. In dit geval het project eOverdracht. Bij de start is het namelijk nog mogelijk om met open vizier na te denken over de effecten en bestaat er nog voldoende gelegenheid om de uitgangspunten van het project zonder grote nadelige consequenties te herzien. Dit voorkomt ook latere, kostbare aanpassingen in processen, herontwerp van systemen of zelfs stopzetten van een project.

In deze DPIA staan de stappen die nodig zijn om een DPIA uit te voeren en te documenteren. Alle voorbeeldtekst uit het plan kan naar eigen inzicht worden aangepast; het dient als handvat. Ook heeft u de mogelijkheid informatie uit deze template over te nemen in uw eigen template.

De Autoriteit Persoonsgegevens (AP) heeft een lijst opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is voordat de verwerking is begonnen. Deze lijst is **niet** uitputtend. Het kan zijn dat je zelf moet beoordelen of de verwerking een potentieel hoog risico oplevert. Zie hier voor de lijst.

Invulinstructie

Beantwoord kort en duidelijk de gestelde vragen in elke paragraaf. Tekst tussen rechte haken < > is een aanwijzing voor het invullen van gegevens. Daarnaast wordt veelvuldig een voorbeeld antwoord in cursief getoond. Je kunt deze toelichting telkens weghalen. Binnen het MeO project van RSO Trijn zijn veel organisaties betrokken. Deze DPIA geldt als template voor de deelnemende organisaties. Neem contact op het de eigen privacy en security-organisatie om deze DPIA voor te leggen en eventueel aan te passen.

Het opstellen van de DPIA is een gezamenlijk proces waaraan de Projectleider, Privacy Officer, Security Officer, Functionaris Gegevensbescherming (verder FG) en de Project Eigenaar deelnemen.

Deel 1 | Projectleider
Het eerste deel van de DPIA wordt ingevuld door een Projectleider, een persoon die goed weet wat de (nieuwe) verwerking inhoudt, op welke manier en waarom iets wordt opgepakt. Dit eerste deel beschrijft onder meer waar het project om gaat en in welke context het wordt uitgevoerd. Uiteraard kan de Projectleider wel vragen om hulp bij de Privacy - of Security Officer.

Deel 2 | Privacy Officer
Het tweede deel wordt ingevuld door de Privacy Officer nadat het eerste deel is ingevuld. In dit deel wordt de juridische validiteit aangetoond (of niet).

Deel 3 | Security Officer
Vervolgens is de Security Officer aan zet in het derde deel. In dit deel worden de risico's en beheersmaatregelen voor het project behandeld. Als het onderwerp van de DPIA groot is, kan het nodig zijn een aanvullende risico analyse op te stellen.

Deel 4 | Functionaris Gegevensbescherming
In het vierde deel wordt aan de FG het advies gevraagd.

Deel 5 | Project Eigenaar
De eindconclusie wordt tenslotte door de Project Eigenaar ingevuld. Daarbij wordt de bestuurder om goedkeuring gevraagd om met dit project verder te gaan en is toegelicht wat er met het advies van de FG is gedaan.

Organisatie specifieke planning
De Projectleider vult op de eerste pagina de gewenste planning in. Behalve de datum voor de evaluatie van de DPIA; dat is een taak van de Privacy Officer.

Bij het invullen van de DPIA wordt deze ook geregistreerd door de Privacy Officer. Vier keer per jaar wordt gekeken welke DPIA's moeten worden geëvalueerd. Bij de registratie wordt direct ook de geplande evaluatiedatum vastgesteld in dit document ingevuld.
Vanuit het verwachtingsmanagement is het goed om naar de planning te kijken en eventueel een opmerking te plaatsen. Iedereen die betrokken is bij de DPIA mag opmerkingen plaatsen in de derde kolom in de tabel planning onder het kopje Documentbeheer.

Sommige organisaties kennen geen uitgebreide differentiatie van functies of rollen. Dan is het advies om andere personen wel mee te laten kijken en dit te toetsen bij de bestuurder.

Rechten en vrijwaring

eOverdracht is een nieuwe manier van de medische overdrachten die nu op een andere wijze plaatsvinden. Indien verwerking belangrijk verandert, en vooral als er op grote schaal bijzondere persoonsgegevens verwerkt worden, is de organisatie verplicht een DPIA uit te voeren.

V&VN en ICTU zijn zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan V&VN en ICTU geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. V&VN en ICTU aanvaarden ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan. De ontvangende partij kan geen rechten ontlenen aan dit document.

1 Invullen door de Projectleider

1.1 Aanleiding en achtergrond

Ondanks dat gegevens steeds meer digitaal worden vastgelegd, kunnen verpleegkundigen en verzorgenden nog onvoldoende gebruikmaken van de voordelen van digitale vastlegging. Denk aan hergebruiken van gegevens, efficiënt uitwisselen en minder registratielast. Gegevens worden in gescheiden systemen opgeslagen en zijn bovendien niet eenduidig. Hierdoor is er geen uitwisseling tussen systemen en moeten verpleegkundigen extra registraties uitvoeren. En moeten ze hun gegevens nog handmatig overtypen als een cliënt wordt overgeplaatst. Daarnaast is de verpleegkundige overdracht niet volledig en kan zelfs ontbreken. De verpleegkundige overdracht is dan ook een kwetsbaar onderdeel in het zorgproces. Hierdoor ontstaan risico's in de zorg voor de cliënt.

Jaarlijks vinden ongeveer 460.000 overdrachten plaats in Nederland, door ongeveer 296.000 verpleegkundigen (52%), verpleegkundig specialisten (1%) en verzorgenden (47%), waarbij zij informatie uitwisselen tussen duizenden verschillende organisaties in verschillende sectoren met het doel om de zorg voor hun patiënten te kunnen continueren. Het gaat om sectoren zoals de thuiszorg, verpleeg- en verzorgingshuizen, geestelijke gezondheids- en verslavingszorg, gehandicaptenzorg en ziekenhuizen. Binnen deze sectoren bestaan verschillende soorten organisaties die ook verschillen van grootte. Vandaar dat het aantal mogelijke overdrachten enorm groot is, waardoor een zeer complex zorgnetwerk bestaat.

