Functie	Naam
Projectleider	Jochem van Hal, Arjo Rozeboom
Proceseigenaar	Annemiek Mulder, ActiZ
Privacy Officer	Erik Steijn
Inkoop	
(C)ISO	
Geconsulteerde FG's	Gerard van den Berg Claudia Benning Dim Schuurmans
Versie	1.0

DPIA uitgangspunten

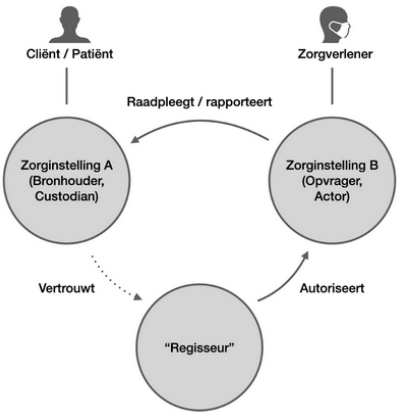
1. Deze DPIA is 'overkoepelend' bedoeld als kader voor het ANW project vanuit Actiz/NUTS. Gebruik deze informatie om in de onderlinge samenwerking en per organisatie te voldoen aan wet- en regelgeving. Voor de eigen regio uitwerking en/of organisatie zal nog een regionale of lokale DPIA opgesteld moeten worden. Om daarmee voor de eigen situatie te voldoen aan de AVG en technische inrichting en beveiliging. Mede in het kader van dit laatste punt zal ook een eigen risico matrix gevuld moeten worden, recht doend aan de situatie ter plekke.
2. Dit document behandelt de rechtmatigheid vanuit de AVG, NEN 7510, NEN 7512 en NEN 7513 normen.
3. Maak de contractuele afspraken onderling in een samenwerkingsovereenkomst/ gegevensdelingovereenkomst en eventueel de zorgovereenkomst.

A. Beschrijving kenmerken gegevensverwerkingen

1. Voorstel

Wat wil je bereiken met het proces/project? Wat is het doel? *[Geef aan welk(e) doel(en) de organisatie met de (nieuwe of gewijzigde) werkprocessen wil bereiken en/of binnen welke context deze gezien moeten worden.*
Het doel is om te komen tot een oplossing voor diverse problemen die zorgprofessionals ervaren in de avond-, nacht- en weekendzorg (ANW). De oplossingsrichting is gebaseerd op het vertrouwensmodel NUTS en bestaat uit herbruikbare, generieke componenten, gebaseerd op open standaarden. De oplossingsrichting richt zich op het zo veilig mogelijk: - inzien van alleen die cliëntinformatie die nodig is om ANW-zorg te kunnen leveren, en ook alleen maar van de cliënten waaraan zorg geleverd dient te worden; - wegschrijven van de benodigde rapportages bij de juiste cliënt in zijn/haar brondossier; - het kunnen vinden van de juiste cliënt(informatie); - het verstrekken van de juiste dossiertoegang aan de juiste medewerker, voor een bepaalde periode.

2. Hoe werkt het precies?

Beschrijf het systeem, de applicaties, de in- en output, of er acties worden gedaan zonder tussenkomst/beoordeling van de mens (maak een plaatje van het proces). *Beschrijf ook alle gegevensverwerkingen (Een verwerking is alles wat je met persoonsgegevens kunt doen: verzamelen, vastleggen, opslaan, bijwerken of wijzigen, opvragen, raadplegen, versturen, combineren, afschermen, vernietigen etc).*
Het werkt als volgt: gegevens opgeslagen bij zorginstelling A (de Custodian) moeten worden ingezien en aangevuld door medewerkers van zorginstelling B (de Actor). De "regisseur[1]" moet door zorginstelling A worden vertrouwd voor het verlenen van autorisaties. Vervolgens kan de "regisseur" autorisaties aanmaken en die delen met zorginstelling B. Deze kan met de verkregen autorisatie in de hand gegevens ophalen bij A.      Eenvoudiger gezegd: de zorgverlener krijgt op zijn eigen mobiele apparaat, via een module in het ECD van zijn eigen werkgever, inzage in de (medische) gegevens van een klant van een andere zorginstelling. Deze gegevens zijn opgeslagen in een IT-omgeving waar de zorgverlener normaal gesproken niet bij kan en worden tijdelijk gepresenteerd in het eigen ECD via het in bezit zijnde mobiele apparaat.

