MODEL VERWERKERSOVEREENKOMST IN HET KADER VAN ONDERAANNEMING WIJKVERPLEEGKUNDIGE ZORG

**DE ONDERGETEKENDE:**

1. [Naam organisatie}, gevestigd te [postcode en plaats] aan de [straat], te dezen rechtsgeldig vertegenwoordigd door [functie en naam vertegenwoordigingsbevoegde persoon] hierna te noemen: "***Verwerkingsverantwoordelijke***” (of vervangen door naam organisatie)”;

en

1. [Naam organisatie}, gevestigd te [postcode en plaats] aan de [straat], te dezen rechtsgeldig vertegenwoordigd door [functie en naam vertegenwoordigingsbevoegde persoon] hierna te noemen: "**Verwerker**” (of vervangen door naam organisatie)”;
2. .

Partijen worden hierna tezamen ook genoemd: “***Partijen***” en individueel “***Partij***”;

**NEMEN HET VOLGENDE IN AANMERKING:**

• Verwerker diensten op het gebied van verpleegkundige zorg verricht ten behoeve van Verwerkingsverantwoordelijke, zoals beschreven in de hoofdovereenkomst [naam], met datum ondertekening: [ ] (hierna: “*Hoofdovereenkomst*’).

• de diensten met zich meebrengen dat persoonsgegevens (hierna: “*Persoonsgegevens*”) worden verwerkt, waarvoor Verwerkingsverantwoordelijke verwerkingsverantwoordelijke is in de zin van de Algemene Verordening Gegevensbescherming (hierna: “Avg”).

• Verwerker de betreffende Persoonsgegevens louter in opdracht van Verwerkingsverantwoordelijke verwerkt en niet voor eigen doeleinden. Verwerker is in dat kader aan te merken als verwerker in de zin van de Avg.

• Partijen in deze Verwerkersovereenkomst hun afspraken met betrekking tot de verwerking van Persoonsgegevens in het kader van de diensten wensen vast te leggen.

• deze Verwerkersovereenkomst, indien van toepassing, alle eerdere overeenkomst(en) van gelijke strekking tussen Partijen vervangt.

**ZIJN OVEREENGEKOMEN ALS VOLGT:**

**Artikel 1 Uitvoering van de verwerking van Persoonsgegevens**

* 1. Verwerkingsverantwoordelijke geeft hierbij opdracht aan Verwerker om Persoonsgegevens te verwerken namens de Verwerkingsverantwoordelijke op de wijze zoals omschreven in **Annex 1** en in overeenstemming met de bepalingen van deze Verwerkersovereenkomst en de Avg.
  2. Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend Persoonsgegevens zal verwerken voor zover dit noodzakelijk is voor de levering van de diensten onder de Hoofdovereenkomst. Overige verwerkingen zullen uitsluitend worden uitgevoerd in expliciete schriftelijke opdracht van Verwerkingsverantwoordelijke of als daartoe een wettelijke verplichting bestaat, dan echter uitsluitend na informeren van Verwerkingsverantwoordelijke. Informeren van Verwerkingsverantwoordelijke blijft achterwege indien dat in strijd zou zijn met de wet.
  3. Verwerker heeft geen zelfstandige zeggenschap over de Persoonsgegevens die door hem worden en mag de Persoonsgegevens niet voor eigen of andere doeleinden verwerken.
  4. De Verwerkingsverantwoordelijke kan aanvullende, schriftelijke instructies aan Verwerker geven ingeval van aanpassingen of wijzigingen in de van toepassing zijnde wet- en regelgeving op het gebied van bescherming van Persoonsgegevens. Verwerker zal alle redelijke instructies van Verwerkingsverantwoordelijke in verband met de verwerking van de Persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van Persoonsgegevens.
  5. Onverminderd het bepaalde in artikel 1 lid 2, is het Verwerker toegestaan om Persoonsgegevens te verwerken indien een wettelijk voorschrift (waaronder begrepen daarop gebaseerde rechterlijke of bestuurlijke bevelen) hem tot een verwerking verplicht. In dat geval stelt de Verwerker voorafgaand aan de verwerking Verwerkingsverantwoordelijke in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker zal Verwerkingsverantwoordelijke, waar mogelijk, in staat stellen zich te verweren tegen deze verplichte verwerking en ook overigens de verplichte verwerking beperken tot het strikt noodzakelijke.
  6. Verwerker zal de Persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze verwerken en in overeenstemming met de op hem als Verwerker rustende verplichtingen op grond van de Avg, Uitvoeringswet Avg en overige van toepassing zijnde wet- en regelgeving. Verwerker zal in dat kader ten minste een register van verwerkingen aanleggen als bedoeld in artikel 30 Avg en Verwerkingsverantwoordelijke op eerste verzoek een kopie van dat register verstrekken.
  7. Indien de dienstverlening door Verwerker de verwerking van gezondheidsgegevens of andere bijzondere Persoonsgegevens impliceert, garandeert Verwerker dat hij niet in strijd met gezondheidswetgeving (waaronder mede doch niet uitsluitend de Wet aanvullende bepalingen verwerking persoonsgegevens in de Zorg, Wet geneeskundige behandelingsovereenkomst en de Gedragscode Elektronische gegevensuitwisseling in de Zorg) zal handelen.

