Data protection impact assessment Stichting Dataplatform Midden-Holland

Data protection impact assessment van de Stichting Dataplatform Midden-Holland ten behoeve van het programma Gedeelde Zorg.

30-04-2021

Versie 21

Auteurs: Bas Rekveldt, Frank Roose

Versiebeheer

Versie	Datum	Status	Auteur	Opmerkingen
01	2019-05-03	Concept	Bas Rekveldt	Opstellen initiële versie.
03	2019-09-09	Concept	Bas Rekveldt	Opmerkingen ZorgTTP toegevoegd.
07	2019-11-30	Concept	Frank Roose	Opmerkingen ZorgTTP verwerkt.
10	2019-12-05	Concept	Frank Roose	Heropbouw document a.h.v. NOREA-risicogebieden.
14	2020-01-21	Concept	Frank Roose	Opmerkingen Nysingh advocaten verwerkt.
16	2020-01-22	Concept	Frank Roose	Definitief concept aangeboden aan stuurgroep.
17	2020-03-17	Concept	Frank Roose	Opmerkingen stuurgroep januari verwerkt.
18	2020-07-07	Concept	Bas Rekveldt	Opmerkingen juristen uit stuurgroep 1 mei verwerkt.
20	2020-10-01	Concept	Bas Rekveldt	Aanpassing i.v.m. cloud infrastructuur
21	2021-04-30	Def	Nysingh	

Copyright

Vertrouwelijkheid

Deze uitgave bevat vertrouwelijke informatie en dient als dusdanig te worden behandeld door de ontvanger.

Inhoudsopgave

1. Organisatie en geraadpleegde experts

Naam, adres van organisatie:
Stichting Dataplatform Midden-Holland IO (Hierna: de Stichting)
Bleulandweg 10
2803 HH Gouda

Opsteller DPIA:
Scamander Solutions BV (Hierna: „**Scamander**")
Bas Rekveldt Consultant
bas.rekveldt@scamander.com

Naam en contactgegevens Functionaris Gegevensbescherming:
<nog in te vullen>

Overige betrokkenen en geraadpleegde experts:

Bart Smit	*Programma Manager Gedeelde Zorg*
Olivier Jacobs	*Commercieel manager van het Groene Hart Ziekenhuis (hierna: GHZ)*
Jean Coenen	*Security en Privacy Consultant van Iscer B.V.*
Gert Jan Kentie	*Directeur van Scamander*
Frank Roose	*Project manager Scamander*
Lindsey Baur	*Adviseur bij ZorgTTP*
Rutger Ketting	*Advocaat Privacy en ICT Nysingh advocaten-notarissen*
Elisabeth Paarlberg	*Jurist bij Zorgpartners Midden-Holland*
Inez Cohen	*Senior bedrijfsjurist bij Vierstroom Zorg Thuis B.V.*
Sandra Grapendaal	*Functionaris gegevensbescherming bij Vierstroom Zorg Thuis B.V.*
Ester Vink	*Senior beleidsmedewerker bij de gemeente Gouda*
Maurice Reedijk	*Functionaris gegevensbescherming bij de gemeente Gouda*
Winke Uytdehaage	*Functionaris gegevensbescherming en senior bedrijfsjurist bij GHZ*

2. Inleiding

Diverse samenwerkende zorgaanbieders in Midden-Holland hebben als gezamenlijke missie om voor de inwoners in de regio een duurzame inrichting van zorg en welzijn te bereiken, gericht op herstel en participatie (gezondheid in de breedste zin van het woord). Om de missie te bereiken is innovatie en samenwerking nodig. Deze innovatie zal vormgegeven worden door middel van een statistisch onderzoek, zoals deze beschreven is in het Onderzoeksprotocol 'Gedeelde Zorg' (hierna: "**Onderzoeksprotocol**"). Hierin werken de deelnemende partijen samen en wisselen gegevens uit ten behoeve van dit onderzoek. Resultaten van dit onderzoek zullen leiden tot nieuwe inzichten en stelt de besturen van de samenwerkende partijen in staat om data gedreven besluiten te nemen.

Voor het onderzoek worden gegevens gebruikt van individuen. Zelfs in gepseudonimiseerde vorm betreffen dit persoonsgegevens en daarom is de Algemene verordening gegevensbescherming (hierna: "**AVG**") van toepassing. Het gaat daarbij onder meer om gezondheidsgegevens van alle inwoners in de regio Midden-Holland. Volgens de Autoriteit Persoonsgegevens (hierna: "**AP**") dient er – aangezien er sprake is van grootschalige elektronische uitwisseling van gezondheidsgegevens - een data protection impact assessment (hierna: "**DPIA**") te worden uitgevoerd voordat met de verwerking wordt begonnen.

3. DPIA

Dit document is opgesteld naar aanleiding van de voorgenomen gegevensverwerkingen binnen het project Big Data, dat onderdeel is van het programma 'Gedeelde Zorg'. In deze DPIA worden de technische, organisatorische en juridische inrichting van het project getoetst aan de gestelde eisen van de AVG.

De definitie van een DPIA volgens de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking 'waarschijnlijk een hoog risico inhoudt' in de zin van Verordening 2016/679 (WP 248) van de voormalige Working Party 29 (hierna: "**WP 29**") is als volgt: "*Een gegevensbeschermingseffectbeoordeling is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken. [...] Met andere woorden: een gegevensbeschermingseffectbeoordeling is een proces voor het verwezenlijken en aantonen van naleving.*"[1] De WP29 is inmiddels opgevolgd door de European Data Protection Board (hierna: "**EDPB**"). Zij onderschrijven de richtsnoeren van WP 248.[2]

In artikel 35 van de AVG wordt de DPIA benoemd en de minimumeisen die hieraan worden gesteld worden in lid 7 toegelicht.[3] Deze minimumeisen bestaan uit:

- Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
- Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- Een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en
- De beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

Deze DPIA gaat in op de genoemde minimumeisen. Daarnaast is deze DPIA gebaseerd op de beginselen en privacy principes in de AVG en de hoofdstukken van deze DPIA zijn ingedeeld op basis van de methodische handreiking uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland.[4]

Alvorens de risico's van de verwerkingen en de getroffen maatregelen worden gedefinieerd, worden eerst de technische en organisatorische inrichting van dit project besproken. Aan de hand van deze onderbouwing vindt vervolgens de juridische onderbouwing plaats. In het laatste hoofdstuk komt de rol van de functionarissen voor gegevensbescherming (hierna: "**FG's**") aan de orde.

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf
[2] https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf, pagina 1, onder '6.'.
[3] http://www.privacy-regulation.eu/nl/artikel-35-gegevensbeschermingseffectbeoordeling-EU-AVG.htm
[4] https://www.norea.nl/download/?id=522

4. NOREA-risicogebieden

Op basis van een overzicht van de risicogebieden waar de privacy van de betrokkene mogelijk wordt geschaad kan er een inschatting worden gemaakt hoe groot de impact is binnen het project en op de deelnemende partijen. Vervolgens kunnen maatregelen genomen worden om de risico's te verkleinen.[5] De risicogebieden zijn als volgt:

- Risicogebieden die samenhangen met de omgeving waarin u opereert:
  1. Het type project.
  2. De partijen die betrokken zijn bij de uitvoering van het project.
  3. De gegevens die u wilt gebruiken.
- Risicogebieden die samenhangen met een bepaalde fase van de verwerking:
  4. Het verzamelen van de gegevens.
  5. Het gebruik van de gegevens.
  6. Het bewaren en vernietigen van de gegevens.
  7. De beveiliging van de gegevens.

Deze risicogebieden komen in het volgende in bovenstaande volgorde aan bod.

4.1. Type project

In deze paragraaf wordt een inleiding gegeven in de gedeelde missie van de deelnemende partijen, zoals beschreven in het Visiedocument van het programma Gedeelde Zorg in Midden-Holland (**bijlage B**).[6] Om de idealen in dit programma te bereiken is vanuit dit programma het project Big Data gestart, waarbij de missie wordt gerealiseerd met het uitvoeren van een statistisch onderzoek. Dit onderzoek staat beschreven in het Onderzoeksprotocol (**bijlage E**).