Om de kwaliteit van de overdracht tussen verpleegkundigen en verzorgenden te verbeteren, is door het Informatieberaad Zorg een Informatiestandaard voor de verpleegkundige overdracht vastgesteld: eOverdracht. Dit is een verzameling afspraken die ervoor moet zorgen dat de zorginformatie met de juiste kwaliteit van de ene naar de andere zorgorganisatie wordt overgedragen. Zodat de kwaliteit en continuïteit van de informatie in de verpleegkundige overdracht wordt verbeterd.

Daarnaast is er ook het Integrale Zorgakkoord (IZA), waar geschreven staat dat gegevensuitwisseling (lees: eOverdracht) gerealiseerd moet zijn in 2025/2026. Dit sluit aan op de Wet Elektronische gegevensuitwisseling in de zorg (Wegiz) die per 1 juli 2023 in werking is getreden.

1.2 Probleemstelling

De implementatie en borging van de verpleegkundige overdracht wordt verschillend en niet volledig opgepakt. Dit heeft gevolgen voor de:

- continuïteit en kwaliteit van zorg. De overdracht wordt vaak in papieren vorm met de cliënt meegegeven of wordt nagestuurd. Verpleegkundigen moeten de gegevens handmatig invoeren in hun systeem. Dat betekent dat zij navraag moeten doen bij de patiënt of mantelzorger en bedenken hoe de informatie moet worden omgezet naar gegevens in hun systeem. Verschil van interpretatie en verlies van informatie kunnen voorkomen. Hierdoor kunnen fouten ontstaan en wordt de zorg niet altijd even goed uitgevoerd.
- registratielast (uitvoerend niveau). Verpleegkundigen zijn veel tijd kwijt aan het omzetten van informatie in hun systeem. Gegevens moeten vaak nog handmatig worden ingevoerd omdat gegevens niet kunnen worden hergebruikt.
- belemmering van het overdrachtsproces (beleidsniveau). Verpleegkundigen, transferverpleegkundigen en wijkverpleegkundigen houden zich bezig met de overdracht van een cliënt. Aangenomen wordt dat verpleegkundigen gemiddeld minimaal 20 minuten bezig zijn met een overdracht en dat er ongeveer 500.000 verpleegkundige overdrachten per jaar zijn.

1.3 Projectdoel en doeleinde gegevensverwerking

De aanleiding voor de gegevensverwerking en daarmee de uit te voeren DPIA is een nieuwe, digitale manier van het overdragen (eOverdracht) van een cliënt (transfer) en bijbehorend verpleegkundig dossier van zorgaanbieder A (een ziekenhuis of VVT-organisatie) naar zorgaanbieder B. Het kenniscentrum Nictiz ontwikkelde ten behoeve van de elektronische overdracht de standaard eOverdracht.

De eOverdracht is een set van cliëntgegevens gericht op de verpleegkundige overdracht en is van belang om de continuïteit en veiligheid van zorg te kunnen waarborgen. Het overdragen van cliëntgegevens betreft hier het overdragen van zorg door verpleegkundig specialisten, verpleegkundigen en verzorgenden in de keten tussen verschillende zorgaanbieders. Met de overdracht worden de verantwoordelijkheden formeel gedeeld met de ontvangende zorgorganisatie.

Het doel van de gegevensverwerking is het op een veilige, eenduidige en elektronische manier overdragen (uitwisselen c.q. delen) van medische gegevens tussen zorgorganisaties ten behoeve van het kunnen overdragen van een cliënt.
Doelen die we hiermee bereiken zijn:

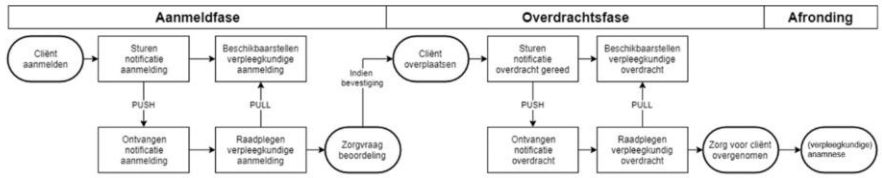
- Het verminderen van administratieve lasten;
- Een verbeterde kwaliteit en volledigheid van de inhoud van de overdracht;
- Het minder herhaaldelijk uitvragen van informatie bij cliënten;
- Het faciliteren van een verbeterde continuïteit van zorg in de keten;
- Dit alles zodat zorgverleners meer tijd aan cliënten kunnen besteden.

1.4 Projectscope

De scope van het project is de overdracht door verpleegkundigen van cliënten naar een andere zorgorganisatie. Het gaat hierbij om de volgende use case(s) te gebruiken.

De volgende use cases kunnen worden geïmplementeerd:
1. Uitwisseling gegevens van ziekenhuis naar thuiszorg.
2. Uitwisseling gegevens van thuiszorg naar ziekenhuis.
3. Uitwisseling gegevens van ziekenhuis naar verpleeghuis.
4. Uitwisseling gegevens van verpleeghuis naar ziekenhuis.
5. Uitwisseling gegevens van ziekenhuis naar gehandicaptenzorg.
6. Uitwisseling gegevens van gehandicaptenzorg naar ziekenhuis.
7. …

De procesflow van de sturende organisatie (bovenste stroom) naar de ontvangende organisatie (onderste stroom) ziet er als volgt uit.



Procesflow eOverdracht met aanmeld- en overdrachtsfase.
Bron: Bureau InZicht: Specificatie-leveranciers-inzicht-pgo-en-eoverdracht (2020)

1.5 Betrokken partijen

Partijen waarvan de gegevens worden verwerkt

Betrokkenen
Cliënten van Thuiszorgorganisatie A
Cliënten van Thuiszorgorganisatie B
Patiënten van Ziekenhuis A
Etc.

Wie zijn de ontvangers?
De volgende personen en organisaties kunnen de eOverdracht data raadplegen.

Betrokkenen
Verpleegkundigen van Thuiszorgorganisatie A betrokken bij de behandeling van de cliënt
Verpleegkundigen van Thuiszorgorganisatie B betrokken bij de behandeling van de cliënt
Verpleegkundigen van Ziekenhuis A betrokken bij de behandeling van de patiënt
Etc.