2.1. Wat zijn de baten voor ANW als organisatie?

Bij baten kun je denken aan vrijheid, welzijn, welvaart, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, efficiëntie en kostenreductie. (Deze brede benadering is belangrijk, omdat ethische en juridische aspecten invloed kunnen hebben op de relatie tussen onze organisatie en de omgeving)
Er zijn diverse kwalitatieve en kwantitatieve baten te vermelden door de inzet van een generieke ANW-functionaliteit, o.a.: - Minder beheerslasten: nu staan ANW-medewerkers vaak in diverse systemen bij verschillende deelnemende ANW-organisaties (HR, ECD, etc.) en wordt niet tijdig doorgegeven dat zij weer uit dienst zijn. Ook hoeven ANW-medewerkers niet voor elke applicatie aparte logins te hebben (met alle risico's vandien). - Privacyveilige oplossing: medewerkers hebben nu vaak toegang tot meer informatie/cliënten dan wenselijk. De ANW-oplossing richt zich alleen op de cliëntinformatie die nodig is om het werk te kunnen doen. - De uitgewerkte oplossing is herbruikbaar door alle leveranciers die met NUTS (willen) werken. Voor een groot deel dus sprake van: eenmalige ontwikkeling, veelvuldig (her)gebruik. En dus minder maatschappelijke kosten. - Zorgprofessionals zijn beter/gericht voorbereid op de cliënten die zij bezoeken tijdens ANW-uren: alleen die informatie die nodig is om zorg te leveren. Daarbij blijven ze digitaal werken in de hun bekende applicatie/omgeving.

2.2. Wat zijn de baten voor het individu (de cliënten)?

Ondanks dat het soms zal gaan om voor de cliënt onbekende zorgprofessionals, zijn de medewerkers zo goed mogelijk voorbereid (en weten dus wat zij moeten/komen doen bij de cliënt). Dit zal ten goede komen aan de relatie met de cliënt en de kwaliteit van zorg.

[1] Een regisseur kan zijn een medewerker, een medisch service centrum of anderszins. NUTS is geen regisseur.

Daarnaast kan, eventueel samen met de cliënt, de rapportage direct worden weggeschreven.

3. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Geef de categorieën een risicoklasse. *Denk aan medewerkers, kinderen, cliënten, bezoekers of gebruikers. Denk bij persoonsgegevens bijvoorbeeld aan naam, adres, telefoonnummer, BSN, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, kenteken, bankrekeningnummer en -saldo, functie, opleiding, inkomens-en vermogensgegevens, lidmaatschap vakbond, persoonlijke voorkeuren, loonschaal, gespreksverslagen, gegevens over de gezondheid of strafrechtelijke gegevens (Denk bij risicoklasse I aan NAW, bij II aan bijzondere persoonsgegevens zoals ras, etniciteit en gezondheid en bij III aan strafrechtelijke gegevens).*

Persoon	**Soort persoonsgegeven**	**Risicoklasse**
Cliënt	Zib patiënt	I
Cliënt	Zib contactpersoon	I
Zorgaanbieder (custodian)	Zib zorgaanbieder	II
Behandelaar	Zib behandelaar	I
Client	Zib alerts (waarschuwingen)	II
Client	Zib wilsverklaring	II
Client	Zib observation (rapportage)	II
Client	Zib woonsituatie	II
Client	Zib metingen (bloeddruk)	II
Client	Zib allergieën	II

4. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer. (Deel het proces op in verschillende stappen)
Het betreft de volgende gegevensverwerkingen: het kunnen inzien van gegevens van cliënten, het rapporteren over cliënten, het wegschrijven naar het eigen cliëntdossier en het kunnen lokaliseren van de cliënt. Daarnaast het autoriseren van de juiste medewerker door een ‘regisseur’. Medewerkers kunnen geen gegevens verwijderen die zij zelf niet hebben toegevoegd.

5. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.
Doeleinden zijn m.n. het kunnen leveren van de juiste zorg en in gang zetten van de benodigde vervolgzorg. Hiertoe dienen betrokken medewerkers inzage te krijgen in het dossier van de cliënt en rapportages toe te kunnen voegen. Dit alles wordt in gang gezet door de regisseur die de ANW-medewerker van dienst de toegang verzorgt tot de benodigde cliëntinformatie.

6. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.
In deze fase is een drietal leveranciers van ECD's betrokken, te weten: Ecare, Nedap en SDB Groep. Zij bouwen de gewenste, generieke functionaliteit/componenten zodat hun ECD's gereed zijn om de geschetste ANW-zorg te kunnen leveren. De eindgebruikers kunnen de rol van, verwerkingsverantwoordelijke, verstrekker (regisseur) en ontvanger (zorgverlener) op zich nemen. Gestart wordt met een drietal regio's en de daarin samenwerkende zorgorganisaties: **VERWERKINGSVERANTWOORDELIJKEN** Als organisatie verstrekker en de medewerkers als ontvangers van persoonsgegevens (maar niet als verwerker zoals bedoeld in de AVG). Achterhoek ● Buurtzorg ● Sensire ● Marga Klompé ● Markenheem - Nedap ● De Gouden Leeuw Groep ● Azora ● Careaz Spoedzorg Rotterdam: ● Laurens ● Aafje ● Lelie Zorggroep ● Humanitas Midden-Brabant: ● Thebe ● Mijzo ● De Wever Friesland: ● Kwadrantgroep **VERWERKERS** ● Ecare ● Nedap ● SDB Groep **NUTS** *"Dit betreft het Nuts-netwerk, dat gebruik maakt van internationale standaarden om een vertrouwenslaag op het internet te realiseren. Die standaarden zijn geïmplementeerd in de Nuts-node: Open Source software die zonder licentiekosten door elke IT leverancier gebruikt kan worden.* *Er is geen centrale Nuts-server. Bij Nuts vormen de deelnemers samen een gedistribueerd netwerk, waarbij verantwoordelijkheid voor het netwerk schaalt met het gebruik van het netwerk. Privacy-gevoelige dossiers blijven — juridisch én technisch — in de handen van zorgverleners."*[2]