4.2. Betrokken partijen en juridische inrichting

De betrokken partijen in dit project zijn te verdelen in verwerkingsverantwoordelijken, betrokkenen, verwerkers en subverwerkers zoals bedoeld in de AVG.[7]

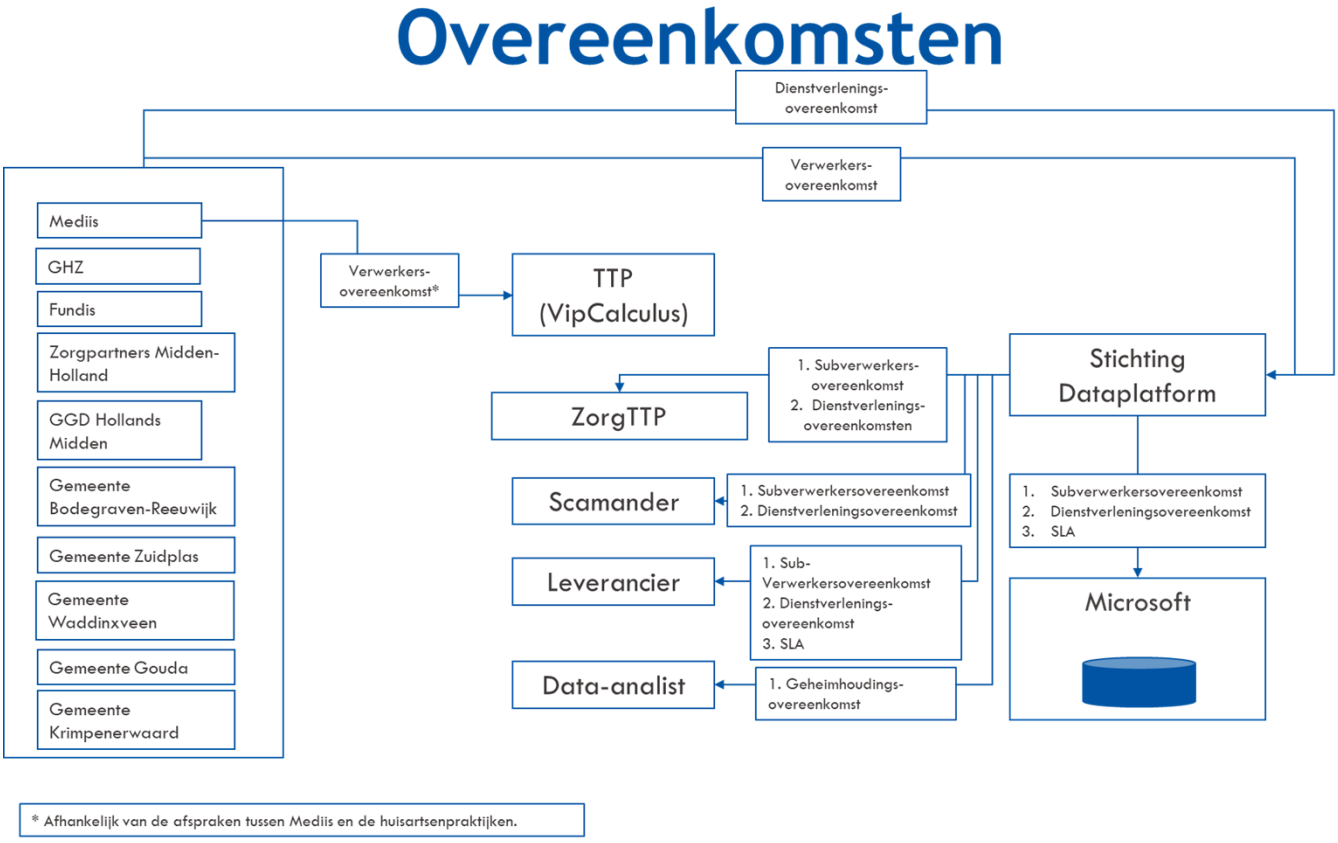
Binnen het programma Gedeelde Zorg[8] werken diverse zorgaanbieders en gemeenten van regio Midden-Holland samen en deze partijen bepalen gezamenlijk het doel en de middelen en zijn daarom gezamenlijke verwerkingsverantwoordelijken. Hieronder volgt een lijst van de verwerkingsverantwoordelijken. De databronnen van deze partijen zijn hieronder opgesomd met daarachter het type partij:

- Het Groene Hart Ziekenhuis (ziekenhuis, hierna: het "**GHZ**")
- Mediis (huisartsen)
- Zorgpartners Midden-Holland (verpleging, verzorging en thuiszorg, hierna: "**VVT**")
- Vierstroom Zorg Thuis B.V. (VVT)
- Gemeente Bodegraven-Reeuwijk (gemeente)
- Gemeente Gouda (gemeente)
- Gemeente Krimpenerwaard (gemeente)
- Gemeente Waddinxveen (gemeente)
- Gemeente Zuidplas (gemeente)

Hieronder een schematisch overzicht van de juridische samenwerkingsstructuur en de overeenkomsten die gesloten worden tussen de deelnemende partijen.

---

[5] https://www.norea.nl/download/?id=522, 15
[6] Def Visiedocument GZMH anoniem.pdf
[7] Subverwerker betekent "andere verwerker" zoals bedoeld in artikel 28 lid 2 AVG
[8] Def Visiedocument GZMH anoniem.pdf



Figuur 1. Overeenkomsten Dataplatform

De verwerkingsverantwoordelijken tekenen gezamenlijk één dienstverleningsovereenkomst met de Stichting Dataplatform Midden-Holland (hierna: de "**Stichting**"). Deze stichting wordt opgericht om de infrastructuur te beheren die noodzakelijk is voor het dataplatform. De Stichting krijgt van de verwerkingsverantwoordelijken bovendien de opdracht om het statistische onderzoek uit te voeren ten behoeve van de verwerkingsverantwoordelijken. De afspraken tussen de verwerkingsverantwoordelijken en de Stichting worden vastgelegd in een dienstverleningsovereenkomst.

De verwerkingsverantwoordelijken besteden gezamenlijk het dataplatform en de verwerking (inrichting, bouw, beheer en analyses op dataplatform) uit aan de Stichting. Daarmee wordt de Stichting een verwerker. De taken van de Stichting inzake deze verwerking worden vastgelegd in een verwerkersovereenkomst tussen de verwerkingsverantwoordelijken en de Stichting.

Voor ondersteuning bij de inrichting, de bouw, het beheer en de analyse van het dataplatform door de Stichting en gedurende het onderzoek worden de diensten van de leverancier Scamander ingehuurd. In dat kader wordt er tussen de Stichting en Scamander een dienstverleningsovereenkomst gesloten. Daarbij treedt Scamander op als subverwerker, aangezien zij in opdracht van de Stichting gegevens verwerkt. In dat kader wordt er een subverwerkersovereenkomst gesloten tussen de Stichting en Scamander.

Voor het onderhoud, beheer en beschikbaar stellen van de hardware infrastructuur is een dienstverleningsovereenkomst afgesloten met Microsoft. Daarin is ook de SLA van Microsoft opgenomen. Het Azure platform van Microsoft is ISO 27001, ISO 27018 en ISO 27701

gecertificeerd. Microsoft treedt hierbij op als subverwerker, aangezien zij in opdracht van de Stichting gegevens verwerkt. In dat kader wordt er een subverwerkersovereenkomst gesloten tussen de Stichting en Microsoft.

Voor het onderhoud, beheer en beschikbaar stellen van de software infrastructuur is een dienstverleningsovereenkomst, met daarbij een Service Level Agreement (SLA) afgesloten tussen de Stichting en Microsoft. Hierin zijn afspraken vastgelegd om de continuïteit, kwaliteit, operationele efficiëntie en veiligheid van de infrastructuur te waarborgen. Omdat hier Microsoft als subverwerker optreedt in opdracht van de Stichting, wordt er ook een subverwerkersovereenkomst getekend om de verantwoordelijkheden over de veiligheid van de gegevens vast te leggen.

Voor het pseudonimiseren, versturen en ontvangen maakt de Stichting gebruik van de diensten en software van een TTP. In dat kader wordt er tussen de Stichting en de TTP een dienstverleningsovereenkomst gesloten. In deze rol is de TTP een subverwerker. De Stichting sluit in dat kader een subverwerkersovereenkomst af met de TTP.

Voor het verzamelen en ontsluiten van de gegevens van de huisartsen maakt Mediis gebruik van de diensten van VipCalculus. Er bestaat al een verwerkersovereenkomst tussen de huisartsen van Mediis en VipCalculus, maar deze moet uitgebreid worden ter ondersteuning van dit onderzoek om het aanleveren van de gegevens aan de Stichting te faciliteren.

Voor het verrichten van het onderzoek zoals beschreven in het Onderzoeksprotocol zal een analist van het GHZ gedetacheerd worden bij de Stichting. In dat kader wordt een detacheringsovereenkomst gesloten tussen de Stichting, het GHZ en de analist van het GHZ. Voor zijn werkzaamheden namens de Stichting zal deze analist een geheimhoudingsovereenkomst sluiten met de Stichting.

De betrokkenen zijn de inwoners van Midden-Holland van 19 jaar en ouder, ongeveer 300.000 mensen. De rechten van de betrokkenen worden verder besproken in paragraaf **Error! Reference source not found.**.

4.3. Gegevens die worden gebruikt

In deze paragraaf volgt een beschrijving van de gegevens die noodzakelijk zijn voor het statistische onderzoek zoals beschreven in het Onderzoeksprotocol.

4.3.1. Alle deelnemende partijen

Voor het onderzoek zijn enkele kenmerken van een persoon nodig om de koppeling tussen de gegevens van de verschillende deelnemende partijen te faciliteren en ook als achtergrondkenmerken om verschillen te kunnen duiden tijdens het onderzoek. In de onderstaande tabel is een overzicht opgenomen van de gegevens die van alle deelnemende partijen minimaal nodig zijn.