**Artikel 2. Geheimhouding**

2.1 Verwerker is verplicht de Persoonsgegevens en al hetgeen waarvan hij met betrekking tot de uitvoering van deze Verwerkersovereenkomst kennisneemt, geheim te houden. Verwerker zal ervoor zorgen dat diens personeel en eventuele derde(n) die noodzakelijkerwijs van de Persoonsgegevens kennis dienen te nemen, zich houden aan de geheimhoudingsverplichting, door hen een geheimhoudingsverklaring te laten ondertekenen. Deze verplichting zal schriftelijk worden vastgelegd en een kopie daarvan zal op eerste verzoek van de Verwerkingsverantwoordelijke ter inzage worden aangeboden.

2.2 Verwerker zal de Persoonsgegevens niet delen met of verstrekken aan derden, tenzij Verwerker daartoe voorafgaande, schriftelijke toestemming of opdracht heeft verkregen van Verwerkingsverantwoordelijke of op grond van dwingendrechtelijke regelgeving daartoe verplicht is. Indien Verwerker op grond van dwingendrechtelijke regelgeving verplicht is om de Persoonsgegevens te delen met of te verstrekken aan derden, dan zal Verwerker de Verwerkingsverantwoordelijke hierover voorafgaand schriftelijk en onverwijld informeren, tenzij dit niet is toegestaan onder de genoemde regelgeving.

**Artikel 3. Beveiligingsmaatregelen**

3.1 Verwerker zal aantoonbaar, passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de (in Annex 1 gespecificeerde) aard van de te verwerken Persoonsgegevens, ter bescherming van de Persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid van de gegevens te garanderen. In deze beveiligingsmaatregelen zijn de mogelijk in de Overeenkomst reeds bepaalde maatregelen begrepen. De maatregelen omvatten in ieder geval:

a.) maatregelen om te waarborgen dat enkel bevoegde medewerkers toegang hebben tot de Persoonsgegevens voor de doeleinden die zijn uiteengezet;

b.) maatregelen waarbij de Verwerker zijn medewerkers en subverwerkers uitsluitend toegang geeft tot Persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die Persoonsgegevens waartoe de toegang voor de betreffende (rechts)persoon noodzakelijk is;

c.) maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

d.) maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan Verwerkingsverantwoordelijke;

e.) maatregelen om de tijdige beschikbaarheid van de Persoonsgegevens te garanderen;

f.) maatregelen om te waarborgen dat Persoonsgegevens logisch gescheiden worden verwerkt van de Persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt;

g.) de overige maatregelen die Partijen zijn overeengekomen zoals vastgelegd in Annex 2.

3.2 Verwerker werkt aantoonbaar in overeenstemming met ISO27001 en/of NEN 7510 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van Persoonsgegevens, waarin in ieder geval de in het eerste lid van dit artikel 3 genoemde maatregelen uiteen zijn gezet. Verwerker voldoet aan de eisen zoals beschreven in NEN7512 en NEN7513 en in andere NEN-normen, voor zover die voor de gezondheidszorg van toepassing zijn verklaard.

3.3 Indien Verwerker deze daarover beschikt, zal hij op eerste verzoek van Verwerkingsverantwoordelijke een door een onafhankelijke en ter zake deskundige derde afgegeven geldig certificaat overleggen, waaruit volgt dat Verwerker de verplichtingen uit dit artikel naleeft.

3.4 Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 3 periodiek evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel 3. Het voorgaande laat de instructiebevoegdheid van Verwerkingsverantwoordelijke om zo nodig aanvullende maatregelen te (doen) treffen onverlet.