[2] Een tekstgedeelte van de website nuts.nl

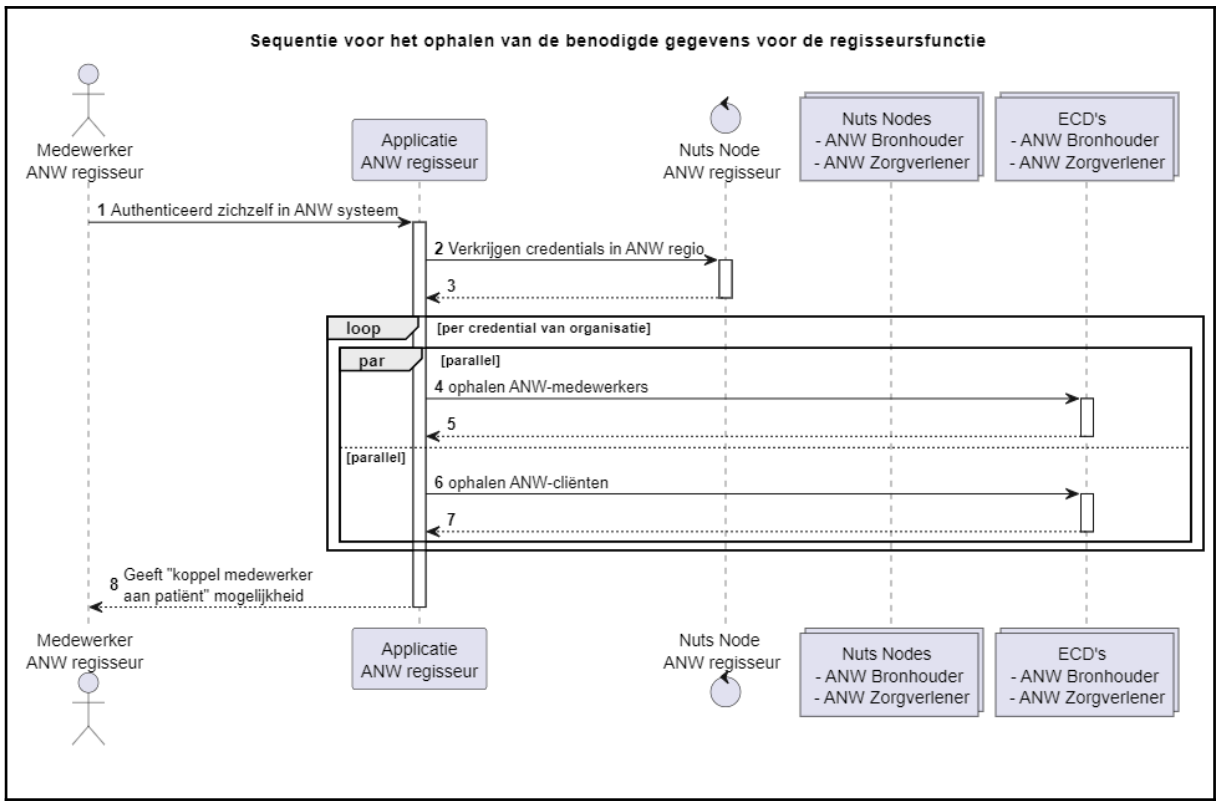
Er gaan geen persoonsgegevens over de Nuts-infrastructuur of een andere infrastructuur dan die van bovengenoemde verwerkingsverantwoordelijken en verwerkers. Nuts is daarom geen partij in de verwerking van persoonsgegevens zoals in de AVG gedefinieerd.

7. Belangen bij gegevensverwerkingen

Beschrijf alle belangen die de verwerkingsverantwoordelijken (de deelnemende (zorg)instellingen) en anderen hebben bij de voorgenomen gegevensverwerkingen.
Het belang is om op efficiënte en effectieve wijze goede zorg te verlenen, waaronder kwalitatief goede verslaglegging in het medisch dossier van de betreffende cliënt.

8. Technieken en methoden van de gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of big-data verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.
Er wordt gebruik gemaakt van de bestaande informatietechnologie (ECD's) van de verwerkingsverantwoordelijke. Deze wordt aangesloten op het vertrouwensmodel NUTS, dat voor de ANW-zorg wordt gebruikt voor o.a. authenticatie, autorisatie, identificatie, adressering/lokalisatie, logging, grondslag/toestemming. Elke deelnemende ANW-leverancier heeft een zogenaamde NUTS-node draaien, waarmee zij kenbaar maken te voldoen aan de vereiste techniek en privacy. Daarnaast kan technisch gezien alleen cliëntinformatie worden opgevraagd van cliënten die ANW-zorg ontvangen. Middels overeenkomsten tussen cliënt en zorgorganisatie wordt contractueel vastgelegd dat de cliënt (een vorm van) ANW-zorg kan krijgen/krijgt. De betrokken ECD-leveranciers bouwen elk de regisseursfunctionaliteit in hun eigen ECD in. Het schema op de volgende pagina geeft de technische werking weer. In detail is dit uitgewerkt in de notitie: "Implementatie beschrijving ANW technisch". Qua authenticatie logt elke medewerker in het ECD in middels 2FA. Zodra een ander ECD wordt bevraagd, gelden de authenticatieregels zoals nu landelijk ook voor de eOverdracht gelden: geen aanvullend authenticatiemiddel (zoals bv Yivi, want deze voldoen nog niet aan het juiste authenticatieniveau), wel kenbaar maken/bevestigen van de identiteit van de opvrager. In alle gevallen dient voldaan te worden aan de NEN 7510, NEN 7512 en NEN 7513.