Kolom	Omschrijving
Persoon_ID	Nummer waarmee de persoon tussen de verschillende tabellen gekoppeld kan worden. Deze wordt door de TTP bepaald op basis van een combinatie van geboortenaam, voorletters, geboortedatum en geslacht. Dit zal telkens op dezelfde wijze gebeuren.
Buurtcode	CBS-buurtcode volgens de indeling van 2019.
Geboortejaar	Omdat de zorg in verschillende jaren geleverd wordt is het beter om een geboortejaar dan de leeftijd te hebben, zodat de leeftijd op het moment

	van zorg berekend kan worden.
Overlijdensjaar	Om rekening te kunnen houden met eventueel overlijden van personen, ook het jaar van overlijden als gegeven.
Geslacht	Man, vrouw of onbekend.
Huishouden	Alleenstaand, samenwonend zonder kinderen, samenwonend met kinderen, instelling of onbekend.

Tabel 1. Overzicht van de te gebruiken persoonsgegevens.

Elk van de deelnemende partijen zal deze gegevens aanleveren omdat niet elke partij dezelfde personen bedient en er wel een volledig overzicht nodig is. In het geval dat meerdere deelnemende partijen gegevens over dezelfde persoon aanleveren, worden die gegevens voor de betreffende persoon gebruikt op basis van herkomst van de gegevens. Hierbij wordt de voorkeur gegeven aan de gegevens die de gemeente aanlevert, daarna die van de huisarts, vervolgens de VVT en het ziekenhuis. Deze volgorde is gebaseerd op de verwachte actualiteit van de gegevens.

4.3.2. Huisartsen

Van de huisartsen zijn gegevens over de consultenten nodig voor het onderzoek. Specifiek gaat het dan om de gegevens in onderstaande tabel. Deze gegevens zullen alleen aangeleverd worden door de huisartsen.

Kolom	Omschrijving
Persoon_ID	Nummer waarmee de persoon tussen de verschillende tabellen gekoppeld kan worden. Deze wordt door de TTP bepaald op basis van een combinatie van geboortenaam, voorletters, geboortedatum en geslacht. Dit zal telkens op dezelfde wijze gebeuren.
Startdatum	Datum waarop het consult begint.
Einddatum	Datum waarop het consult eindigt (indien van toepassing).
SoortZorg	Indien beschikbaar ICPC-code en omschrijving voor het consult.
Kosten	Gemaakte of verwachte kosten gedurende de hele periode (startdatum t/m einddatum) voor het consult.

Tabel 2. Overzicht van de te gebruiken gegevens uit de data van huisartsen.

4.3.3. Verzorgings- en verpleeghuizen en thuiszorgorganisaties

Voor het onderzoek zijn gegevens over de geleverde extra- en intramurale zorg nodig die via de Zorgverzekeringswet (Zvw) en de Wet langdurige zorg (Wlz) gefinancierd worden. In onderstaande tabel is een overzicht opgenomen van deze gegevens. Deze gegevens zullen aangeleverd worden door de VVT-organisaties.

Kolom	Omschrijving
Persoon_ID	Nummer waarmee de persoon tussen de verschillende tabellen gekoppeld kan worden. Deze wordt door de TTP bepaald op basis van een combinatie van geboortenaam, voorletters, geboortedatum en geslacht. Dit zal telkens op dezelfde wijze gebeuren.
Startdatum	Datum waarop de zorg/indicatie begint.
Einddatum	Datum waarop de zorg/indicatie eindigt (indien van toepassing).
Financiering	Zorg in Natura of PGB (indien bekend).

Kolom	Omschrijving
SoortZorg	Type zorg die geleverd wordt gedurende de periode. Extramuraal op categorie niveau (Persoonlijke Verzorging, Verpleging, Begeleiding, Dagbesteding). Intramuraal op zorgzwaartepakket niveau (VV 1-10, GGZ B/C 1-7, VG 1-8, LG 1-7, ZG 1-4, LVG)
Hoeveelheid	In het geval van extramurale zorg een gemiddeld aantal uren per week. Voor intramurale zorg het aantal dagen per week.
Kosten	Gemaakte of verwachte kosten gedurende de hele periode (startdatum t/m einddatum) voor de zorg.

Tabel 3. Overzicht van de te gebruiken gegevens uit de data van de VVT.

4.3.4. Gemeenten

Voor het onderzoek zijn gegevens nodig over de zorg die via de Wet maatschappelijke ondersteuning (Wmo) is geleverd aan inwoners in de regio. In onderstaande tabel is een overzicht opgenomen van deze gegevens. Deze gegevens worden door de deelnemende gemeenten aangeleverd.

Kolom	Omschrijving
Persoon_ID	Nummer waarmee de persoon tussen de verschillende tabellen gekoppeld kan worden. Deze wordt door de TTP bepaald op basis van een combinatie van geboortenaam, voorletters, geboortedatum en geslacht. Dit zal telkens op dezelfde wijze gebeuren.
Startdatum	Datum waarop de zorg/indicatie begint.
Einddatum	Datum waarop de zorg/indicatie eindigt (indien van toepassing).
Financiering	Zorg in Natura of PGB (indien bekend).
SoortZorg	Type voorziening of hulpmiddel in categorieën (Begeleiding, Beschermd wonen, Dagbesteding, Hulp bij het huishouden, Kortdurend verblijf, Opvang, Persoonlijke verzorging, Rolstoelen, Spoedopvang, Vervoerdiensten, Vervoervoorzieningen, Woondiensten, Woonvoorzieningen).
Hoeveelheid	Het gemiddeld aantal uren per week of anders het aantal voorzieningen/hulpmiddelen van het type.
Kosten	Gemaakte of verwachte kosten gedurende de hele periode (startdatum t/m einddatum) voor de zorg.

Tabel 4. Overzicht van de te gebruiken gegevens uit de data van de gemeenten.

4.3.5. Ziekenhuis

Vanuit het ziekenhuis zijn gegevens voor het onderzoek nodig over de verrichtingen en opnametrajecten van patiënten bij het ziekenhuis. In onderstaande tabel is een overzicht opgenomen van deze gegevens. Deze gegevens worden aangeleverd door het ziekenhuis.

Kolom	Omschrijving
Persoon_ID	Nummer waarmee de persoon tussen de verschillende tabellen gekoppeld kan worden. Deze wordt door de TTP bepaald op basis van een combinatie van geboortenaam, voorletters, geboortedatum en geslacht. Dit zal telkens op dezelfde wijze gebeuren.
Startdatum	Datum waarop het traject begint.
Einddatum	Datum waarop het traject eindigt (indien van toepassing).
Diagnose	Gestelde diagnose in het traject (code/omschrijving).
Specialisme	Specialisme binnen het ziekenhuis die de zorg levert.
SoortZorg	ICDC code/omschrijving.
Kosten	Gemaakte of verwachte kosten gedurende de hele periode (startdatum t/m einddatum) voor de zorg.

Tabel 5. Overzicht van de te gebruiken gegevens uit de data van het ziekenhuis.

4.3.6. Dienstverleningsovereenkomst

Afspraken over de exacte opbouw van de aan te leveren bestanden en onderliggende selecties worden vastgelegd in de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting. Daarnaast wordt hierin vastgelegd wie de contactpersoon is in het geval er een incident is met het aanleveren van de gegevens.

4.4. Voorwaarden voor het gebruik van de gegevens

In deze paragraaf wordt de rechtmatigheid van het gebruik van de gegevens beschreven. Daarnaast wordt een beschrijving gegeven van hoe de informatievoorziening richting de betrokkenen wordt gefaciliteerd en de wijze waarop er wordt voorzien in de uitoefening van de rechten van betrokkenen.

4.4.1. Rechtmatigheid

De verwerking van persoonsgegevens in het kader van dit project betreft een verdere verwerking in de zin van artikel 6 lid 4 AVG. Het betreft namelijk een verwerking voor een ander doeleinde dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. De deelnemende partijen (zorgaanbieders en gemeenten) verwerkten de betreffende persoonsgegevens immers al en hadden daarvoor een eigen verwerkingsgrondslag zoals bedoeld in artikel 6 lid 1 AVG.

Indien een verdere verwerking niet berust op toestemming van de betrokkene of een wettelijke bepaling, dan dient beoordeeld te worden of er sprake is van een toegestane verdere verwerking. Die beoordeling hoeft dus niet gemaakt te worden indien er om toestemming aan de betrokkene wordt gevraagd voor de verdere verwerking. Dat is voor twee van de deelnemende partijen het geval. Ten aanzien van Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. berust de verdere verwerking namelijk op toestemming van de betrokkene (zie hierna).

Indien er sprake is van een toegestane verdere verwerking is er geen afzonderlijke verwerkingsgrond vereist dan die op grond waarvan de verzameling van persoonsgegevens werd toegestaan.