**Artikel 4 Toezicht op naleving**

4.1 Verwerkingsverantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor in artikel 3 lid 1 en 2 genoemde maatregelen. Verwerker stelt Verwerkingsverantwoordelijke, indien Verwerkingsverantwoordelijke daarom verzoekt, hiertoe in elk geval eenmaal per jaar in de gelegenheid op een door Partijen in gezamenlijk overleg nader te bepalen tijdstip en verder indien Verwerkingsverantwoordelijke daar aanleiding toe ziet naar aanleiding van (vermoeden van) informatie- of privacy-incidenten, dat te (laten) controleren. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijk onderzoek in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

4.2 Verwerker zal in alle redelijkheid haar medewerking verlenen aan het onder 4.1 bedoelde onderzoek en is verplicht aan Verwerkingsverantwoordelijke en/of auditors ingehuurd door Verwerkingsverantwoordelijke toegang te verschaffen tot (relevante delen van) de ruimtes, systemen en/of servers waarin/waarmee de verwerking van de Persoonsgegevens op enig moment plaatsvindt en zal aan Verwerkingsverantwoordelijke en/of auditors ingehuurd door Verwerkingsverantwoordelijke, alle relevante informatie verstrekken. De tijd die Verwerker hiervoor spendeert is voor eigen kosten.

4.3 Verwerker verstrekt op eerste verzoek van Verwerkingsverantwoordelijke een rapportage aan Verwerkingsverantwoordelijke waarin Verwerker informeert over de stand van de beveiligingsmaatregelen zoals omschreven in artikel 3.1 en **Annex 2**, incidenten of datalekken zoals omschreven in artikel 6 die hebben plaatsgevonden en mogelijke beveiligingsrisico's ten aanzien van de Persoonsgegevens.

4.4 Verwerkingsverantwoordelijke en Verwerker kunnen naar aanleiding van de onder artikel 5.3 benoemde rapportage, nadere beveiligingsmaatregelen overeenkomen. Een overzicht van deze aanvullende beveiligingsmaatregelen zal als annex aan deze Verwerkersovereenkomst worden gehecht.

**Artikel 5 Medewerkingsverplichtingen**

5.1 Verwerker zal zijn volledige en tijdige medewerking verlenen aan Verwerkingsverantwoordelijke bij de nakoming van de op Verwerkingsverantwoordelijke rustende verplichtingen voortvloeiende uit de rechten die in de Avg aan de betrokkenen zijn toegekend.

5.2 Een door Verwerker ontvangen klacht of een verzoek van een betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zo spoedig mogelijk doorgestuurd naar Verwerkingsverantwoordelijke.

5.3 Op het eerste daartoe strekkende verzoek van Verwerkingsverantwoordelijke zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van Persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de toepasselijke (privacy) wetgeving naleeft.

5.4 Verwerker zal voorts op eerste verzoek van Verwerkingsverantwoordelijke alle noodzakelijke bijstand verlenen bij de nakoming van de op grond van de toepasselijke privacywetgeving op Verwerkingsverantwoordelijke rustende wettelijke verplichtingen (zoals het uitvoeren van een privacy impact assessment).

**Artikel 6. Datalek en incidenten**

6.1 Verwerker zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 6 rapporteren aan Verwerkingsverantwoordelijke.

6.2 Zodra zich een incident met betrekking tot de verwerking van de Persoonsgegevens voordoet, heeft voorgedaan of zou kunnen voordoen, is Verwerker verplicht om Verwerkingsverantwoordelijke, nadat Verwerker daarvan kennis heeft gekregen, daarvan in kennis te stellen en daarbij alle relevante informatie te verstrekken. De in kennis stelling vindt direct (uiterlijk binnen 24 uur) nadat Verwerker kennis heeft gekregen van het incident plaats. Verwerker zal in alle relevante informatie verstrekken, waaronder in ieder geval informatie omtrent (1) de aard van het incident, (2) de (mogelijk) getroffen gegevens, (3) de geconstateerde en de vermoedelijke gevolgen van het incident, en (4) de maatregelen die getroffen zijn of zullen worden om het incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken.

6.3 Verwerker zal voor eigen rekening alle benodigde maatregelen treffen die nodig zijn om de (mogelijke) schade te beperken en zal Verwerkingsverantwoordelijke ondersteunen bij meldingen aan betrokkenen en/of autoriteiten.