9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen. *Denk aan wetten, besluiten, gedragscodes, convenanten of beroepscodes. Ook normenkaders zoals ISO/NEN.*
In dit kader geldt onder meer de volgende wet- en regelgeving: ● WGBO: vanwege zorgverlening en dossiervorming. Zowel de zorgaanbieder als de ANW-zorgverlener is gehouden aan de eisen aan de wgbo zoals het verlenen van goede zorg en dossiervorming. ● Wegiz: Deze wet is van toepassing omdat partijen zich richten op elektronische gegevensuitwisseling en daarbij er zorg voor moeten dragen (zoals Wegiz vereist) dat de juiste informatie op het juiste moment op de juiste plek is. Voor de ICT-leverancier is van belang dat taal en techniek conform de norm is. ● Wkkgz: voorschriften omtrent kwaliteit. Deze wet gaat onder meer over kwaliteit en de mogelijkheid om in dat kader (bijzondere) persoonsgegevens te delen met andere zorgverleners. ● NEN 7510: informatiebeveiliging. Deze norm is onmiskenbaar verbonden aan gegevens. ● NEN 7512: veiligheid van de uitwisseling van informatie tussen partijen. NUTS en de gegevensuitwisseling moet passen binnen de kaders van deze norm. ● NEN 7513: logging van de toegang tot het medisch dossier. Ieder elektronisch patientdossier moet de toegang tot het dossier loggen conform deze norm. Ook de toegang van een ANW-zorgverlener moet gelogd worden. ● NTA 7516: van toepassing indien in dit kader ook informatie per email of apps wordt uitgewisseld. Het zal voorkomen dat na de zorgverlening via email aanvullende informatie verstrekt of gevraagd wordt. Dan is deze norm van toepassing.

- Wabvpz: In de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg wordt het gebruik van het burgerservicenummer (BSN) en bepaalde vormen van elektronische uitwisseling van medische gegevens tussen zorgverleners geregeld.

Daarnaast gelden o.a. de beroepscodes die gelden voor iedere zorgprofessional.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.
De ANW-functionaliteit is een functionaliteit, als onderdeel van de bestaande ECD's. Dit betekent dus dat het in basis gaat over zorgprofessionals die in hun ECD werken en informatie inzien en rapporteren bij een cliënt. Er vindt dus niks aanvullends plaats dat al niet bestaat qua dossiervoering in het ECD. De bewaartermijnen zijn hiermee dus niet anders dan reeds wettelijk vastgesteld. Indien er sprake is van medische informatie, wordt de WGBO gevolgd en is er sprake van een bewaartermijn van 20 jaar (ingaand na de laatste wijziging in het zorgdossier).

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

1. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. *Kies 1 uit de volgende opties : overeenkomst, wettelijke plicht, vitaal belang, toestemming, gerechtvaardigd belang, publieke taak.*
De grondslag voor deze gegevensverwerking is AVG artikel 6 lid 1.c: de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting. Met name omdat de WGBO de zorgaanbieder verplicht een dossier te voeren van de zorgverlening en daarbij (bijzondere) persoonsgegevens moet verwerken. Daarnaast kan ook vitaal belang en het uitvoeren van een overeenkomst van toepassing zijn. Artikel 9. lid 2h is hierbij ook van toepassing.

2. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.
De AVG ziet deze persoonsgegevens als bijzondere persoonsgegevens: • persoonsgegevens waaruit iemands ras of etnische afkomst blijkt; • persoonsgegevens waaruit iemands politieke opvattingen blijken; • persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken; • persoonsgegevens waaruit het lidmaatschap van een vakbond blijkt;

- gegevens over iemands gezondheid;
- gegevens over iemands seksueel gedrag of seksuele gerichtheid;
- genetische gegevens;
- biometrische gegevens (bedoeld voor de unieke identificatie van een persoon).

Op de gezondheidsgegevens na, wordt er verder geen gebruik gemaakt van bijzondere persoonsgegevens tenzij dit noodzakelijk is voor de zorgverlening. Voor dit doel is de verwerking van bijzondere persoonsgegevens toegestaan, aangezien dit de basis is voor zorgverlening. De uitzondering om deze gegevens te mogen verwerken is vastgelegd in de AVG artikel 9 lid 2 sub h en i.

3. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. *Gebruik je de persoonsgegevens die je voor dit proces of project hebt verzameld ook nog voor iets anders? Is deze verdere verwerking dan verenigbaar is met het doel waarvoor ze zijn verzameld? Denk bijvoorbeeld aan gegevens voor de zorgovereenkomst die vervolgens worden gebruikt voor een onderzoek.*
De gegevens worden alleen voor het vooraf aangegeven doel verwerkt en niet voor andere doeleinden gebruikt.

4. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit. a) Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden? b) Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?
De voorgenomen gegevensverwerking is noodzakelijk en evenredig. Maatregelen worden getroffen zodat niet meer informatie wordt gedeeld dan strikt noodzakelijk (dataminimalisatie). De inbreuk op de privacy van betrokkene staat in verhouding tot doelrealisatie en is niet op een andere, eenvoudigere wijze te realiseren. Ook kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt.

5. Rechten van betrokkenen

Wat zijn de (mogelijk) negatieve gevolgen voor de betrokkenen *Beschrijf en beoordeel risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen.*

Iedere zorgaanbieder (custodian) is zelf verantwoordelijk voor de procedures met betrekking tot de rechten van betrokkenen inzake zorgverlening, zoals inzage, rectificatie, verwijdering en portabiliteit. Deze nieuwe functionaliteit heeft daar geen invloed op.

C. Beschrijf en beoordeel de risico's van de gegevensverwerkingen

1. Risico's[3]

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op: a) Welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen; b) De oorsprong van deze gevolgen; c) De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden; d) De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

NB: Voor de gegevensverwerking gelden grotendeels de risico's zoals die vanwege het voldoen aan de NEN 7510 t/m NEN 7513 geïnventariseerd zijn. Extra risico's ontstaan vanwege de openstelling van het ECD voor externe medewerkers.

Nr.	Risico	Oorsprong	Gevolg	Kans	Impact
1.	Cliënt informatie is niet (tijdig) zichtbaar/tot beschikking/geen toegang tot dossier	- Cliënt is mogelijk niet gekenmerkt als ANW-cliënt in het dossier - Autorisatie niet juist - Technische oorzaak ECD custodian - technische oorzaak ECD zorgverlener - Technische oorzaak NUTS	Geen toegang tot juiste informatie, betekent zorg leveren zonder deze informatie. Dat kan uiteraard altijd.	Klein	Klein
2.	Niet mogelijk om een rapportage toe te voegen	- Technische oorzaak ECD custodian - technische oorzaak ECD zorgverlener - Technische oorzaak NUTS - Autorisatie niet juist	Er kan niet in het dossier gewerkt worden, rapportage dient op papier plaats te vinden en de volgende dag in het dossier te worden gezet (waarna papier vernietigd wordt)	Klein	Klein
3.	Toegang tot verkeerde/teveel cliënt(informatie)	- Autorisatie niet juist - Foutieve cliënt selectie door regisseur	Zorglevering bij juiste cliënt altijd mogelijk. Teveel informatie zien of informatie van een cliënt zien	Klein	Matig

[3] Dit hoofdstuk bevat voorbeelden van risico's. Bij de toepassing van deze DPIA dienen de betreffende zorginstellingen zelf hun eigen afwegingen te maken, bijvoorbeeld met behulp van een eigen risicomatrix.

			waarmee geen behandelrelatie is, betekent melding maken van een datalek.		
4	Devices zijn niet geblokkeerd waardoor printscreens/ downloads van het dossier gemaakt kunnen worden.	- Niet goed ingesteld door de ICT-afdeling van de betreffende organisatie	RIsico dat ongeoorloofd printscreens worden gemaakt van dossierinformatie	Klein	Groot

Verder is door de privacy-officer van Sensire e.e.a als aandachtspunt/risico vermeld. Dit staat hieronder vermeld met daarbij een toevoeging op welke wijze hier een oplossing voor is (of niet):