1.6 Techniek en methoden van de gegevensverwerkingen

Methode van de gegevensverwerking
Hiervoor verwijzen naar het functionele ontwerp dat is opgesteld door Nictiz, zie https://informatiestandaarden.nictiz.nl/wiki/Landingspagina_Verpleegkundige_Zorg
Dit functioneel ontwerp beschrijft alle uitwisselscenario's (use cases) voor de eOverdracht met de transacties, transactiegroepen, de systemen, de systeemrollen en de bedrijfsrollen van zorgverleners of patiënten. Daarvoor worden de eisen gegeven voor het sturen of ontvangen van gegevens.

Techniek gegevensverwerking
De volgende technieken worden toegepast in het proces van de eOverdracht.

Registeren in bronsysteem
- De zorgverlener in het ziekenhuis blijft zoals gebruikelijk de cliëntinformatie registreren in het bronsysteem. BSN-validatie is hierbij verplicht.
    - Werkstation met toegang tot het bronsysteem *<EPD>* en internet
- De zorgverlener in het de thuiszorgorganisatie blijft zoals gebruikelijk de cliëntinformatie registreren in het bronsysteem. BSN-validatie is hierbij verplicht.
    - (Mobiel) device met toegang tot het bronsysteem *<ECD>* en internet
- De zorgverlener in het de thuiszorgorganisatie blijft zoals gebruikelijk de cliëntinformatie registreren in het bronsysteem. BSN-validatie is hierbij verplicht.
    - Werkstation met toegang tot het bronsysteem *<Behandeldossier>* en internet
- Werkstation met toegang tot *<broker>* en internet browser
- Koppeling EPD
- Koppeling ECD
- Firewall
    - EPD en ECD staan achter de firewall
- Gebruik Internet en connectie:
    - HTTPS-protocol
    - Poort 443 moet derhalve open staan voor https connectie
    - eOverdracht maakt gebruik van officiële certificaten (SHA256 en RSA2018 bit)
- De volgende afspraken zijn gemaakt over authenticatie
    - De authenticatie en inrichting is in lijn met NEN7510
    - Iedere zorgprofessional is geïdentificeerd en voorzien van een unieke eigen gebruikersnaam op zowel de werkplek als in het gebruikte informatiesysteem.
    - Zorgverleners authentiseren zich voor het bronsysteem minimaal volgens twee-factorauthenticatie.

- De regionale samenwerkingsovereenkomst (onderling tussen de zorgorganisaties) en in de dienstverleningsovereenkomst (indien gebruik gemaakt wordt van een broker) leggen vast dat de zorgaanbieder authentiseert met minimaal twee-factor-authenticatie in lijn met NEN7510, en dat zorgaanbieders (en leverancier) elkaar hierop onderling kunnen en mogen vertrouwen.
- VPN-verbinding in lijn met NEN7510 tussen de betrokken partijen.

- In de dagelijkse praktijk werken ook niet-zorgverleners met het bronsysteem (administratie, praktijkondersteuning, spreekuur voorbereiden). Organisatorisch moet dus geborgd worden dat zij geen toegang hebben tot de eOverdrachtgegevens of moeten er dekkende werkafspraken gemaakt worden o.b.v. een aantoonbare/reproduceerbare autorisatiematrix (naam – functie – toegang – toelichting) over welke rollen zodanig rechtstreeks betrokken zijn bij het verlenen van de zorg dat gebruik maakt van de eOverdrachtgegevens.
- Zie ook verderop onder Logging. Logging en periodieke monitoring (door zorgorganisatie) zijn essentieel in het signaleren van het “doorbreken” van ontbrekende behandelrelatie.

1.7 Samenstelling werkgroep Informatiebeveiliging en Privacy

Benoem hier de medewerkers van de werkgroep Informatiebeveiliging en Privacy uit uw samenwerkingsverband.

Rol	Naam	Contactgegevens
Projectleider		
Privacy Officer		
Security Officer		
Functionaris Gegevensbescherming		
Project Eigenaar		
Etc.		

1.8 Classificatie van gegevens en informatiesystemen

Keuze	Niveau	**Beschikbaarheid**: uitval van de gegevensuitwisseling levert:
☐	Laag	geringe gevolgen op voor de betrokkenen Kantoortijden (8:30-17:00 uur) Gegevensverlies max 24 uur bij uitval
☒	Midden	Matige gevolgen op voor de betrokkenen Dag en avond (7:00 - 22:00 uur) Gegevensverlies max 1 uur bij uitval
☐	Hoog	Omvangrijke gevolgen op voor de betrokkenen Dag en avond (5:00 - 23:00 uur) Gegevensverlies max 1 uur bij uitval
☐	Zeer hoog	Catastrofale gevolgen op voor de betrokkenen Continue (7 dagen per week, 24 uur per dag)

Keuze	Niveau	**Integriteit**: onjuistheid of onvolledigheid van de gegevensuitwisseling levert:
☐	Laag	geringe gevolgen op voor de betrokkenen
☐	Midden	matige gevolgen op voor de betrokkenen
☐	Hoog	omvangrijke gevolgen op voor de betrokkenen
☒	Zeer hoog	catastrofale gevolgen op voor de betrokkenen.

Keuze	Niveau	**Vertrouwelijkheid**: Ongewenste openbaarmaking of verspreiding van de uitgewisselde gegevens levert:
☐	Laag	geringe gevolgen op voor de betrokkenen
☐	Midden	matige gevolgen op voor de betrokkenen
☒	Hoog	omvangrijke gevolgen op voor de betrokkenen
☐	Zeer hoog	catastrofale gevolgen op voor de betrokkenen

Maximaal gegegevensverlies: geen
Maximaal uitvalsduur: 1 uur
Zie verder SLA.

2 Invullen door de Privacy Officer

In dit hoofdstuk wordt de noodzaak en evenredigheid toegelicht. De onderwerpen in dit hoofdstuk geven u hier richtlijnen voor. Achter elke stap staat telkens het bijbehorende artikel uit de AVG benoemd. De verwerking moet uiteraard aan de AVG voldoen. Controleer hetgeen wordt ingevuld op overeenstemming met het bijbehorende artikel.

2.1 Gespecificeerde, expliciete en gerechtvaardigde doeleinden (art. 5 lid 1)

Het doel van de verwerking is gespecificeerd, expliciet en gerechtvaardigd, zoals hieronder nader is toegelicht.

2.1.1 Doel te bereiken met geanonimiseerde of gepseudonimiseerde gegevens?

Het doel kan niet worden bereikt met geanonimiseerde of gepseudonimiseerde data. Het gaat om het beschikbaar maken van medische gegevens uit bronsystemen aan de betrokken zorgprofessionals waarmee de cliënt een behandelrelatie heeft en indien er sprake is van een toestemmingsgrondslag.