6.4 Verwerker zal Verwerkingsverantwoordelijke te allen tijde zijn medewerking verlenen en zal de instructies van Verwerkingsverantwoordelijke opvolgen, met als doel Verwerkingsverantwoordelijke in staat te stellen een deugdelijk onderzoek te verrichten naar het incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het incident, waaronder begrepen het informeren van de Autoriteit Persoonsgegevens en/of de betrokkene zoals bepaald in artikel 6.8.

6.5 Onder “incident” wordt in elk geval het volgende verstaan:

(a) een klacht of (informatie)verzoek van een natuurlijk persoon met betrekking tot de verwerking van Persoonsgegevens door Verwerker;

(b) een onderzoek naar of beslaglegging door overheidsfunctionarissen op de Persoonsgegevens of een vermoeden dat dit gaat plaatsvinden;

(c) iedere ongeautoriseerde toegang, verwerking, verwijdering, verminking, verlies of enige vorm van onrechtmatige verwerking van de Persoonsgegevens;

(d) een inbreuk op de beveiliging en/of de vertrouwelijkheid, zoals uiteengezet in artikel 4 van deze Verwerkersovereenkomst, althans ieder ander incident, die/dat leidt (of mogelijk leidt) tot onopzettelijke of onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking van – of toegang tot – de Persoonsgegevens, of enige aanwijzing dat een dergelijke inbreuk zal plaatsvinden of heeft plaatsgevonden.

6.6 Verwerker zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om Verwerkingsverantwoordelijke van een onmiddellijke reactie over een incident te voorzien, en om effectief samen te werken met Verwerkingsverantwoordelijke om het incident af te handelen en zal Verwerkingsverantwoordelijke voorzien van een exemplaar van dergelijke procedures indien Verwerkingsverantwoordelijke daarom verzoekt.

6.7 Meldingen die worden gedaan op grond van dit artikel worden ogenblikkelijk gericht aan de in **Annex 3** opgenomen werknemer van Verwerkingsverantwoordelijke of, indien relevant, aan een andere door Verwerkingsverantwoordelijke tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekendgemaakte andere werknemer van Verwerkingsverantwoordelijke.

6.8 Verwerkingsverantwoordelijke zal, indien naar zijn oordeel noodzakelijk, betrokkenen, de Autoriteit Persoonsgegevens en andere derden informeren over incidenten. Het is Verwerker niet toegestaan informatie te verstrekken over incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is.

6.9 In concrete gevallen, en altijd na overleg met en schriftelijke toestemming van Verwerkingsverantwoordelijke, kan het mogelijk zijn dat de Verwerker de eerste melding van een incident aan de Autoriteit Persoonsgegevens doet. Over deze melding en over de voortgang daarvan, houdt de Verwerker Verwerkingsverantwoordelijke voortdurend op te hoogte.

**Artikel 7. Subverwerkers en EER**

7.1 Verwerker is slechts gerechtigd bij de uitvoering van haar werkzaamheden een derde in te schakelen indien Verwerkingsverantwoordelijke daarvoor voorafgaande schriftelijk toestemming heeft gegeven en indien voor betreffende derde bij de verwerking van de Persoonsgegevens dezelfde voorwaarden gelden als in deze Verwerkersovereenkomst omschreven

7.2 Met toestemming van Verwerkingsverantwoordelijke schakelt Verwerker bij de uitvoering van haar werkzaamheden de in **Annex 4** opgenomen subverwerker(s)/ derde(n) in.

7.3 Onverminderd een eventuele toestemming van Verwerkingsverantwoordelijke voor het inschakelen van een derde partij blijft Verwerker altijd volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een subverwerker.