Op grond van artikel 6 lid 4 AVG is een verdere verwerking toegestaan indien het doel van de verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld. Uit overweging 50 van de AVG volgt dat de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of

statistische doeleinden, als een met de aanvankelijke doeleinden verenigbare rechtmatige verwerking moet worden beschouwd. De verwerking van persoonsgegevens in het kader van dit project vindt plaats met het oog op statistisch onderzoek en dus is er sprake van een toegestane verdere verwerking.

Het verwerken van bijzondere categorieën van persoonsgegevens, waaronder medische gegevens, is op grond van artikel 9 lid 1 AVG verboden, tenzij er een beroep kan worden gedaan op één van de in artikel 9 lid 2 AVG genoemde uitzonderingsgronden. Voor dit project kan er ten aanzien van alle deelnemende partijen met uitzondering van Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. (zie hierna) een beroep worden gedaan op de uitzonderingsgrond genoemd in artikel 9 lid 2 onder j AVG: de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Meer specifiek; ook hier gaat het om statistisch onderzoek.

Voor de deelnemende zorg verlenende partijen betekent dit dat zij moeten voldoen aan de voorwaarden zoals deze beschreven zijn in artikel 7:458 BW. Voor de overige deelnemende partijen gelden de voorwaarden beschreven in artikel 24 UAVG. Er zit veel overlap in de voorwaarden in deze artikelen. Hieronder volgt een overzicht van de voorwaarden om aan beide artikelen te kunnen voldoen:

1. De verwerking betreft een wetenschappelijk, historisch of statistisch onderzoek.
2. Het onderzoek dient een algemeen belang.
3. Het onderzoek kan niet zonder de persoonsgegevens uitgevoerd worden.
4. Het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost of (voor zover het zorginstellingen betreft) gelet op de aard en het doel van het onderzoek in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.
5. De betrokkenen geen uitdrukkelijk bezwaar hebben gemaakt.
6. In het medisch dossier een aantekening wordt gemaakt dat het voor dit onderzoek gebruikt is.
7. Er zijn waarborgen die voorkomen dat de persoonlijke levenssfeer van de betrokkenen onevenredig geschaad wordt.

Uit het onderstaande volgt dat er in het kader van dit project aan deze voorwaarden wordt voldaan door alle deelnemende partijen met uitzondering van Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V.. Zij voldoen namelijk niet aan voorwaarde 4. Voor Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. is het vragen van uitdrukkelijke toestemming aan de betrokkenen van wie zij persoonsgegevens verstrekken niet onmogelijk en kost dat ook geen onevenredige inspanning. Dit komt met name door het relatief geringe aantal betrokkenen waar het om gaat (ten aanzien van Zorgpartners Midden-Holland circa 10.000 en ten aanzien van Vierstroom Zorg Thuis B.V. circa 4.500).

Om deze reden zullen Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. de betrokkenen van wie zij persoonsgegevens verstrekken om uitdrukkelijke toestemming vragen. Uitdrukkelijke toestemming van de betrokkene betreft een van de andere mogelijke uitzonderingsgronden uit artikel 9 lid 2 AVG (onder a). Ten aanzien van Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. berust de betreffende verdere verwerking dus op toestemming van de betrokkene (zie hiervoor). In dat kader zullen Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. de betrokkenen informeren over hun recht om de uitdrukkelijke toestemming – indien die gegeven wordt – te allen tijde in te trekken en over de wijze waarop de betrokkenen dit kunnen doen.

Onderstaande onderbouwing voor de conclusie dat voldaan wordt aan bovengenoemde zeven voorwaarden geldt dus voor alle deelnemende partijen met uitzondering van Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V..

Voorwaarde 1
De verwerking betreft een statistisch onderzoek. Een beschrijving hiervan is te vinden in het Onderzoeksprotocol.

Voorwaarde 2
Het doel van het statistisch onderzoek is om indicatoren te bepalen die van invloed zijn op de escalatie van het zorggebruik. Dit om effectieve interventietrajecten te kunnen formuleren om deze escalatie te voorkomen. Hiermee wordt de volksgezondheid bevorderd en beschermd.

Voorwaarde 3
Uit eerdere pilots uitgevoerd in opdracht van Stichting Transmuraal Netwerk Midden-Holland, waar vanuit openbare bronnen op wijkniveau gegevens worden gegenereerd (RIVM), is duidelijk geworden dat een verfijning van de data noodzakelijk is om de knelpunten nader te duiden. Deze verfijning is alleen mogelijk door de gegevens van de deelnemende partijen te delen voor dit onderzoek.

Voorwaarde 4
Voor het onderzoek zullen gegevens gebruikt worden van inwoners in de regio Midden-Holland van de afgelopen vijf jaar. Elk van de deelnemende zorg verlenende partijen beschikt zelf over gegevens over slechts een deel van de betrokkenen van het onderzoek. Daarnaast is het waarschijnlijk dat niet alle betrokkenen van het onderzoek nog in de regio wonen en ook de deelnemende partijen niet langer in staat zijn om deze betrokkenen te bereiken voor het vragen van toestemming. Het alsnog achterhalen van gegevens van deze betrokkenen om toestemming te vragen voor dit onderzoek, wordt gezien als een onevenredige inspanning.
Daarnaast volgt uit de wetsgeschiedenis dat toestemming niet hoeft te worden gevraagd indien daarbij zulke grote aantallen patiënten betrokken zijn dat redelijkerwijs niet kan worden gevergd dat inspanningen worden gedaan om deze allen te bereiken.[9] Gelet op het aantal betrokkenen (patiënten) waarvan persoonsgegevens worden verwerkt in het kader van het onderzoek is daarvan sprake.
Voor zorginstellingen geldt daarnaast dat door het vragen van toestemming en de mogelijkheid dat een deel van de populatie daardoor uitgesloten wordt in dit onderzoek zou in het eerste onderdeel van het onderzoek bovendien een verkeerde indeling van zorggebruik gemaakt worden op basis van de gemaakte kosten voor de zorg. Het vergelijken van 'heavy' en 'medium' users op basis van deze verkeerde indeling zou leiden tot een verkeerd inzicht in de verschillen tussen deze groepen. Hierdoor zou het vervolgens ook niet mogelijk zijn om in een vervolgtraject effectieve interventies op te zetten. Eenzelfde overweging geldt ook voor de medicalisering van de ouderen zorg. Het vragen van toestemming zou derhalve kunnen leiden tot een selectieve respons en daardoor tot onjuiste onderzoeksresultaten.

[9] Kamerstukken II, 1991/92, 21561, nr 20, p. 3.

Voorwaarde 5
Indien een betrokkene uitdrukkelijk bezwaar heeft gemaakt tegen het gebruik van zijn of haar gegevens voor onderzoeksdoeleinden dan zullen deze niet gebruikt worden voor dit onderzoek. In paragraaf 4.4.3 staan beschreven hoe een betrokkene bezwaar kan maken.

Voorwaarde 6
De deelnemende zorg verlenende partijen zullen hiervan een aantekening moeten maken op het moment dat zij gegevens aanleveren voor dit onderzoek.

Voorwaarde 7
Zoals beschreven staat in paragraaf 4.5, zijn voor het onderzoek alleen gepseudonimiseerde gegevens beschikbaar en is er geen toegang tot de originele gegevens. Hierdoor zijn de persoonsgegevens niet direct herleidbaar tot een betrokkene en is indirecte herleidbaarheid alleen mogelijk met additionele informatie die niet gebruikt wordt voor dit onderzoek en daarmee dus ook niet beschikbaar is op het platform waar de analyses voor het onderzoek worden verricht.

4.4.2. Transparantie
De Betrokkenen worden zoveel mogelijk geïnformeerd door het beschikbaar stellen van het Onderzoeksprotocol, deze DPIA, een overzicht van de gebruikte gegevens en een toegankelijke beschrijving (gebaseerd op het Onderzoeksprotocol en DPIA) van het onderzoek. Deze informatie wordt beschikbaar gesteld op een website van de Stichting.

Voor het actief verstrekken van informatie aan bestaande patiënten geldt – net als voor het vragen van toestemming – voor alle deelnemende partijen met uitzondering van Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. dat dit niet goed mogelijk is gelet op het grote aantal patiënten en het gegeven dat niet alle patiënten zonder onevenredige inspanning meer achterhaald kunnen worden.

Zorgpartners Midden-Holland en Vierstroom Zorg Thuis B.V. zullen de betrokkenen van wie zij de gegevens aanleveren dus wel actief bovengenoemde informatie verstrekken, namelijk op het moment dat zij de betrokkenen om uitdrukkelijke toestemming voor de verstrekking van hun gegevens vragen.

Bezwaar en/of intrekking van toestemming

Contactinformatie van de verschillende deelnemende partijen en instructies voor betrokkenen om bezwaar tegen het gebruik van zijn of haar gegevens voor deze verwerking te maken, zullen opgenomen worden op de website van de Stichting.