Veilig en niet meer data dan nodig

- De zorgverlener mag niet meer informatie zien dan nodig is om de acute hulp te verlenen. Dit aspect geldt in de breedte (niet meer dan nodig) maar ook in de diepte (informatie van 10 jaar geleden is waarschijnlijk niet relevant voor de hulpvraag). *Reactie: er is exact vastgesteld welke informatie er nodig is voor de ANW-medewerker om zorg te kunnen leveren. Alleen voor deze informatie zal de ANW-medewerker geautoriseerd worden.*
- Medische gegevens worden via een technische oplossing beschikbaar gesteld aan een ander dan de data-eigenaar (de andere zorginstelling). Dit vraagt om goede technische maatregelen zodat de data-eigenaar blijft voldoen aan de AVG en NEN 7510, de norm voor informatiebeveiliging in de zorg. Denk hierbij aan:
  - Op het moment dat de zorgverlener de informatie niet meer nodig heeft moet alle informatie die zichtbaar is geweest in het andere ECD en op het mobiele apparaat onherstelbaar verwijderd worden. *Reactie: als er informatie wordt toegevoegd, gebeurt dit in het bronsysteem/ECD van de organisatie waar de cliënt in zorg is. Er zal nog enige tijd de mogelijkheid geboden worden om een rapportage te wijzigen, aan te vullen (4-8 uur). Daarna heeft de ANW-medewerker geen toegang meer tot het dossier van de desbetreffende cliënt en is de informatie ook alleen maar beschikbaar in het dossier van de cliënt zelf.*
  - De functionaliteit mag geen downloadfunctie hebben. *Reactie: deze inrichting wordt vooraf gecontroleerd/getest bij ICT-afdeling van de deelnemende organisaties. Tevens wordt getoetst of dit gedrag wordt voorkomen middels een gebruikersovereenkomst/gedragsregels tussen organisatie en zorgprofessional.*
  - De printscreenfunctie van het mobiele apparaat moet uitgezet zijn. *Reactie: Deze inrichting wordt vooraf gecontroleerd/getest bij ICT-afdeling van de deelnemende organisaties. Tevens wordt getoetst of dit gedrag wordt voorkomen middels een gebruikersovereenkomst/gedragsregels tussen organisatie en zorgprofessional.*
  - De medewerkers zijn bewust gemaakt van de extra gevoeligheid van het werken met klantgegevens van andere zorginstellingen. *Reactie: voorafgaand aan livegang zal hier aandacht aan worden besteed: in training en verder overeengekomen protocollen.*
  - Gegevenstransport moet veilig en versleuteld zijn. *Reactie: hiervoor geldt NUTS, dat cryptografie als belangrijk uitgangspunt heeft.*

Gebruikers, autorisaties en andere beveiligingskwesties:

De rechten (autorisaties) om gebruik te kunnen maken van deze functionaliteit krijgt de medewerker omdat hij medewerker is bij een zorginstelling en gekenmerkt is als ANW-zorgverlener.

- De zorginstellingen moeten zorgen voor een betrouwbaar doorstroom en uitstroomproces van personeel, zodat de ANW-toegang tot andere IT-omgevingen direct stopt op het moment dat de medewerker een andere functie heeft. *Reactie: dit is juist één van de redenen om een aparte ANW-toepassing te maken omdat medewerkers vaak in informatiesystemen van andere organisaties stonden (en toegang bleven houden tot systemen van andere organisaties). Nu werken medewerkers alleen nog in de applicatie van de eigen organisatie (eigen ECD). Bij uitdiensttreding vervalt ook de toegang tot het ECD en daarmee de ANW-functionaliteit.*
- Er wordt specifieke (gezamenlijk opgestelde) informatie verstrekt aan ANW-zorgverleners over hun rechten en plichten ten aanzien van de zorgaanbieders en hun cliënten, met daarin aandacht voor informatiebeveiliging en privacy. *Reactie: voorafgaand aan livegang zal hier aandacht aan worden besteed: in training en verder overeengekomen protocollen.*
- De ANW-zorgverlener is uniek gedefinieerd in alle ECD's waar hij gegevens van verwerkt. Groepsaccounts of niet-persoonsgebonden accounts zijn ***nooit*** toegestaan. *Reactie: groepsaccounts zijn nu ook al niet toegestaan. ANW-medewerkers krijgen een eigen rol/autorisatie in de applicatie.*
- De ANW-zorgverlener dient als zodanig gedefinieerd te zijn en uitsluitend in dat geval de bijbehorende rechten te krijgen in het ECD. *Reactie: ANW-medewerkers krijgen een eigen rol/autorisatie in de applicatie.*
- De (toegangs)rechten voor ANW-zorg en daarmee de toegang tot externe IT-systemen dienen met hoge(re) frequentie beoordeeld te worden. *Reactie: inregelen van een periodieke controle op actuele ANW-medewerkers en hun rol/rooster.*
- De zorginstellingen dienen ervoor te zorgen dat de medewerker zich altijd met 2 factoren heeft geauthenticeerd voordat hij gebruik kan maken van de ANW-functionaliteit. *Reactie: is reeds standaard functionaliteit van de deelnemende ECD's.*

Logging en beheersing

De toegang tot medische dossiers dient gelogd te worden.

- Het ECD dient de toegang tot gegevens van de ANW-zorgverlener te loggen conform de NEN 7513 (wie heeft wat wanneer gedaan en waarom). *Reactie: is reeds standaard functionaliteit van de deelnemende ECD's.*
- Het is daarbij noodzakelijk dat de ANW-zorgverlener eenduidig en onweerlegbaar herkenbaar is, met vermelding van contactgegevens zodat bij vragen direct contact opgenomen kan worden en niet eerst gezocht hoeft te worden naar deze gegevens. *Reactie: ANW-medewerkers zijn conform rooster ingeroosterd en hiermee direct te achterhalen (als datum en tijdstip bekend zijn).*
- Alle deelnemende zorginstellingen moeten procesafspraken met elkaar maken over de beoordeling van de logging en hoe vragen hierover onderling afgehandeld moeten worden (1 loket).
- De patiënt heeft het recht om de toegang tot zijn medische dossier in te zien, zoals vastgelegd in de NEN 7513. Ook hier moet eenduidig blijken dat er sprake is geweest van ANW-zorg door een medewerker van een andere organisatie. *Reactie: in de rapportage in het ECD is zichtbaar wie op welk moment een rapportage heeft gedaan (en of dit wel/geen ANW-medewerker is geweest).*
- Het is nuttig als het ECD een specifieke rapportage heeft ten aanzien van het gebruik n.a.v. ANW-zorg. Deze rapportage kan gebruikt worden voor controle van de toegang en eventueel ook helpen bij de financiële afhandeling.

D. Voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

1. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Nr. Risico	Maatregelen ISO	NEN norm	Restrisico
Printscreen/downloaden mogelijk van dossierinformatie	- Technisch beperken van functionaliteit device - Gebruikersovereenkomst/ gedragsregels tussen organisatie en zorgprofessional	NEN 7510	Foto maken met b.v. mobiel blijft altijd mogelijk
Risico's op onterechte toegang: teveel informatie/verkeerde cliënt	- Periodieke toetsing inrichting & autorisatie (rollen/rooster) - Aandacht in training & protocollen voor zorgprofessional hoe te handelen. - Controle van autorisaties en actualiteit betrokken ANW-medewerkers (of nog in dienst)	NEN 7510	Geen
Logging van medewerkers in detail niet duidelijk	- Inrichten logging voor inzage door ANW-medewerkers - Procesafspraken maken rondom afhandeling/toetsing logging - Opstellen aanvullende rapportages logging, specifiek voor ANW	NEN 7510 / NEN 7513	Geen, als maatregelen goed zijn ingeregeld
Clientinformatie is niet beschikbaar/rapportages zijn niet toe te voegen	- Procesafspraken maken hoe hier mee om te gaan (inclusief vernietiging rapportages op papier).	NEN 7510	Geen, als maatregelen goed zijn ingeregeld

2. Transparantie

Welke maatregelen zijn genomen om de transparantie van de toepassing te borgen?
De kern van NUTS is dat het open standaarden betreft en uit generieke bouwstenen is opgebouwd. Alle specificaties waarop de toepassing is gebouwd, zijn vrij toegankelijk via NUTS.nl. Op elk willekeurig moment kan getoetst worden door een externe partij of de toepassing conform de beschreven specificaties is gebouwd.

3. Verwerkersovereenkomst

Het volgende is vastgesteld:

- NUTS is geen partij die persoonsgegevens verwerkt.
- Iedere zorgaanbieder die zijn ECD beschikbaar stelt voor ANW-zorg is en blijft verwerkingsverantwoordelijke voor zijn eigen ECD.
- De ANW-zorgverlener, die (incidenteel) inlogt bij op een ECD van een andere zorginstellingen, noch zijn werkgever is aan te merken als verwerker zoals gedefinieerd in de AVG. Een verwerkersovereenkomst (zoals AVG dat voorschrijft) is niet nodig.

E. Advies Functionaris Gegevensbescherming

Eindoordeel Functionaris voor Gegevensbescherming
Datum: 12 juni 2024

Aanleiding voor de DPIA
Vanwege de invoering van Nuts voor ANW-zorg en het aanpassen van het ECD is het wenselijk een herbeoordeling te doen van de informatiebeveiliging via deze data protection impact assessment.

Ontwikkelingen
De verwerking van persoonsgegevens door de verwerkingsverantwoordelijken en verwerkers vindt al plaats. Ook vindt er al ANW-zorg plaats. Het gebruik van Nuts is een aanvulling hierop.
Met deze DPIA is vastgesteld of risico's toenemen of dat er nieuwe risico's ontstaan. Daarnaast is met deze DPIA vastgesteld of bepaalde beheersmaatregelen aangescherpt moeten worden.

Rechtmatigheid (grondslag en doelbinding)
De rechtmatigheid van de verwerking is voldoende onderbouwd in onderdeel B.
Vastgesteld is dat Nuts geen inzage krijgt in persoonsgegevens en daarom geen partij is voor wat betreft de verwerking van persoonsgegevens. In essentie verandert er weinig: De custodian (verwerkingsverantwoordelijke) heeft de rechtmatigheid al bepaald. Externe ANW zorgmedewerkers kregen al toegang tot het ECD, alleen vindt deze toegang nu op een andere wijze plaats. Het gebruik van Nuts valt binnen de rechtmatigheidseisen.

Risico's

- Met deze gewijzigde verwerking is er een toename van de afhankelijkheid van informatiesystemen met als gevolg toename risico's ten aanzien van beschikbaarheid. Namelijk: In de oude situatie werkte de zorgverlener in de ECD van de custodian. In de nieuwe situatie werkt de zorgverlener met zijn eigen ECD, Nuts-onderdelen en het ECD van de custodian (en de diverse interfaces). De kans op verstoringen is niet groot, maar het is

wenselijk om goede afspraken te maken over het opzoeken van verstoringen (inspanningsverplichting bij de IT-aanbieders).