7.4 Verwerker zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Verwerkingsverantwoordelijke, geen Persoonsgegevens verwerken of laten verwerken door hemzelf of door subverwerkers in landen buiten de Europese Economische Ruimte (“EER”) zonder een passend beschermingsniveau. Verwerker stelt de in **Annex 3** genoemde medewerker van Verwerkingsverantwoordelijke onmiddellijk schriftelijk op de hoogte van alle (geplande) permanente of tijdelijke doorgiftes van Persoonsgegevens naar een land buiten de EER. Verwerker zal pas uitvoering geven aan dergelijke (geplande) doorgiftes na schriftelijke toestemming van Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke heeft te allen tijde het recht om aanvullende voorwaarden te verbinden aan haar toestemming voor een dergelijke verwerking

**Artikel 8. Aansprakelijkheid**

8.1 Verwerker is, overeenkomstig het bepaalde in artikel 82 Avg, aansprakelijk voor alle schade of nadeel van Verwerkingsverantwoordelijke en betrokkenen die het gevolg zijn van (i) aan Verwerker toerekenbare schendingen van de wet- en regelgeving betreffende de verwerking van Persoonsgegevens, (ii) zijn werkzaamheden onder deze Verwerkersovereenkomst en/of (iii) de niet-nakoming door Verwerker van verplichtingen uit deze Verwerkersovereenkomst.

8.2 Verwerker vrijwaart Verwerkingsverantwoordelijke en stelt Verwerkingsverantwoordelijke schadeloos voor alle claims, acties, aanspraken van derden en voor eventuele boetes en dwangsommen van de Autoriteit Persoonsgegevens of een andere toezichthouder die het gevolg zijn van een schending van de wet- en regelgeving en in het bijzonder de Avg of een andere toerekenbare tekortkoming door Verwerker en/of diens subverwerkers of onderaannemers in de nakoming van de verplichtingen onder deze Verwerkersovereenkomst.

8.3 Verwerker draagt zorg voor afdoende dekking van de aansprakelijkheid.

**Artikel 9. Duur en beëindiging**

9.1 Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst heeft een looptijd die is gelijk aan van de Hoofdovereenkomst.

9.2 De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onlosmakelijk deel uit van de Hoofdovereenkomst. Beëindiging van de Hoofdovereenkomst, op welke grond dan ook (opzegging/ontbinding), heeft tot gevolg dat de Verwerkersovereenkomst eveneens op dezelfde grond beëindigd wordt (en vice versa), tenzij partijen in voorkomend geval anders overeenkomen.

9.3 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van deze Verwerkersovereenkomst gelden. Tot deze bepalingen behoren onder meer die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.

9.4 Verwerker informeert ogenblikkelijk Verwerkingsverantwoordelijke indien een faillissement dreigt dan wel surséance van betaling, zodat Verwerkingsverantwoordelijke tijdig kan beslissen de Persoonsgegevens terug te vorderen alvorens faillissement wordt uitgesproken.

**Artikel 10. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens**

10.1 Verwerker zal de Persoonsgegevens niet langer bewaren dan nodig is voor het in artikel 1 en Annex 1 genoemde doel. Indien de Persoonsgegevens niet meer nodig, zal Verwerker Verwerkingsverantwoordelijke raadplegen ter zake (de voortzetting van) het bewaren van die Persoonsgegevens.

10.2 Bij beëindiging van de Verwerkersovereenkomst zullen de Persoonsgegevens nog 6 maanden kosteloos voor Verwerkingsverantwoordelijke worden bewaard, tenzij er sprake is van een situatie als bedoeld in artikel 10.3. Na 4 maanden zal Verwerker een signaal geven aan Verwerkingsverantwoordelijke, dat de gegevens over 2 maanden worden vernietigd, tenzij Verwerkingsverantwoordelijke wenst dat de gegevens nog langer worden bewaard.

10.3 Aan het einde van de overeengekomen bewaartermijnen of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker, kosteloos, naar keuze van Verwerkingsverantwoordelijke, de Persoonsgegevens onherroepelijk vernietigen of teruggeven aan Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens onherroepelijk vernietigd of verwijderd zijn. Eventuele teruggave van de alle gegevens (waaronder de Persoonsgegevens) zal in een door Verwerkingsverantwoordelijke nader te bepalen gegevensformaat langs elektronische weg plaatsvinden. Indien teruggave, onherroepelijke vernietiging of verwijdering niet mogelijk zijn, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de Persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

10.4 Bij het einde van de Verwerkersovereenkomst zal Verwerker alle subverwerkers die betrokken zijn bij het verwerken van Persoonsgegevens op de hoogte stellen van de beëindiging van de Verwerkersovereenkomst. De verplichtingen uit artikel 10.2 en 10,3 zijn van overeenkomstige toepassing op deze subverwerker, en Verwerker zal waarborgen dat alle betrokken subverwerkers hieraan uitvoering zullen geven.