In het geval er bezwaar wordt uitgeoefend of de uitdrukkelijke toestemming wordt ingetrokken door een betrokkene dan zal dit moeten worden doorgevoerd in de systemen waarbij de gegevens over de desbetreffende personen worden verwijderd en/of in vervolg niet meer zullen worden verwerkt. De deelnemende partijen kunnen zelf een keuze maken hoe ze deze informatie aan de betrokkenen verstrekken. Afspraken hierover zijn onderdeel van de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting. Voor die dienstverleningsovereenkomst zie **bijlage A**.

4.4.3. Rechten van betrokkenen
In de AVG zijn rechten beschreven die elke betrokkene heeft met betrekking tot een verwerking. Te weten het recht op inzage (artikel 15 AVG), rectificatie (artikel 16 AVG),

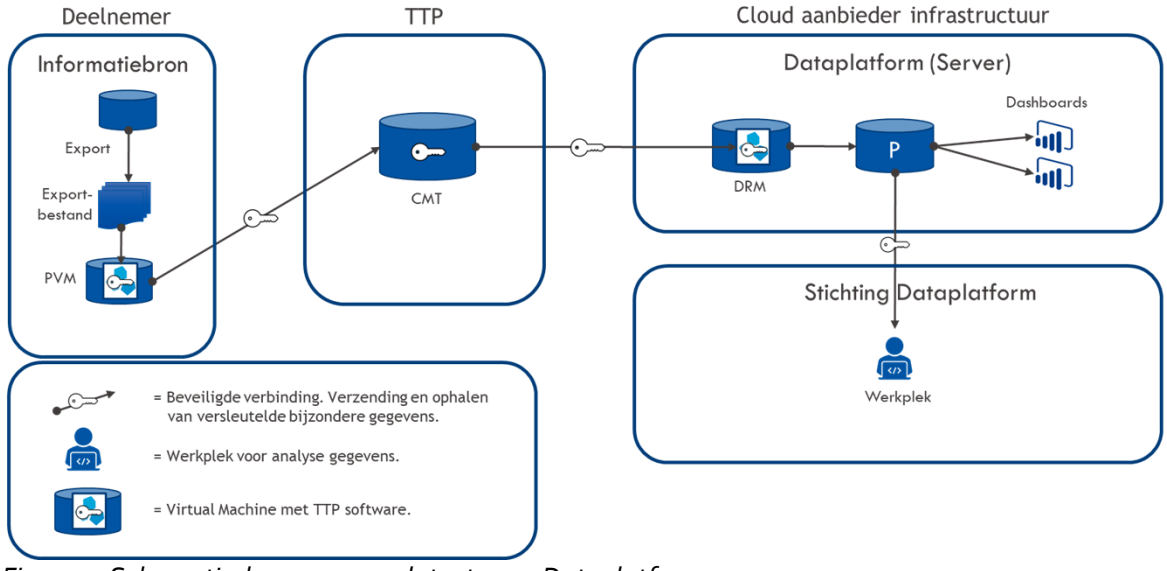
vergetelheid (artikel 17 AVG), beperking van de verwerking (artikel 18 AVG), overdraagbaarheid (artikel 20 AVG) en bezwaar (artikel 21 AVG).

Vanwege de technische maatregelen die genomen worden in deze verwerking is het niet langer mogelijk om betrokkenen te identificeren in de gegevens. Echter, dankzij de techniek van ZorgTTP is het wel mogelijk om te voldoen aan het recht op inzage, rectificatie, vergetelheid, beperking van de verwerking en overdraagbaarheid.

In het geval dat een betrokkene (of een wettelijk vertegenwoordiger daarvan) zijn rechten wil uitoefenen met betrekking tot de verwerking van zijn of haar persoonsgegevens voor dit onderzoek dan zullen de deelnemende partijen hiervan op de hoogte gebracht worden. De betrokkene zal gevraagd worden zich op passende wijze te identificeren (kopie van identiteitsbewijs waarop geboortenaam, voorletters, geboortedatum en geslacht herkenbaar zijn, maar waarop in ieder geval het gelaat en BSN onherkenbaar gemaakt zijn). De deelnemende partij zal in de verzendmodule van ZorgTTP de persoon opvoeren die bezwaar maakt met bijbehorende aanpassing. Deze data wordt gepseudonimiseerd en het verzoek wordt gekenmerkt met specifieke metadata en verstuurd naar ZorgTTP. ZorgTTP ontvangt de gepseudonimiseerde gegevens en de metadata voor het gekenmerkte verzoek. Vervolgens kenmerkt ZorgTTP het pseudoniem met de bijbehorende aanpassing. Dit pseudoniem wordt nogmaals gepseudonimiseerd en met bijbehorende kenmerkende metadata naar het Dataplatform gestuurd. Daar ontvangt de onderzoeker bij het Dataplatform de data met de opmerking om een specifiek pseudoniem aan te passen. Dit wordt als zodanig uitgevoerd. De onderzoeker koppelt terug aan de deelnemende partij dat de data is aangepast en refereert naar de bijbehorende kenmerkende metadata.
Op deze manier is het mogelijk om daar de gegevens van een enkele betrokkene te verwijderen.

4.5. Het verzamelen van gegevens

Voor het onderzoek zullen de benodigde gegevens (zie voor een overzicht hiervan paragraaf **Error! Reference source not found.**) op een centraal dataplatform gedeeld worden. Hieronder is een schematische weergave gemaakt van de datastroom. Voor een inhoudelijke beschrijving van de infrastructuur en de bijbehorende beveiliging wordt verwezen naar **bijlage C**.



Figuur 2. Schematische weergave datastroom Dataplatform

Voordat de gegevens hier terechtkomen zijn ze bij een van de deelnemende partijen ingevoerd in een bronsysteem. Vanuit dit bronsysteem wordt lokaal een exportbestand gegenereerd met daarin de voor het onderzoek relevante gegevens. De exacte specificaties van dit exportbestand staan beschreven in de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting.

Het bestand wordt verwerkt met de door de Third Trusted Party (TTP) aan de informatiebron beschikbaar gestelde versleutel- en verzendsoftware, de Privacy Verzend Module (PVM). Daarbij wordt het aangeboden bestand lokaal voor de eerste maal bewerkt met de door de TTP beschikbaar gestelde software. In deze bewerking wordt een scheiding aangebracht tussen de gegevens die gepseudonimiseerd moeten worden en de overige inhoudelijke gegevens, zoals beschreven in de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting. Op basis van dit onderscheid ondergaan de persoonsgegevens vervolgens een eerste bewerking voor de pseudonimisatie.

Hierna volgt transport via een beveiligde internetverbinding naar de TTP. De TTP voert met behulp van centrale pseudonimisatie software, de Centrale Module TTP (CMT), een tweede bewerking uit op de ontvangen gegevens waarbij een voor de ontvanger specifiek wachtwoord wordt gebruikt. Na deze bewerking is sprake van definitieve pseudoniemen in het bestand. Na verwerking wordt het gepseudonimiseerde bestand vrijgegeven en kan het worden opgehaald door de Doel Receive Module (DRM) in het dataplatform. Deze data is nu onomkeerbaar gepseudonimiseerd. De sleutel die gebruikt wordt voor het pseudonimiseren van de gegevens is uniek en specifiek voor dit gebruik van de Stichting en blijft na het genereren altijd hetzelfde. De sleutels zijn beveiligd opgeslagen en zijn niet toegankelijk.

Door het gebruik van een TTP worden de gegevens op locatie bij de deelnemende partijen reeds een eerste maal gepseudonimiseerd. Daardoor zijn de originele gegevens alleen daar beschikbaar. Hierdoor zullen op het dataplatform alleen gepseudonimiseerde gegevens terechtkomen en zijn alleen deze gegevens beschikbaar voor het onderzoek.

Op het dataplatform worden de gegevens opgeslagen en gestructureerd in een datawarehouse, maar zullen de originele waarden niet worden gewijzigd. Wel zullen hier controles plaatsvinden om vast te stellen of de afgesproken gegevens volgens de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting aangeleverd zijn. Mochten er uit deze controles of uit de verdere analyses tijdens het onderzoek onvolkomenheden ontdekt worden in de gegevens, dan zal dit teruggekoppeld worden aan de deelnemende partijen via de betreffende contactpersoon die vastgelegd is in de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting. Afspraken over welke datakwaliteit noodzakelijk is voor het onderzoek worden opgenomen in de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting. Het is de verantwoordelijkheid van de deelnemende partij die de gegevens aanlevert dat de kwaliteit op orde is.

4.6. Het gebruik van gegevens

De analyses voor het onderzoek worden verricht vanaf een beveiligde werkplek. Deze werkplek is alleen toegankelijk voor geautoriseerde gebruikers; de onderzoekers. Het bestuur van de Stichting kan gebruikers autoriseren voor toegang tot deze werkplek door middel van whitelisting van de ip-adressen. Vanaf deze werkplek is er toegang tot de verzamelde gegevens op het dataplatform om te combineren, ordenen en analyses te verrichten zoals beschreven in het Onderzoeksprotocol. De data blijven in deze omgeving voor de duur van het onderzoek en zal niet worden doorgezonden, verspreid of door derden opgevraagd kunnen worden.