- Net als in de situatie zonder gebruik van Nuts is er een risico van vertrouwelijkheid: kunnen alleen de hiervoor aangewezen zorgverleners die gegevens zien die nodig zijn voor de ANW-zorg van alleen die cliënt(en)? Met het gebruik van Nuts worden bepaalde risico's verlaagd. Bijvoorbeeld omdat het door- en uitstroomproces van de werkgever bepalend wordt voor de toegang tot het ECD van de custodian. De custodian(s) geven hiervoor vertrouwen aan de zorgaanbieders, maar blijven net als nu verantwoordelijk. Dat vraagt om transparantie en duidelijkheid in wat men over en weer van elkaar verwacht.

Maatregelen
De basis is dat alle zorgaanbieders, zowel custodians als zorgaanbieders die personeel leveren voor ANW-zorg, allen moeten voldoen aan de eerder genoemde wet- en regelgeving. In dit geval met name de NEN 7510. Dit wordt nu iets complexer omdat er vertrouwd wordt op maatregelen van andere zorgaanbieders. Bijvoorbeeld:

- De autorisatie om toegang te krijgen tot de cliënten van custodian (en om deze weer in te trekken) worden bepaald door het HR-proces bij de zorgaanbieder.
- Dit geldt ook voor de instructies/gedragsregels voor zorgverleners en bewustzijn op het gebied van privacy en informatiebeveiliging.
- Andersom moet de zorgaanbieder ook vertrouwen dat er zorgvuldig wordt omgegaan met de gegevens van de medewerker die hij inzet voor ANW-zorg.
- Bij de custodian kunnen bij controle van gebruikers en de toegang tot medische dossiers vragen ontstaan. Deze vragen moet hij ergens in kunnen dienen en de zorgaanbieder moet de verplichting hebben daarop te reageren.

Bij het ontwerp en de ontwikkeling van de extra module is al rekening gehouden met de nodige technische maatregelen zoals autorisaties en MFA. Het juiste gebruik ervan ligt bij de zorgaanbieders.

ADVIES
Naast de technische maatregelen die met Nuts worden geïmplementeerd adviseren de betrokken FG's dat de samenwerkingspartners de verwachting en verplichtingen op het gebied van informatiebeveiliging en privacy duidelijk en transparant opnemen in een samenwerkingsovereenkomst/zorgovereenkomst. Hiermee wordt duidelijk wat de randvoorwaarden en verplichtingen zijn voor de samenwerkingspartners om ANW-zorg op veilige wijze mogelijk te maken.

Hierin worden een aantal afspraken gemaakt worden zoals hieronder benoemd[4]:

Samenwerkingspartners verklaren over en weer:

- Te voldoen aan wet- en regelgeving.
- Geheimhouding over (vertrouwelijke) cliënt-, medewerker- en bedrijfsgegevens.
- Persoonsgegevens in het ECD uitsluitend te gebruiken voor het doel waarvoor deze verwerkt en verstrekt worden. Dit geldt zowel voor custodian (m.b.t. zorgverlener gegevens) als de zorgverlener (m.b.t. alle beschikbare gegevens in het ECD).
- Het eigen door- en uitstroomproces op orde te hebben zodat gewaarborgd is dat uitsluitend geautoriseerde medewerkers toegang krijgen tot het ECD van de andere partij.

[4] Niet limitatief en bewust beknopt geformuleerd

- Dat de eigen IT-infrastructuur uitsluitend via multifactor authenticatie toegankelijk is, zodat gewaarborgd is dat de medewerker die toegang krijgt tot het ECD van de samenwerkingspartner geauthenticeerd is met tenminste twee factoren.
- De rechten van medewerkers voor ANW-zorg periodiek worden beoordeeld, maar tenminste twee keer per jaar.
- Er uitsluitend gebruik wordt gemaakt van persoonsgebonden gebruikersaccount zodat medewerkers herkenbaar zijn en verantwoordelijk kunnen worden gehouden voor hun handelen.
- Dat risico's en omissies in informatiebeveiliging(sprocessen) adequaat worden opgepakt.
- Medewerkers periodiek worden ingelicht over de geldende afspraken voor ANW-zorg, ook op het gebied van informatiebeveiliging en privacy.
- Zonder onnodige vertraging te reageren op vragen over activiteiten van medewerkers in het ECD van de zorgaanbieder (custodian), bijvoorbeeld als de controle van de logging van de toegang tot medische dossiers daar aanleiding toe geeft.
- Een datalek te melden aan de ander indien dat relevant is. Bijvoorbeeld omdat de naam en gelogde gegevens van de medewerker van zorgaanbieder onderdeel uitmaakt van het datalek. Ook het onverwacht voor langere tijd niet beschikbaar zijn van Nuts valt ook onder een datalek omdat dit invloed kan hebben op de zorg voor de cliënt.
- Elkaar te ondersteunen in het oplossen van verstoringen in de IT-infrastructuur.

Met genoemde technische en organisatorische maatregelen, met daarbij een adequate risicoafweging die iedere zorginstelling zelf moet doen voor haar situatie en eventuele aanvullende maatregelen, komen de betrokken FG's tot de conclusie dat deze verwerking van persoonsgegeven doorgang kan vinden.

Startdatum verwerkingen (indien van toepassing)	Wanneer bijwerken register (indien van toepassing)	Datum herziening DPIA (indien van toepassing)
nvt	nvt	nvt