**Artikel 11. Algemene bepalingen**

11.1 De Verwerkersovereenkomst maakt onlosmakelijk en integraal onderdeel uit van de Hoofdovereenkomst. Bij tegenspraak tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen uit de Hoofdovereenkomst, prevaleren de bepalingen uit deze Verwerkersovereenkomst, tenzij uitdrukkelijk in deze Verwerkersovereenkomst anders is bepaald.

11.2 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

Aldus overeengekomen en in tweevoud ondertekend te …………op …….. datum

Namens Verwerkingsverantwoordelijke Namens Verwerker

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Handtekening) (Handtekening)

Naam: Naam rechtsgeldige vertegenwoordiger Naam: Naam rechtsgeldige vertegenwoordiger

Functie: Functie Functie: Functie

Datum: Datum Datum: Datum

**Annexen:**

1. Overzicht Persoonsgegevens, doeleinden, bewaartermijn en toegang
2. Overzicht beveiligingsmaatregelen
3. Contactgegevens
4. Lijst met Subverwerkers

**ANNEX 1: Overzicht Persoonsgegevens, doeleinden, bewaartermijn en toegang**

* **Welke persoonsgegevens zullen worden verwerkt in het kader van de Hoofdovereenkomst**

Verwerkingsverantwoordelijke zal Verwerker de volgende categorieën persoonsgegevens laten verwerken:

Invullen categorieën persoonsgegevens

Bijvoorbeeld gegevens van Cliënten:

Naam,

Adres

Telefoonnummer,

E-mailadres,

BSN/ cliëntnummer

Gezondheidsgerelateerde gegevens

Gegevens van de huisarts

* **Voor welke doeleinden worden de persoonsgegevens verwerkt**

De persoonsgegevens onder sub 1 worden uitsluitend gebruikt voor de levering van de verpleegkundige zorg, zoals omschreven in de Hoofdovereenkomst.

[beschrijven werkzaamheden / dienstverlening]

Bijvoorbeeld:

- Levering van de overeengekomen verpleegkundige zorg

- Bijhouden van het Cliëntendossier

* **Wat is de duur van de opslag**

De persoonsgegevens worden niet langer bewaard dan nodig voor de levering van de verpleegkundige zorg onder de Hoofdovereenkomst en facturering daarvan, één en ander in overeenstemming met artikel 10.

[ bewaartermijn aangeven]

Het gaat hier dus om de bewaartermijn van de onderaannemer en niet de bewaartermijn voor de zorgaanbieder.

**ANNEX 2: Beveiligingsmaatregelen**

Verwerker dient in ieder geval de volgende maatregelen te nemen:

* Verantwoordelijkheden voor informatiebeveiliging zijn toegewezen
* Wijzigingen in gegevens of in informatieverwerking worden uitsluitend uitgevoerd onder een procedure voor wijzigingsbeheer
* Verwerker heeft geselecteerde en gescreende medewerkers opgeleid en ervaring in het vakgebied security (informatie).
* Verwerker is gecertificeerd om professioneel haar security diensten en producten te kunnen aanbieden en ondersteunen richting opdrachtgever.
* Verwerker voert periodiek eigen interne audits uit om de benodigde bewijzen van conformiteit aan normen en eisen te waarborgen.
* Verwerker heeft adequate procedures over communicatie, support en beheer met opdrachtnemer afgestemd en handelt overeenkomstig.
* Vastgesteld beveiligingsbeleid dat ook is geïmplementeerd
* Fysieke maatregelen voor toegangsbeveiliging, inclusief organisatorische controle
* Inbraakalarm
* Maatregelen tegen kwaadaardige programmatuur
* Kluis voor opslag van gegevensbestanden
* Logische toegangscontrole m.b.v. 2-factor authenticatie, biometrie etc.
* Automatische logging van toegang tot gegevens, incl. een controleprocedure
* Controle van toegekende bevoegdheden
* Encryptie door versleuteling van persoonsgegevens tijdens verzending
* Encryptie door versleuteling van gegevensopslag
* Bedrijfscontinuïteitsbeheer, continuïteitsplannen
* Back-up (op (brand)veilige plaatsen) en herstel

Indien er sprake is van een elektronische uitwisseling van Persoonsgegevens dan zullen Partijen ook afspraken moeten maken over de volgende onderwerpen:

1. **Autorisatiebeleid**

Partijen moeten een autorisatiebeleid vaststellen voor toegang tot de Persoonsgegevens via het uitwisselingssysteem.