Resultaten van het onderzoek worden aan de deelnemende partijen beschikbaar gesteld via dashboards en rapportages op basis van geanonimiseerde gegevens. Dit betekent dat deze dashboards en rapportages niet op individueel niveau rapporteren, maar op een geaggregeerd niveau. Hierbij is het uitgangspunt dat groepen waarover resultaten beschikbaar worden gesteld nooit kleiner dan 10 mogen zijn.

4.7. Het bewaren en vernietigen van de gegevens

Voor het onderzoek zullen gegevens van de afgelopen vijf jaar gebruikt worden. Gedurende de looptijd van het onderzoek zullen deze gegevens op het dataplatform bewaard worden. Na afloop van het onderzoek zullen de gegevens vernietigd worden.

4.8. Beveiliging

Voor de beveiliging van de gegevens wordt bij de verwerking gebruikgemaakt van de diensten van de TTP. Deze partij kan persoonsgegevens onomkeerbaar versleutelen en pseudonimiseren. Het is dus niet mogelijk om vanuit een pseudoniem de persoonsgegevens te achterhalen die gebruikt zijn in de constructie van het pseudoniem. Door de extra pseudonimisatie door de TTP is het voor geen enkele partij mogelijk om het pseudoniem te herleiden als deze in het dataplatform terecht komt. De bron heeft in geen geval toegang tot de versleutelde data, alleen de bron data. De ontvangende partij heeft toegang tot de pseudoniemen.

De Privacy Verzend Module (PVM) van de TTP pseudonimiseert de aangeboden gegevens en maakt daarbij gebruik van beveiligde internetverbindingen met de Centrale Module TTP bij de TTP. Een beveiligde verbinding maakt gebruik van het TLS protocol versie 1.2. In dit protocol identificeert de server zich met een digitaal certificaat uitgegeven door een Certificate Authority (CA). De verbinding komt alleen tot stand wanneer de CA bevestigt dat het certificaat nog actief is en niet ingetrokken. Hierbij wordt de OCSP-service gebruikt (of eventueel de CRL geraadpleegd). De server certificaten zijn ondertekend door een keten van certificaten die uitkomt bij een vertrouwd root certificaat. De PVM controleert alle certificaten in de keten op intrekking. De afnemercertificaten zijn digitale certificaten die worden uitgegeven door de QuoVadis CA en worden gebruikt voor de versleuteling van de te pseudonimiseren gegevens. De PVM controleert de status van het afnemercertificaat eveneens door middel van OCSP. Het enige gebruik van QuoVadis certificaten voor TLS betreft de client authenticatie voor pseudonimisatie binnen de Risicoverevening. In dat geval wordt door de PVM-verbinding gemaakt met een beveiligde verbinding voor de upload van gegevens naar CMT.

De server waarop de gegevens ontvangen en verzameld worden van de deelnemende partijen wordt gehost door de cloud provider Microsoft op het Azure platform in de regio West Europa. Toegang tot de server wordt dusdanig ingericht dat alleen geautoriseerde personen toegang zullen hebben tot deze server voor het doen van het onderzoek en voor onderhoud en beheer. Het Azure platform van Microsoft beschikt over, onder andere, ISO 27001, ISO 27018 en ISO 27701 certificeringen op het gebied van beveiliging en privacy.

De werkplek waarop de analyses voor het onderzoek gedaan worden, bevindt zich in een afgesloten ruimte waartoe alleen geautoriseerde personen toegang zullen hebben. Deze autorisatie zal door het bestuur van de Stichting alleen gegeven worden aan de onderzoekers die de gegevens verwerken in het kader van het onderzoek. In eerste instantie zal dat gaan om de gedetacheerde analist van het GHZ.

In de gegevensverwerking worden nieuwe technologieën gebruikt. Voor de versleuteling wordt speciale software van de TTP gebruikt. De reden hiervoor is extra veiligheid voor de versleuteling en verzending van data. Op de infrastructuur van de informatiebron wordt de Privacy Verzend Module (PVM) van de TTP geïnstalleerd. Hier wordt de data bij de databron voor een eerste maal gepseudonimiseerd, waardoor de persoonsgegevens de deur van de organisatie niet in onversleutelde vorm verlaten. De TTP maakt daarnaast gebruik van een eigen Centrale Module TTP (CMT) om de data extra te pseudonimiseren. De ontvangende partij ontvangt de data met de ontvangstmodule (DRM) van de TTP. De data worden doorgestuurd naar de database in het dataplatform in de cloud. Deze database staat in Duitsland. Alleen vanaf de werkplek bij de Stichting kan toegang verkregen worden tot het dataplatform.

5. AVG-privacy principes

In dit hoofdstuk worden de privacy principes bekeken waar deze DPIA aan moet voldoen.

5.1. Gegevensbeperking

De samenstelling en noodzaak van de te verzamelen gegevens worden in de volgende paragraaf toegelicht op de volgende AVG-beginselen: [vereiste conform WP29]

- Proportionaliteit: staat het belang van de verwerking in verhouding tot de inbreuk op de privacy van Betrokkenen?
- Subsidiariteit: kan het doel ook worden bereikt met minder gegevens of andere gegevens?

Informatie met betrekking tot de proportionaliteit en subsidiariteit wordt beschreven in het Onderzoeksprotocol in paragraaf 7.4.5 voor wat betreft de proportionaliteit en paragraaf 7.2 en 7.3.4 voor wat betreft de subsidiariteit (**bijlage E**).

5.2. Gegevenskwaliteit

Omdat het onderzoek een verdere verwerking is van de gegevens en het niet mogelijk is om terug te koppelen richting de deelnemende partij om welke betrokkene het gaat in geval van onjuiste gegevens, worden er geen aanvullende maatregelen getroffen binnen het onderzoek om de kwaliteit van de gegevens te waarborgen. Er wordt van uitgegaan dat ieder van de deelnemende partijen al adequate maatregelen heeft getroffen om de kwaliteit van de gegevens te borgen.

Mochten er tijdens de analyses problemen ten aanzien van de kwaliteit van de gegevens aan het licht komen, dan zullen deze teruggekoppeld worden aan de contactpersoon van de betreffende deelnemende partij(en) zoals opgenomen in de dienstverleningsovereenkomst tussen de deelnemende partijen en de Stichting. Daarbij geldt de beperking dat het niet mogelijk is om terug te koppelen om welke records het gaat waarin de fouten optreden.

5.3. Verantwoordelijkheid en verantwoording

De verwerkingsverantwoordelijke moet verantwoordelijk kunnen worden gehouden voor het naleven van maatregelen die uitvoering geven aan de AVG-privacy principes. In het kader daarvan is deze DPIA uitgevoerd. Hiermee worden voorafgaand aan de verwerking de privacy risico's voor betrokkenen in kaart gebracht. De DPIA is een iteratief proces, dat opnieuw moet worden uitgevoerd zodra er nieuwe dataleveranciers toetreden of zodra afspraken wijzigen of de inhoud van verzamelde data wijzigt. Twee keer per jaar wordt het programma geëvalueerd met vertegenwoordigers van zorgaanbieders, gemeenten, patiënten en leveranciers. Met dit iteratieve proces onderwerpt de Stichting zich aan een periodieke evaluatie en toont zij aan compliant te zijn met de AVG, zoals vereist volgens WP29[10]. De resultaten van het onderzoek zullen besproken worden in deze stuurgroep.

5.3.1. Toezichthoudende en sturende organen tijdens het onderzoek

Voor uitvoering en sturing op het onderzoek zijn er toezichthoudende en sturende organen in het leven geroepen om het onderzoek in goede banen te leiden en toe te zien op de budgettaire en juridische voorwaarden:

- Stuurgroep: minimaal één afgevaardigde van de deelnemende partijen en een bestuurder van de Stichting. Wanneer er besluiten genomen dienen te worden door de stuurgroep tijdens het onderzoek, kan de stuurgroep gebruik maken van de expertise uit één of meerdere van de projectgroepen.

[10] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf

- Projectgroepen:
    - Business Intelligence (BI) Team: minimaal één afgevaardigde van de deelnemende partijen. Verantwoordelijk voor invulling van de BI gerelateerde taken. Voornamelijk data gerelateerd.
    - ICT Team: minimaal één afgevaardigde van de deelnemende partijen. Verantwoordelijk voor invulling van de ICT gerelateerde taken, zoals inrichting en opzetten infrastructuur.
    - FG & Juridisch Team: minimaal één afgevaardigde van de deelnemende partijen. Bevat minimaal de rollen: Functionaris Gegevensbescherming (FG), Jurist en Information Security Officer (ISO). Verantwoordelijk voor het toetsen en toezien op de correcte handhaving van de juridische invulling van het project.
- Projectmanager: is vertegenwoordigd in alle projectgroepen, brengt verslag uit naar de stuurgroep.