2.1.2 Welke categorieën persoonsgegevens worden verwerkt?

<Vink aan welke van toepassing zijn>

☒ Gewone persoonsgegevens
☒ Bijzondere persoonsgegevens
☒ Wettelijk voorgeschreven persoonsnummer (bijv. BSN)
☐ Uniek identificerende gegevens (bijv. biometrische gegevens, vingerafdruk)
☐ Gegevens die gedrag, locatie of prestaties in kaart brengen
☐ Andere gegevens met een hoge gevoeligheid

Omzetten van gegevens	Beschikbaar maken	Opslaan	Wettelijke bewaartermijn
Cliënten			
Persoonsgegevens[1], waaronder NAW, geboortedatum, Telefoon, Mailadres en BSN. Medische gegevens	Persoonsgegevens, waaronder NAW, geboortedatum, Telefoon, Mailadres en BSN. Medische gegevens	Persoonsgegevens, waaronder NAW, geboortedatum, Telefoon, Mailadres en BSN. Medische gegevens	Gegevens: 20 jaar Toestem-mingen: 20 jaar Logging: 5 jaar

[1] De persoonsgegevens die worden verwerkt bij de eOverdracht bestaat uit gestructureerde informatie, hetzij de zorginformatiebouwstenen (zibs), en ongestructureerde informatie (pdf). Het actuele overzicht van de betreffende zibs is beschikbaar via https://informatiestandaarden.nictiz.nl/wiki/Landingspagina_Verpleegkundige_Zorg en bestaat uit algemene cliënten context en medische gegevens (medische – en verpleegkundige context).

Omzetten van gegevens	Beschikbaar maken	Opslaan	Wettelijke bewaartermijn
Zorgmedewerkers			
Zorgaanbieder (ID, AGB, Organisatie, contactgegevens) Persoonsgegevens zorgverlener (ID, UZI/BIG/AGB), Naam, Contactgegevens, Rol	Zorgaanbieder (ID, AGB, Organisatie, contactgegevens) Persoonsgegevens zorgverlener (ID, UZI/BIG/AGB), Naam, Contactgegevens, Rol	Zorgaanbieder (ID, AGB, Organisatie, contactgegevens) Persoonsgegevens zorgverlener (ID, UZI/BIG/AGB), Naam, Contactgegevens, Rol	Gegevens: 20 jaar

2.1.3 Doel te bereiken zonder deze gegevens?

☐ Ja
☒ Nee

2.2 Rechtmatigheid (art. 6)

	Grondslagen
☒	Toestemming van de betrokken persoon
☒	Noodzakelijk voor de uitvoering van een overeenkomst
☐	Noodzakelijk voor de nakoming van een wettelijke plicht
☐	Ter bescherming van vitale belangen
☐	Vervulling van een taak van algemeen belang of uitoefening van openbaar gezag
☐	Noodzakelijk voor de behartiging van een gerechtvaardigd belang

Voor het delen van medische informatie met een andere zorgverlener, al dan niet via eOverdracht, is uitdrukkelijke toestemming nodig van de cliënt om het beroepsgeheim te mogen doorbreken. Dit kan ook veronderstelde toestemming zijn onder de volgende voorwaarden:

- De patiënt moet van tevoren goed zijn geïnformeerd over de reikwijdte van de keten en over de hulpverleners die over zijn gegevens moeten kunnen beschikken wanneer dat noodzakelijk is voor een goede behandeling of verzorging.
- Het moet gaan om concrete situaties.
- Het moet voor de patiënt duidelijk zijn dat gegevens voor zorgdoeleinden worden verstrekt.
- De patiënt heeft geen bezwaar gemaakt.
- De toestemming van de patiënt moet een vrije keuze zijn.
- Een patiënt moet zijn toestemming kunnen intrekken.
- De gegevensverstrekking blijft beperkt tot gegevens die noodzakelijk zijn voor de ontvanger.

De uitzondering op het verwerkingsverbod van bijzondere persoonsgegevens, ook voor eOverdracht, is het verlenen van zorg gebaseerd op het uitvoeren van een zorgovereenkomst. De zorgverlener moet voldoen aan de WGBO en andere wet- en regelgeving waarmee de verwerking valt onder AVG artikel 9h/i.

2.3 Beperkt tot wat noodzakelijke gegevens zijn (art. 5 lid 1 onder c)

De gegevens zijn noodzakelijk voor het verwezenlijken van het doel.

In de zibs is opgenomen welke informatie in welke situatie nodig is om te verwerken en te delen. Meer informatie dan in de zibs staat, wordt niet verwerkt en niet gedeeld. Op basis van de standaard eOverdracht en de zibs zijn de verwerkte persoonsgegevens ter zake dienend en beperkt tot wat noodzakelijk is ten behoeve van de verpleegkundige overdracht.

Bij de verpleegkundige aanmelding moet expliciete toestemming gevraagd worden om persoonsgegevens te vermelden. Standaard instelling moet zijn 'geen persoonsgegevens'. Opt-in op basis van toestemming, niet opt-out.

2.4 Beperkte bewaartermijn (art. 5 lid 1 onder e)

Medische dossiers van patiënten moeten minimaal twintig jaar bewaard worden. Die termijn gaat in op het tijdstip waarop de laatste wijziging in het dossier is aangebracht. Als de gegevens extern bij een verwerker staan opgeslagen, moet er een bewaartermijn en eventueel een exit-strategie worden afgesproken met de leverancier:

- Medische dossier: 20 jaar
- Logging: 5 jaar.

2.5 Informatieverstrekking aan betrokkenen (art. 12, 13 en 14)

Informatie over de verwerking van persoonsgegevens staat in het zorgplan of de zorgovereenkomst die met de cliënt wordt afgesloten. Wanneer er sprake is van een verpleegkundige overdracht tussen zorgorganisaties wordt de cliënt bij voorkeur schriftelijk, maar in ieder geval mondeling geïnformeerd over de informatie-uitwisseling tussen beide instanties en dit wordt vastgelegd in het bronsysteem. De cliënt kan hiertegen bezwaar maken. Meer informatie hierover is ook te vinden in <*link naar organisatie-specifieke privacy verklaring*>.