Het beleid is erop gericht de verwerking van Persoonsgegevens te beperken tot hetgeen noodzakelijk is in het kader van zorgverlening aan de Cliënt.

Het autorisatiebeleid omvat ten minste:

- richtlijnen met betrekking tot het verlenen van toegang tot Persoonsgegevens via het elektronisch uitwisselingssysteem, waaronder richtlijnen met betrekking tot mandatering van Verwerker;

- autorisatieprotocollen waarin de reguliere toegang tot de Persoonsgegevens wordt gebonden aan de rol van de Zorgaanbieder.

1. **Beveiligingsmaatregelen (Gedragscode EgiZ)**

***NEN-normen***

Partijendragen overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem dat zij gebruiken in het kader van de samenwerking uit deze Overeenkomst.

Een Zorgaanbieder draagt overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem.

Partijen werken met een zorgserviceprovider die is geautoriseerd op basis van overeenkomstig NEN 7512 vastgestelde criteria.

Partijen waarborgen dat de leverancier van het elektronisch uitwisselingssysteem voldoet aan de volgende voorwaarden:

a. een van de leverancier onafhankelijke organisatie heeft na onderzoek vastgesteld dat de leverancier en het systeem dat hij beheert voldoen aan het bepaalde in NEN 7510 en NEN 7512 en heeft die bevinding opgenomen in een door die organisatie ten behoeve van de leverancier opgesteld audit-rapport;

b. de in onderdeel a bedoelde vaststelling is niet langer dan vijf jaar geleden gedaan.

***Terminologie***

Bij het vastleggen van beleid, procedures en verantwoordelijkheden als bedoeld in NEN 7510, NEN 7512 of NEN 7513 in documenten, gebruiken Zorgaanbieder de termen en definities als genoemd in NEN 7510, NEN 7512 of NEN 7513.

***Verantwoording***

De Partijen leggen aan de leverancier van het elektronische uitwisselingssysteem op dat deze zich steeds vergewist van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van Persoonsgegevens, en dat deze zich verantwoord over de toepassing daarvan bij de inrichting en het gebruik van haar systemen.

***Identificatie en Authenticatie***

Partijen zorgen voor technische middelen van voldoende niveau voor het vaststellen en verifiëren van de identiteit van Partijen (en hun medewerkers) en de Cliënten

Voor identificatie en authenticatie van Partijen en medewerkers wordt gebruik gemaakt van passende middelen, zoals de UZI-pas of middelen met een vergelijkbaar beveiligingsniveau.

Bij het elektronisch uitwisselen tussen Partijen van Persoonsgegevens wordt gebruik gemaakt van het BSN.

In verband met de uitoefening van de voorafgaande toetsing van zorgovereenkomst door de Cliënt, zoals bedoeld in paragraaf 2 sub c, dient authenticatie van Cliënt met tenminste 2-factor authenticatie, zoals DigiD + sms-functie te worden gebruikt, zolang er nog geen algemeen beschikbare 2-factor authenticatie beschikbaar is voor patiënten/cliënten.

***Logging***

De Partijen dragen er zorg voor dat de logging van het uitwisselingssysteem voldoet aan het bepaalde in NEN 7513.

De Partijen bewaren de gegevens in de logging gedurende een termijn van tenminste vijf jaar vanaf het moment van het schrijven van de logregel.

De Partijen houden voorzieningen in stand waarmee zijzelf of de Cliënt de logging kan inzien.

De Partijen stellen een beleid vast met betrekking tot:

- de toegang tot de gegevens in de logging;

- het uitvoeren van een periodieke controle van de logging op onbevoegde raadplegingen;

- het uitvoeren van specifieke controles op raadplegingen die hebben plaatsgevonden in noodsituaties, en

- de te volgen procedure bij vermeend of geconstateerd misbruik en/of datalek.

**ANNEX 3: Contactgegevens**

Hier invoegen contactgegevens van de medewerkers van Verwerker en Verwerkingsverantwoordelijke waarmee contact dient te worden opgenomen in het geval van “incidenten”/datalekken.

In principe de functionaris voor de gegevensbescherming (FG)

**Aanspreekpunt Verwerkingsverantwoordelijke:      Aanspreekpunt Verwerker:**

Afdeling:

Naam:

Functie:

e-mailadres:

Telefoonnummer:

Vervanger:

Functie:

e-mailadres:

Telefoonnummer:

**Annex 4: Lijst met sub-verwerkers**