5.4. Mening van betrokkenen

Op grond van artikel 35 lid 9 AVG moet de verwerkingsverantwoordelijke de betrokkenen of hun vertegenwoordigers naar hun mening vragen over de voorgenomen verwerking. Vertegenwoordigen van betrokkenen zijn geïnformeerd over de voorgenomen verwerkingen van persoonsgegevens tijdens diverse overleggen met een cliëntenpanel met cliëntvertegenwoordigers van de betrokken zorgorganisaties. Tijdens deze overleggen is de cliëntvertegenwoordigers ook naar hun mening gevraagd. Van de overleggen zijn verslagen gemaakt. .

6. Risicobeoordeling en maatregelen

In de vorige hoofdstukken is een systematische beschrijving van de gegevensverwerking gegeven. In dit hoofdstuk wordt ingegaan op de uitgevoerde inventarisatie van de gesignaleerde risico's bij die verwerkingen en de beoogde maatregelen om de risico's aan te pakken, zoals op grond van de AVG vereist is.[11] De inventarisatie is gebaseerd op een ingevulde 'DPIA vragenlijst' die als **bijlage G** bij deze DPIA is opgenomen.

6.1. Risico's

Uit de inventarisatie volgen de in onderstaande tabel weergeven risico's.

Risico	**Mogelijke gevolgen voor de betrokkenen**	**Bedreigingen die tot verwezenlijking risico kunnen leiden**	**Waarschijnlijkheid risico (laag/gemiddeld/hoog)**	**Ernst risico (laag/gemiddeld/ hoog)**
Onrechtmatige toegang tot/verstrekking van de persoonsgegevens	De persoonsgegevens komen bij derden terecht, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, betrokkenen kunnen (deels) hun rechten en vrijheden niet uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen.	Ontoereikende beveiligingsmaatregelen	Laag	Hoog
Ongewenste wijziging van de persoonsgegevens	De persoonsgegevens komen niet (geheel) meer overeen met de werkelijkheid, betrokkenen kunnen (deels) hun rechten en vrijheden niet uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen.	Ontoereikende beveiligingsmaatregelen	Laag	Laag
Verlies/vernietiging van de persoonsgegevens	Verlies van vertrouwelijkheid van door het beroepsgeheim	Ontoereikende beveiligingsmaatregelen	Laag	Laag

[11] AVG artikel 35, lid 7, onder d, en overweging 90

	beschermde persoonsgegevens.			
Onbedoeld gebruik van de persoonsgegevens	De persoonsgegevens zouden ook voor ander onderzoek gebruikt kunnen worden waardoor ze langer gebruikt worden, betrokkenen kunnen (deels) hun rechten en vrijheden niet uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen.	Ontoereikende beschrijving van het onderzoek waarvoor de gegevens gebruikt worden of ontoereikende controle op gebruik conform beschreven onderzoek	Middel	Gemiddeld
Onbedoelde vermenging van persoonsgegevens	De persoonsgegevens komen niet (geheel) meer overeen met de werkelijkheid, betrokkenen kunnen (deels) hun rechten en vrijheden niet uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen.	Fouten in het pseudonimisatieproces	Laag	Laag

6.2. Maatregelen

In onderstaand schema zijn de beoogde maatregelen opgenomen die de gesignaleerde risico's moeten beperken.

Risico	**Beoogde maatregelen ter beperking van het risico**	**Effect op risico**	**Restrisico**
Onrechtmatige toegang tot/verstrekking van de persoonsgegevens	Technische en organisatorische beveiligingsmaatregelen , waaronder beveiligde verbindingen, dubbele pseudonimisatie, sluiten van verwerkersovereenkomsten	Risico aanzienlijk verkleind	Laag
Ongewenste wijziging van de persoonsgegevens	Beperken van rechten onderzoeker.	Risico verkleind.	Laag

Verlies/vernietiging van de persoonsgegevens	Backups in de Cloud.	Risico aanzienlijk verkleind.	Laag
Onbedoeld gebruik van de persoonsgegevens	Maken van goede afspraken met onderzoeker en controle op de naleving van de gemaakte afspraken	Risico wordt nog kleiner	Laag
Onbedoelde vermenging van persoonsgegevens	Contracteren zorgvuldig opererende TTP.	Risico wordt nog kleiner	Laag

In de paragrafen hieronder worden de gesignaleerde risico's en de beoogde maatregelen nader beschreven.

6.3. Onrechtmatige toegang

6.3.1. Het risico en de mogelijke gevolgen

Het risico bestaat dat onrechtmatige toegang tot/verstrekking van de persoonsgegevens plaatsvindt, met als mogelijke gevolgen dat derden ongeoorloofde toegang tot de gegevens krijgen die voor het onderzoek worden gebruikt, dat er sprake is van verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens en/of dat betrokkenen (deels) hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen. Dit risico kan zich in verschillende stadia van het onderzoek voordoen. Om dit te voorkomen zijn de volgende maatregelen getroffen.

6.3.2. Ontsluiten van gegevens in het bronsysteem

Voor dit onderzoek dienen gegevens uit het bronsysteem van de deelnemende partijen ontsloten te worden. Deze werkzaamheden worden door medewerkers van de deelnemende partijen zelf verzorgd. Hierbij wordt ervan uitgegaan dat de deelnemende partijen adequate maatregelen hebben getroffen. Voordat de gegevens verstuurd worden door de deelnemende partij worden deze voor de eerste maal gepseudonimiseerd en versleuteld met behulp van software van de TTP. Hierdoor wordt directe herleidbaarheid van de gegevens vanaf dit punt voorkomen. Indirecte herleidbaarheid is alleen mogelijk met een grote inspanning waardoor de impact van ongeoorloofde toegang aanzienlijk verkleind wordt.

6.3.3. Verwerking van de gegevens bij de TTP

Het versturen van de gegevens naar de TTP geschiedt via een beveiligde verbinding. Vervolgens ondergaan de gegevens bij de TTP een tweede pseudonimisatie en worden ze in een beveiligde omgeving klaargezet voor verzending naar het dataplatform. Het versturen van de gegevens naar het dataplatform geschiedt wederom via een beveiligde verbinding. De TTP is een gerenommeerde partij en beschikt over een ISO27001 certificaat en NEN 7510 certificaat, tevens is er een verwerkersovereenkomst gesloten met de TTP. Door het gebruik van een TTP wordt de kans op en de impact van ongeoorloofde toegang aanzienlijk verkleind. In **bijlage A** is een gedetailleerde beschrijving van de werking van de TTP opgenomen.

6.3.4. Onderzoek

De gegevens voor het onderzoek worden op het dataplatform ontvangen. Alleen geautoriseerde gebruikers hebben toegang tot deze systemen. De onderzoekers worden door de stuurgroep geautoriseerd om dit onderzoek te doen en verrichten daartoe de handelingen zoals beschreven in het onderzoeksprotocol.

Voordat de onderzoekers geautoriseerd worden zal er in het geval van detachering een geheimhoudingsverklaring getekend worden door de onderzoeker. Wanneer er een (sub-)verwerker ingeschakeld wordt voor het uitvoeren van het onderzoek zal er een (sub-)verwerkersovereenkomst gesloten worden. Alle onderzoekers zullen op de hoogte gesteld worden van het beveiligingsbeleid dat geldt voor het gebruik van de infrastructuur. De normen daarvoor (waaronder ISO27001/NEN7510) zijn vastgelegd in **bijlage C** en de exacte invulling zal gegeven worden door de leverancier van de infrastructuur.

Onderdeel van deze infrastructuur is een beveiligde en afgesloten werkplek die alleen toegankelijk is voor geautoriseerde gebruikers, gefaciliteerd door de Stichting. De gegevens voor het onderzoek zijn alleen vanaf deze werkplek toegankelijk. De resultaten van het onderzoek zullen alleen in geaggregeerde (anonieme) vorm gedeeld worden. Hierdoor hebben alleen de geautoriseerde gebruikers toegang tot de gegevens voor het onderzoek.

Door zowel de beveiligingsmaatregelen van de werkplek, de beschrijving van het onderzoek in het Onderzoeksprotocol dat de onderzoekers dienen te volgen en het beperkte aantal geautoriseerde gebruikers wordt de kans op ongeoorloofde toegang zo klein mogelijk gehouden.

6.3.5. Beheer van het dataplatform

Omdat de Stichting niet zelf over de capaciteit beschikt om de infrastructuur op te zetten en/of beheren, wordt dit uitbesteed aan een leverancier. De Stichting zal afspraken met deze leverancier maken om een gedegen en betrouwbare dienst te leveren. Hiertoe worden er een dienstverleningsovereenkomst met een Service Level Agreement en een Verwerkersovereenkomst afgesloten met de leverancier. De beveiligingsnormen waaraan deze infrastructuur en het beheer daarvan dient te voldoen (waaronder ISO27001/NEN7510) zijn opgenomen in **bijlage C**. Het dataplatform zal daarom vanaf de omgeving van de beheerder toegankelijk moeten zijn.