2.6 Recht van inzage en recht van overdraagbaarheid gegevens (art. 15 en 20)

Op grond van de AVG en WGBO heeft de client recht op inzage en overdraagbaarheid van de gegevens. Het doel van eOverdracht is om in gestandaardiseerde vorm elektronische overdracht van (bijzondere) persoonsgegevens van cliënten mogelijk te maken. Het recht op overdraagbaarheid van gegevens is hier niet van toepassing.

2.7 Recht op rectificatie en recht op gegevenswissing (art. 16, 17 en 19)

Het correctierecht volgt uit artikel 16 AVG. De Betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Ook kan hij onvolledige persoonsgegevens aanvullen door middel van een aan de Verwerkingsverantwoordelijke gerichte schriftelijke of elektronische verklaring/verzoek.

Het recht op vernietiging van (gegevens uit) patiëntendossiers is geregeld in artikel 455 WGBO.
1. De hulpverlener vernietigt de gegevens uit het dossier na een daartoe strekkend schriftelijk of elektronisch verzoek van de patiënt.
2. Lid 1 geldt niet voor zover het verzoek gegevens betreft waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de patiënt, alsmede voor zover het bepaalde bij of krachtens de wet zich tegen vernietiging verzet.'
Het hier bedoelde recht op vernietiging heeft betrekking op de gegevens in het patiëntendossier in de zin van artikel 454 WGBO. De gegevens in de Logging zijn niet aan te merken als onderdeel van het patiëntendossier aangezien zij geen betrekking hebben op de behandeling. Voor deze gegevens geldt het vernietigingsrecht uit de WGBO dus niet.

Voor het verwijderen van gegevens of een dossier is de verwerkingsverantwoordelijke (zorgorganisatie) primair verantwoordelijk na het verstrijken van de bewaartermijn. De zorgverlener voert de regie. De leverancier van het bronsysteem ondersteunt dit technisch.

2.8 Relatie met verwerkers (art. 28)

Zorg voor getekende Verwerkersovereenkomsten met alle betrokken leveranciers die verwerkers zijn van bronsystemen en/of brokers.

2.9 Waarborgen internationale doorgiftes (hoofdstuk V)

Internationale doorgiftes

☒ De gegevens blijven binnen de EU, de Europese Economische Regio (Noorwegen, IJsland, Liechtenstein).

☐ Cloudomgeving

Locatie server en uitwijkserver:
<Vul de locatie van zowel de server en uitwijkserver in>

Vermelding in het verwerkingsregister
In het kader van transparantie is het aan te bevelen om de verwerking van persoonsgegevens via eOverdracht te vermelden in het Verwerkingsregister van de zorginstelling.

3 Invullen door de security officer

De richtlijnen voor het opstellen van DPIA's eisen dat de risico's worden ingeschat die gepaard gaan met de verwerking die wordt beschreven. Dit dient te gebeuren voor de drie factoren van Informatiebeveiliging: Beschikbaarheid, Integriteit en Vertrouwelijkheid.

Daarbij kan het door de projectleider ingevulde plan van aanpak gebruikt worden als basis om in te schatten of er ernstige risico's aan de verwerking of het project verbonden zijn. Als uit de risico inschatting van de projectleider blijkt dat er verhoogde risico's zijn, vul dan een uitgebreide risico analyse in samen met de projectleider, of gebruik onderstaande pagina's om de risico's te beschrijven op zowel kans als impact en de te nemen maatregelen.

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten van betrokkenen. Neem daarbij de volgende stappen:

- Stel als zorgorganisatie vooraf vast wat de risicobereidheid (doelrisico) is
- Stel vast welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen
- Stel de impact (ernst) vast van deze gevolgen voor de betrokkenen
- Stel de kans (waarschijnlijkheid) vast dat deze gevolgen zullen intreden
- Implementeer en borg de noodzakelijke maatregelen om het netto risico te mitigeren zodat deze lager is dan het doelrisico (risicobereidheid)
- Leg de risico's en maatregelen vast in het Information Security Management System (ISMS).

Legenda

Kans

1. Zeldzaam: Zal gedurende enkele jaren niet gebeuren
2. Onwaarschijnlijk: Zal minimaal jaarlijks gebeuren
3. Mogelijk: Zal minimaal maandelijks (weer) gebeuren
4. Waarschijnlijk: Zal minimaal wekelijks (weer) gebeuren
5. Bijna zeker: Zal minimaal dagelijks (weer) gebeuren

Impact

1. Gering: Financieel: tot €1.000 / Geen effect op gezondheid klant / Imago: individueel
2. Klein: Financieel: €1.000 - €10.000 / Nauwelijks effect op gezondheid klant / Imago: persoonlijke kring
3. Gemiddeld: Financieel: €10.000 - €100.000 / Enig effect op gezondheid klant / Imago: plaatselijke pers/stadsblad, wijk/gemeente
4. Groot Financieel: €100.000 - €1.000.000 / Groot effect op gezondheid klant / Imago: (landelijke) pers
5. Desastreus: Financieel: > €1.000.000 / Overlijden / Imago: landelijke pers en politiek

3.1 Vertrouwelijkheid: onrechtmatige toegang

<Beschrijf de mogelijke situaties of oorzaken die de vertrouwelijkheid van de persoonsgegevens voor de onderzochte verwerking kunnen aantasten. Vul aan of wijzig waar van toepassing.>

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
Ongeautoriseerde toegang tot eOverdracht functionaliteit en cliëntinformatie binnen bronsysteem door een eigen medewerker	**Zeldzaam 1** vanwege ingerichte functie-scheiding en autorisatiematrix binnen bronsysteem Toegang tot eOverdracht functionaliteit is een aparte autorisatie, die op functie/afdelingsniveau wordt toegekend aan de afdelingen Zorgservice / Zorgadvies	**Klein 2** bij ongeautoriseerde toegang krijgt een onbevoegde medewerker mogelijk inzicht in medische gegevens en identificerende gegevens zonder dat er sprake is van een behandelrelatie. Vanwege getroffen maatregelen rond screening en geheimhoudingsplicht wordt de impact als gering ingeschat.	1. Zorg voor functiescheiding en autorisatiematrix binnen het bronsysteem. (NEN7510 H9 Toegangsbeveiliging) 2. Richt aparte autorisatie om voor eOverdracht en beperkte toekenning daarvan binnen de organisatie. (NEN7510 H9 Toegangsbeveiliging) 3. Zorg voor gescreende medewerkers die aan geheimhouding zijn gebonden. (NEN7510 H7 Veilig personeel) 4. Bewustwording medewerkers gericht op inzien dossier zonder behandelrelatie.
Ongeautoriseerde toegang tot cliëntinformatie via een middels eOverdracht aangesloten zorgorganisatie	**Zeldzaam 1** vanwege het notified pull principe van eOverdracht.	**Gering 1** Bij interne inbreuken of die tussen deelnemende organisaties wordt de impact hiervan relatief laag ingeschat, vanwege getroffen maatregelen rond	1. Het notified pull principe maakt het voor andere organisaties alleen mogelijk cliëntinformatie te benaderen indien deze actief door de verzender wordt aangeboden via het netwerk. 2. Toegang wordt gelimiteerd tot alleen data van de specifieke cliënt via het gebruik van tokens. Het token wordt ongeldig zodra de eOverdracht is voltooid. 3. Voor het 'ophalen' van een aangeboden eOverdracht vindt Twee-factor-authenticatie plaats

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
		screening en geheimhouding bij alle deelnemende partijen.	bij de ontvangende partij. (NEN7512)
Versturen van cliënt informatie via eOverdracht zonder aantoonbare toestemming van de cliënt, met name bij de aanmelding.	**Onbekend,** afstemmen met leverancier bronsysteem hoe toestemming aantoonbaar zal worden geborgd en vastgelegd in het bronsysteem	**Gemiddeld 3** mogelijk in de vorm van Aantasting van het imago, Non-compliancy t.a.v. de naleving van privacy wetgeving en financiële schade bij claim cliënt of boete Autoriteit Persoonsgegevens	1. Nader te bepalen afhankelijk van de gekozen grondslag voor de verwerking (uitvoering zorgovereenkomst / toestemming) en invulling van aantoonbaarheid. 2. Zorg voor logging in bronsysteem (NEN 7513 logging) 3. Beschrijven rollen en taken. Opstellen werkafspraken hoe de logging-gegevens onderling gedeeld en gelezen kunnen worden.
Versturen van cliënt informatie via eOverdracht naar de verkeerde zorgorganisatie (menselijke fout)	**Zeldzaam 1** er wordt procedureel gebruik gemaakt van één op één verzending tussen zorgorganisaties. De kans bestaat dat de verkeerde zorgorganisatie wordt geselecteerd, maar door het beperkte aantal deelnemende organisaties wordt die kans niet groot ingeschat,	**Gering 1** want bij een verkeerde selectie zal ook de ontvangende zorgorganisatie de aangeboden eOverdracht eerst moeten accepteren. Tijdige identificatie en correctie van fouten is daarmee waarschijnlijk, voordat informatie foutief wordt overgedragen.	1. Zorg voor een overzichtelijk klein aantal mogelijke ontvangers 2. Eén op één overdracht i.p.v. brede notificatie 3. Zorg voor een Unieke identificatie (DID) van zorgaanbieders binnen het netwerk 4. Zorg voor procedurele waarborgen in de vorm van check bij notified pull (verzendende organisatie) en acceptatie (ontvangende organisatie) 5. Training van medewerkers (controle voor verzending en acceptatie van de eOverdracht)

Met opmerkingen [Dv1]: Vraag is of dit een issue is, aangezien mijn eerdere opmerking over toestemming.

Met opmerkingen [EK2R1]: De verstrekker is verantwoordelijk voor de grondslag. Indien via een elektronische gegevensuitwisselingsysteem (zeker bij een 'pull' situatie)zal dit alleen kunnen op basis van uitdrukkelijke toestemming.

Met opmerkingen [SD3R1]: toestemming!

Met opmerkingen [SV4R1]: De Wabvpz is niet van toepassing en dus hoeft de toestemming niet expliciet vastgelegd te zijn. In dit geval gaat het dan inderdaad over het doorbreken van het beroepsgeheim onder de behandelovereenkomst.

Met opmerkingen [EK5]: Kan technisch worden afgedwongen dat bij ontbreken van toestemming dit systeem niet gebruikt kan worden? Of moeten medewerkers hiervan goed op de hoogte worden gebracht?

Met opmerkingen [SV6R5]: De Wabvpz is niet van toepassing en dus hoeft de toestemming niet expliciet vastgelegd te zijn. In dit geval gaat het dan inderdaad over het doorbreken van het beroepsgeheim onder de behandelovereenkomst.

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
Ongeautoriseerde toegang tot cliëntinformatie door een leverancier of aangesloten sub verwerker, waaronder systeembeheerders	**Zeldzaam 1**	**Gering 1**	1. Zorg ervoor dat de leverancier van de systemen beschikt over relevante certificeringen die onafhankelijk getoetste zekerheid geven over het niveau van (technische) informatiebeveiliging, waaronder NEN7510, ISO27001 en ISAE3402. 2. Zorg voor een verwerkersovereenkomst en organisatorische aansluiting van incidentenprocedures i.h.k.v. datalekken en inbreuken op vertrouwelijkheid 3. Zorg dat periodieke logging plaatsvindt over de overdracht: wie heeft op welk moment gegevens ingezien of opgehaald. (NEN7513 Logging)
Ongeautoriseerde toegang tot overdrachtsinformatie via het publieke internet (hacking)	**Zeldzaam 1**	**Desastreus 5** Medische gegevens en identificerende persoonsgegevens in handen van (kwaadwillende) onbevoegden. Voor betrokkenen morele en/of financiële schade bij misbruik, aangevuld met risico op publicatie, doorverkoop en identiteitsfraude met BSN. Voor zorgorganisaties reputatieschade en daaruit voortkomend	1. Multi-Factor Authenticatie (MFA) is verplicht bij alle deelnemende partijen voor toegang tot de dossier applicaties. Gebruik van extra authenticatie stap, zoals Yivi / ZorgID Smart wordt duidelijk vanaf 1 juli 2024. (NEN7512 Gegevensuitwisseling) 2. Zorg voor juiste versleuteling op alle verbindingen. (NEN7512 Gegevensuitwisseling) 3. Zorg dat de juiste encryptie is toegepast. eOverdracht maakt gebruik van officiële certificaten (SHA256 en RSA2018 bit) 4. Leverancier bronsysteem beschikt over relevante certificeringen die een mate van onafhankelijk getoetste zekerheid geven over het niveau van (technische) informatiebeveiliging, waaronder NEN7510, ISO27001 en ISAE3402. (NEN7510 H15 Leveranciersrelaties) 5. Bewustwording medewerkers gericht op inzien dossier zonder behandelrelatie.