6.3.6. Conclusie

Door de genomen technische en organisatorische beveiligingsmaatregelen is de kans klein dat derden ongeoorloofd toegang zullen krijgen tot de gegevens die voor het onderzoek gebruikt zullen worden, dat er sprake zal zijn van verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens en/of dat betrokkenen (deels) hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen. In het geval een derde toch ongeoorloofd toegang krijgt tot de gegevens, dan is door de dubbele pseudonimisatie de kans bovendien klein dat de gegevens door deze derde te herleiden zijn tot de betrokkenen.

6.4. Ongewenste wijziging

6.4.1. Het risico en de mogelijke gevolgen

Het risico bestaat dat de gegevens die voor het onderzoek worden gebruikt, per ongeluk worden gewijzigd met als mogelijke gevolgen dat de persoonsgegevens niet (geheel) meer overeenkomen met de werkelijkheid en/of dat betrokkenen (deels) hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen. Een dergelijke wijziging zou voor de betrokkenen echter zeer geringe gevolgen hebben, omdat de gegevens tijdens het onderzoek geheel gescheiden zijn van de originele door de bron aangeleverde gegevens.

Ongewenste wijziging van de gegevens zou gevolgen kunnen hebben voor de resultaten van het onderzoek en dan slechts wanneer de wijziging zou leiden tot significant andere resultaten.

6.4.2. Genomen maatregelen

De in paragraaf 6.2 beschreven maatregelen zorgen er voor dat de kans dat ongewenste wijziging van de gegevens zich voordoet, klein is. En mochten er onverhoopt toch gegevens gewijzigd worden, dan kan dit opgelost worden door een nieuwe levering van gegevens bij de deelnemende partijen te vragen.

6.4.3. Conclusie

Er is weliswaar een risico op ongewenste wijziging van de gegevens die voor het onderzoek worden gebruikt, maar indien dit risico zich zou verwezenlijken, zou dit slechts zeer geringe gevolgen hebben voor de betrokkenen. Om de kans op ongewenste wijziging van gegevens te voorkomen, zijn bovendien diverse maatregelen getroffen. Mocht het risico zich desondanks verwezenlijken, dan kunnen de gewijzigde gegevens worden vervangen door een nieuwe levering uit het bronbestand.

6.5. Verlies of vernietiging van gegevens

6.5.1. Het risico en de mogelijke gevolgen

Het risico bestaat dat de gegevens die voor het onderzoek worden gebruikt, per ongeluk verloren gaan of vernietigd worden, met als mogelijk gevolg dat sprake is van verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens. Van dat gevolg zal echter geen sprake zijn,, omdat de gegevens die voor het onderzoek gebruikt worden, kopieën zijn van de originele door de bron aangeleverde gegevens.

Verlies of ongewenste vernietiging van de gegevens zou alleen gevolgen kunnen hebben voor de resultaten van het onderzoek en dan nog slechts wanneer het verlies of de ongewenste vernietiging zou leiden tot significant andere resultaten.

6.5.2. Genomen maatregelen

De in paragraaf 6.2 beschreven maatregelen zorgen er voor dat de kans dat ongewenste verdwijning van de gegevens zich voordoet, klein is. En mochten er onverhoopt toch gegevens verdwijnen, dan kan dit opgelost worden door een nieuwe levering van gegevens bij de deelnemende partijen te vragen.

6.5.3. Conclusie
Er is weliswaar een risico op ongewenste verdwijning van de gegevens die voor het onderzoek worden gebruikt, maar indien dit risico zich zou verwezenlijken, zou dit geen gevolgen hebben voor de betrokkenen. Om de kans op ongewenste verdwijning van gegevens te voorkomen, zijn bovendien diverse maatregelen getroffen. Mochten het risico zich desondanks verwezenlijken, dan kunnen de verdwenen gegevens worden aangevuld met een nieuwe levering uit het bronbestand.

6.6. Onbedoeld gebruik

6.6.1. Het risico en de mogelijke gevolgen
Het risico bestaat dat de gegevens die voor het onderzoek worden gebruikt, ook voor andere onderzoeken gebruikt zouden kunnen worden, met als mogelijke gevolgen dat de persoonsgegevens langer worden verwerkt en/of dat betrokkenen (deels) hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen. Wanneer de gegevens langer worden verwerkt zou bijvoorbeeld het risico op ongeoorloofde toegang gedurende een langere periode blijven bestaan.

6.6.2. Genomen maatregelen
Om te voorkomen dat de gegevens voor andere verwerkingen dan het onderzoek worden gebruikt is het Onderzoeksprotocol opgesteld waarin beschreven staat welke verwerkingen de onderzoekers uitvoeren en welke vragen er met het onderzoek beantwoord worden. De organen benoemd in paragraaf 5.3.1 houden hierop toezicht.

De in paragraaf 6.2 beschreven maatregelen zorgen er bovendien voor dat indien er toch sprake zou zijn van onbedoeld gebruik, het risico op nadelige gevolgen voor de betrokkenen wordt beperkt.

6.6.3. Conclusie
Er is weliswaar een risico op onbedoeld gebruik van de gegevens die voor het onderzoek worden gebruikt, maar door toezicht op de onderzoekers wordt de kans dat dit risico zich verwezenlijkt, aanzienlijk verkleind. Indien zich onverhoopt toch onbedoeld gebruik van de gegevens zou voordoen, beperken de in paragraaf 6.2 genomen maatregelen bovendien het risico op nadelige gevolgen voor de betrokkenen.

6.7. Vermenging van gegevens

6.7.1. Het risico en de mogelijke gevolgen
Aangezien de persoonsgegevens van betrokkenen uit verschillende bronnen afkomstig zijn, bestaat het risico dat er iets misgaat bij het samenvoegen van de gegevens, waardoor persoonsgegevens ten onrechte worden gekoppeld aan een bepaalde betrokkene, met als mogelijke gevolgen dat de persoonsgegevens niet (geheel) meer overeenkomen met de werkelijkheid en/of dat betrokkenen (deels) hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen. Een dergelijke vermenging zou voor de betrokkenen slechts zeer geringe gevolgen hebben, omdat de gegevens tijdens het onderzoek geheel gescheiden zijn van de originele door de bron aangeleverde gegevens.

Ongewenste vermenging van de gegevens zou gevolgen kunnen hebben voor de resultaten van het onderzoek en dan slechts wanneer de vermenging zou leiden tot significant andere resultaten.

6.7.2. Genomen maatregelen

De in paragraaf 6.2 beschreven maatregelen zorgen er voor dat de kans dat ongewenste vermenging van de gegevens zich voordoet, klein is. En mochten er onverhoopt toch gegevens vermengd worden, dan kan dit – mits dit onderkend wordt – opgelost worden door een nieuwe levering van gegevens bij de deelnemende partijen te vragen.

6.7.3. Conclusie

Er is weliswaar een risico op ongewenste vermenging van de gegevens die voor het onderzoek worden gebruikt, maar indien dit risico zich zou verwezenlijken, zou dit slechts zeer geringe gevolgen hebben voor de betrokkenen. Om de kans op ongewenste vermenging van gegevens te voorkomen, zijn bovendien diverse maatregelen getroffen. Mochten het risico zich desondanks verwezenlijken, dan kunnen de vermengde gegevens worden vervangen door een nieuwe levering uit het bronbestand.

6.8. Conclusie

De in dit hoofdstuk naar voren gebrachte risico's kunnen door de eveneens in dit hoofdstuk beschreven maatregelen en waarborgen zodanig worden afgedekt dat er geen sprake is van hoge restrisico's. Om die reden is er geen voorafgaande raadpleging van de Autoriteit Persoonsgegevens als bedoeld in artikel 36 AVG nodig.

7. Rol van de FG's

In dit hoofdstuk wordt ingegaan op de rol van de FG's van de verwerkingsverantwoordelijken.

7.1 Verplichtingen op grond van de AVG

De verwerkingsverantwoordelijken beschikken allemaal over een FG. Op grond van artikel 35 lid 2 AVG dienen verwerkingsverantwoordelijken bij het uitvoeren van een DPIA advies in te winnen bij hun FG. Daarnaast dient de FG op grond van artikel 39 lid 1 onder c AVG toe te zien op de uitvoering van de DPIA.

7.2 Toezicht op de uitvoering van de DPIA

Alle FG's van de verwerkingsverantwoordelijken zijn bij de totstandkoming van deze DPIA betrokken en hebben op die manier toezicht kunnen houden op de uitvoering van de DPIA.

7.3 Advies van de FG's

De adviezen van de FG's met betrekking tot deze DPIA zijn als **bijlage F** aan deze DPIA gehecht.

8. Bijlagen

A. Dienstverleningsovereenkomst
B. Def Visiedocument GZMH anoniem.pdf
C. Factsheet_pseudonimisatie_ZorgTTP_2017.pdf
D. v20200701_Adviesrapport__infrastructuur_Stichting_Dataplatform_Midden_Holland.pdf (concept versie)
E. Onderzoeksprotocol Gedeelde zorg
F. Adviezen van de FG's van verwerkingsverantwoordelijken
G. Ingevulde DPIA vragenlijst