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
		mogelijk financiële claims en/of boetes van de autoriteiten. Mogelijk verlies van cliënten en omzet. Indirect schade voor herstel van fouten.	
Onderschepping van cliëntinformatie tijdens transmissie tussen verzendende - en ontvangende zorgorganisatie	**Zeldzaam 1**	**Desastreus 5** idem aan bovenstaande	1. Stel een uitwisselovereenkomst op met de communicerende partijen waarin deze zekerheidsaspecten geborgd zijn. (NEN7512 Gegevensuitwisseling) 2. Zorg voor correcte en doeltreffende versleuteling (NEN7510 Cryptografie) 3. eOverdracht maakt gebruik van officiële certificaten (NEN7510 H10 Cryptografie) 4. Leverancier bronsysteem beschikt over relevante certificeringen die een mate van onafhankelijk getoetste zekerheid geven over het niveau van (technische) informatiebeveiliging, waaronder NEN7510, ISO27001 en ISAE3402. (NEN7510 H15 Leveranciersrelaties)
Zwak wachtwoordgebruik door personeel	**Zeldzaam 1**	**Gemiddeld 3**	1. Periodieke awareness campagnes en best practice overzicht voor personeel over het belang van sterke wachtwoorden (NEN7510 H7.2 Veilig personeel -- Tijdens het dienstverband 2. Multi-Factor Authenticatie (MFA) is verplicht bij alle deelnemende partijen voor toegang tot de dossier applicaties. Gebruik van extra authenticatie stap, zoals Yivi / ZorgID Smart wordt duidelijk vanaf 1 juli 2024. (NEN7512 Gegevensuitwisseling) 3. Technisch afdwingen van sterke en complexe wachtwoorden/wachtwoordbeleid.

3.2 Integriteit: ongewenste wijziging van gegevens

<Beschrijf de mogelijke situaties of oorzaken die de integriteit van de persoonsgegevens voor de onderzochte verwerking kunnen aantasten.>

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
Onjuiste of onvolledige cliëntinformatie wordt verstuurd in verpleegkundige eOverdracht als gevolg van een menselijke fout	**Zeldzaam 1** door standaardisatie en informatie direct uit de bron. Menselijke fouten kunnen echter nooit helemaal worden uitgesloten.	**Groot 4** mogelijke fouten in de vervolgbehandeling van de betrokken cliënt.	1. Maak gebruik van de zibs en sluit aan op de landelijke afspraken over gestructureerde / ongestructureerde data 2. Zorg ervoor dat de informatie rechtstreeks uit het bronsysteem komt 3. Borg in het proces dat na verzending door de ontvangende zorgorganisatie een handmatige toets plaats op ontvangen data.
Onjuiste of onvolledige cliëntinformatie in verpleegkundige eOverdracht als gevolg van technische fout in bronsysteem	**Onbekend**	**Desastreus 5** mogelijke fouten in de vervolgbehandeling van de betrokken cliënt.	1. Maak gebruik van de zibs en sluit aan op de landelijke afspraken over gestructureerde / ongestructureerde data 2. integriteitsmaatregelen in eOverdrachtsmodule bronsysteem (zoals een checksum, fail secure, etc.) 3. Borg in het proces dat na verzending door de ontvangende zorgorganisatie een handmatige toets plaats op ontvangen data.
Onjuiste of onvolledige cliëntinformatie in verpleegkundige eOverdracht als gevolg van technische fout in het NUTS netwerk.	**Gering 1** door de toepassing van diverse integriteits-maatregelen, waaronder versleutelde hashes en onafhankelijke validatie per node in het gedistribueerde netwerk	**Desastreus 5** mogelijke fouten in de vervolgbehandeling van de betrokken cliënt.	1. Zorg ervoor dat de authenticatie en autorisatie verloopt via de landelijke afspraken, waarbij de daadwerkelijke eOverdracht plaatsvindt na succesvolle authenticatie tussen de applicaties van zorgorganisaties zelf (scheiding proces en autorisatie) (NEN7512) 2. Maak gebruik van de aanwezige maatregelen in het netwerk waarmee de authenticiteit, integriteit en volledigheid van eOverdrachten (transacties) worden gevalideerd.

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
Cliëntinformatie wordt verwisseld en gekoppeld aan de verkeerde cliënt	**Zeldzaam 1**	**Gemiddeld 3** mogelijke fouten in de vervolgzorg van de betrokken cliënt.	1. Borg in het proces dat identificatie van de cliënt plaatsvindt op basis van BSN als gestructureerde zib in iedere eOverdracht 2. Na verzending vindt door ontvangende zorgorganisatie handmatige toets plaats op ontvangen data.

3.3 Beschikbaarheid van gegevens

<Beschrijf de mogelijke situaties of oorzaken die de beschikbaarheid van de persoonsgegevens voor de onderzochte verwerking kunnen aantasten.>

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
Onbeschikbaarheid van eOverdracht door technisch falen van het bron- of doelsysteem.	**Onwaar-schijnlijk 2** onbeschik-baarheid als gevolg van onderhoud (gepland) en storingen (ongepland) kunnen aan beide zijden voorkomen.	**Gering 1 (initieel)** **Op termijn 2 Klein** Bij onbeschikbaar heid van één van de twee systemen kan een eOverdracht niet plaatsvinden, waardoor cliëntinformat ie niet beschikbaar gemaakt kan worden waar nodig. Mogelijk nadelige gevolgen voor zorg van de cliënt in geval van urgentie. In de huidige fase wordt nog niet zwaar	1. Zorg voor alternatieve (analoge) procedures voor doorgang verpleegkundige overdracht. 2. Stel een SLA met de leveranciers van de systemen op met contractueel bepaalde oplostijden, Recovery Time Objective (RTO) en Recovery Point Objective 3. Zorg dat voldoende beschikbaarheids- en continuïteitsmaatregelen getroffen voor het bronsysteem, waaronder redundantie, hosting in hoog-beschikbare datacentra en doorlopende monitoring. 4. Zorg dat voldoende beschikbaarheids- en continuïteitsmaatregelen getroffen door ontvangende zorgorganisaties

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
		gesteund op eOverdracht en zijn alternatieve methoden van overdracht beschikbaar. Op termijn kan de impact groter worden wanneer alternatieve procedures zijn afgebouwd.	
Onbeschikbaarheid door technisch falen van netwerkverbinding of koppelvlak bij verzender danwel ontvanger.	**Zeldzaam 1**	**Gering 1**	1. Zorg voor redundant uitgevoerde netwerkverbindingen 2. Zorg voor automatische terugval op 4G verbindingen
Cliëntinformatie gaat verloren als gevolg van technisch falen of hacking.	**Zeldzaam 1**	**Gering 1**	1. Zorg voor een directe overdracht tussen zorgorganisaties zodat in geval van technisch falen tijdens eOverdracht de cliëntinformatie in het bronsysteem behouden blijft. (NEN7510 H9 Toegangsbeveiliging) 2. Ook in geval van hacking tijdens eOverdracht blijft de cliëntinformatie in het bronsysteem behouden. NB: Er is in dit geval wel sprake van een vertrouwelijkheidsrisico, zoals bovenstaand benoemd.
Deelnemende organisaties voldoen niet aan wettelijk geldende retentietermijnen.	**Zeldzaam 1**	**Gering 1**	1. Zorg dat de wettelijke retentietermijn voor dossierinformatie (20 jaar) wordt toegepast in de bronsystemen. 4. Deelnemende organisaties zijn ieder zelf verantwoordelijk voor het toepassen van wettelijk geldende retentietermijnen
Zorg voor volledige dossiervoering in de bronsystemen	**Waarschijn-lijk 4**	**Groot 4**	1. Borg dat alle gegevens worden opgeslagen in het bronsysteem. Als zorginformatie alleen wordt

Bedreigingen en kwetsbaarheden	Kans [1 t/m 5]	Impact [1 t/m 5]	Maatregelen om risico's aan te pakken
			opgeslagen in de broker en niet in het bronsysteem, dan zullen technische en organisatorische maatregelen en bevoegdheden van medewerkers geregeld moeten worden. (NEN7510 H17 Informatiebeveiligings-continuïteit)

3.4 Overige maatregelen

Naast de genoemde maatregelen is hieronder een checklist opgesteld om te waarborgen dat alle benodigde maatregelen effectief zijn geborgd.

Maatregel	Noodzakelijk?	Toelichting
Verwerkersovereenkomst, zie https://www.brancheorganisatieszorg.nl/nieuws_list/boz-modelverwerkersovereenkomst-vernieuwd/	☒	Benader betrokken leveranciers
SLA	☒	Benader betrokken leveranciers
Uitvoeren DPIA	☒	Benader de FG
Fysieke beveiligingsmaatregelen	☒	Onderdeel van de NEN
Beleid voor gebruik	☒	
Autorisatiematrix	☒	
Wijzigingsprocedure t.a.v. toegangsrechten	☒	Benader betrokken leveranciers
Mogelijkheid tot logging	☒	Benader betrokken leveranciers
Noodprocedure aanwezig/fallback scenario	☒	Benader betrokken leveranciers
Back up aanwezig	☒	
Training	☒	Beoordeel of gebruikers/ beheerders periodiek geschoold moeten worden
Toegangscontrole leverancier	☒	Benader betrokken leveranciers
Penetratietest	☒	Benader betrokken leveranciers of b enader de partij die deze test uitvoert
Architectuuroverzicht	☒	Benader betrokken leveranciers
Twee-factor-authenticatie	☒	Benader betrokken leveranciers
Risicoanalyse	☒	
Organisatie voldoet aan alle NEN7510, NEN7512 en NEN7513 maatregelen		

4 Betrekken van belanghebbenden

4.1 Advies Functionaris Gegevensbescherming (FG)

<Indien er een FG voor uw organisatie is ingesteld, laat deze dan zijn of haar mening over de verwerking geven. In de zorgsector is het zelfs verplicht dat de FG advies geeft. Als er geen advies van de FG wordt gevraagd, licht dan toe waarom je deze niet vraagt>

4.2 Advies betrokkenen of hun vertegenwoordigers

<Vraag betrokkenen of hun vertegenwoordiger, zoals de Ondernemingsraad, de Cliëntenraad of de Medezeggenschapsraad, om een oordeel over de verwerking. Als je dit oordeel niet vraagt, licht dan toe waarom je dat niet doet.>

5 Conclusie

5.1 Voorafgaande raadpleging AP

<Als uit deze DPIA blijkt dat er een hoog risico is als er geen maatregelen worden genomen, dan dien je vooraf de AP om raad te vragen. Leg uit waarom dit wel of niet het geval is.>

5.2 Akkoord van bestuurder

<Voorbeeld antwoord
Voor het uitvoeren van dit project / deze verwerking(en) heeft het bestuur goedkeuring gegeven. Daarbij zijn de volgende acties uitgevoerd op basis van het advies van de FG.>

5.3 Eindconclusie

De Projectleider, Privacy Officer, Security Officer, Functionaris Gegevensbescherming, Project Eigenaar hebben in samenwerking met het gehele samenwerkingsverband voor de eOverdracht geïnventariseerd welke risico's samenhangen bij het overdragen van gegevens binnen een digitale overdracht van:
<benoem hieronder de use cases die van toepassing zijn, zie opsomming hieronder>

- Uitwisseling gegevens van ziekenhuis naar thuiszorg.
- Uitwisseling gegevens van thuiszorg naar ziekenhuis.
- Uitwisseling gegevens van ziekenhuis naar verpleeghuis.
- Uitwisseling gegevens van verpleeghuis naar ziekenhuis.
- Uitwisseling gegevens van ziekenhuis naar gehandicaptenzorg.
- Uitwisseling gegevens van gehandicaptenzorg naar ziekenhuis.

Daarbij is in kaart gebracht op welke wijze deze risico's met maatregelen gemitigeerd kunnen worden. Deze maatregelen worden doorgevoerd in de voorbereidingsfase van het project en geborgd bij alle communicerende partijen in het samenwerkingsverband.

Dit is een uitgave van ICTU en V&VN

Dank aan SRVZ en AVG Compleet B.V. voor het beschikbaar stellen van de DPIA van SRVZ als inspiratie voor dit format.