Achtergrond en doelen.

Achtergrond.
het protocol persoonsgegevens omvat een omschrijving van een verzameling van alle gegevens die de Marshoeve verzamelt en inzet tot het realiseren van de geleverde zorg. Daarnaast worden gegevens verzameld van medewerkers voor het realiseren van een kloppende salarisadministratie en personeelsdossier.
De beleidspunten sluiten aan en is gebaseerd op de Wet Bescherming Persoonsgegevens. (WBP zie bijlage 1).

Doel.
De veiligheid van gegevens van cliënt, medewerker en externe partij dusdanig te beschermen dat hierdoor geen schade kan ontstaan op welk gebied dan ook. Alle partijen een respectvolle behandeling te bieden omtrent de omgang met persoonlijke en mogelijk gevoelige informatie.

Toepassingsgebied
Het protocol persoonsgegevens is van toepassing op alle medewerkers, stagiaires en vrijwilligers aanwezig op de Marshoeve. Voor zowel het verwerken als inzien van persoonsgegevens. Het protocol is niet vrijblijvend en biedt alsmede verplichte kaders en richtlijnen omtrent de omgang en verwerking van persoonsgegevens.

Opzet protocol
het protocol omvat verschillende informatie omtrent omgang met persoonsgegevens.

1. Definities
2A. Verwerken persoonsgegevens zorg
2B. Verwerken persoonsgegevens financiële administratie
2C. Verwerken digitale systemen
3. Opslaan en beveiliging persoonsgegevens
4. Exporteren persoonsgegevens.
5. Handeling bij datalek.
6. Geheimhouding
7. Aansprakelijkheid
8. Teruggave en bewaartermijn
9. Bijlage en overige documentatie
10. Technische en organisatorische beveiligingsmaatregelen

Inleiding

De Marshoeve verleent zorg en begeleiding op locatie de Marshoeve te Dalmsholte. Om deze zorg te verlenen zijn wij genoodzaakt specifieke documenten in ontvangst te nemen van onze cliënten en medewerkers. Deze betreffen NAW, medische, psychisch/diagnostische en financiële gegevens. Gegevens worden noodzakelijk verwerkt voor het bieden van kwaliteitszorg. Gegevens worden maximaal 15 jaren bewaard met uitzondering van de financiële administratie. Deze wordt 7 jaar bewaard. De Bescherming van de persoonlijk gegevens zijn een recht van de cliënt en plicht als organisatie. Medewerkers in dienst bij de Marshoeve zijn betrokken bij de privacy en persoonlijke leefomgeving van de cliënt. Hierin dient ten alle tijden de privacy gewaarborgd te worden. Cliënten, medewerkers en vertegenwoordigers moeten zonder twijfel erop kunnen vertrouwen dat de persoonsgegevens veilig opgeslagen zijn. Daarnaast moeten zij erop kunnen vertrouwen dat de verwerking van de dergelijke gegevens op een zorgvuldige manier gebeurt. Het verzuimen van omgang vormen beschreven in dit protocol zal resulteren in een schending van de privacy van de persoon(en) in kwestie en een schending van de professionele integriteit van de medewerker van de Marshoeve. Het voorkomen van dergelijke situaties is van groot belang binnen de zorg en specifiek binnen de gezinnen waar de Marshoeve mee werkt.

Verwerken en verstrekken persoonsgegevens.

Het protocol dient ten alle tijden te worden opgevolgd. Richtlijnen beschreven in het protocol zijn verplicht en bieden medewerkers en cliënten de waarborging van veiligheid die zij mogen verwachten van de Marshoeve. Daarnaast zijn richtlijnen wettelijk bepaald en zullen deze nageleefd en gecontroleerd worden.
Het verstrekken van persoonsgegevens aan derden is alleen mogelijk indien vertegenwoordiger hier schriftelijk toestemming voor geeft. Normaliter zijn biologische of pleegouders vertegenwoordiger van een cliënt. Dit kan worden overgeheveld wanneer er sprake is van Onder Toezicht Stelling (OTS) of mentorschap of bewindvoering. In een dergelijke situatie is de Marshoeve niet gemachtigd om met ouders contact op te nemen over het delen van informatie aan de wettelijk vertegenwoordiger van een persoon.
Uitzondering van het verstrekken van cliënt gegevens aan derden zonder toestemming zijn:

a. Medewerkers werkzaam op of voor de Marshoeve
b. Zorgkantoor
c. Professionals die rechtstreeks betrokken zijn bij de zorgverlening. Denk aan psycholoog, psychiater, orthopedagoog.
d. Sociale verzekeringsbank, enkel ter controle van besteedde financiën.
e. Coöperatie Boer en Zorg
f. Federatie Landbouw en Zorg, enkel wanner er een 3-jaarlijkse audit plaatsvind.

Het verstrekken van medewerkers gegevens worden enkel in overleg met de desbetreffende medewerker gedaan. Enkele organisatie en personen hebben hierin een uitzondering. Noemende;

a. Directeur, teamleider en boekhouder de Marshoeve
b. Pensioenfonds
c. Arbodienst
d. Belastingdienst
e. Zorgverzekeraar
f. Extern administratiekantoor Bleijenberg

Verantwoording vastleggen persoonsgegevens

De Marshoeve verwacht dat haar medewerkers zorgvuldig met gevoelige informatie omgaan zoals beschreven in het protocol. Daarnaast hebben medewerkers de verplichting om personen zo goed mogelijk op de hoogte te stellen waar gegevens voor worden vastgelegd. Hierbij dienen een aantal richtlijnen te worden gevolgd.

- Persoonsgegevens worden zoveel mogelijk digitaal bewaard.
- Uitleg wordt gegeven aan wettelijk vertegenwoordiger van cliënt omtrent de verwerking van gegevens.
- ID kaart wordt gecontroleerd. Hiervan worden documentnummer, bsn en geboortedatum overgenomen. Er enkel een kopie gemaakt mits er gebruik wordt gemaakt van een ID – Cover.
- Persoonsgegevens worden niet onbeheerd achtergelaten. Laptop of pc zijn uitgeschakeld of vergrendeld. Dossiers zijn niet aanwezig op het bureau wanneer een medewerker niet aanwezig is; clean desk policy.
- Cliënt gerelateerde informatie zal alleen gedeeld worden middels werkmail, deze is volledig beveiligd en middels ONS.
- Cliënten dossiers worden bewaard in afgesloten ruimte.

1.Protocol verwerking persoonsgegevens.

1.Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en

Hebben de volgende betekenis:
1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens,

1.2 een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon
Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een

Dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegeven betrekking hebben;
1.6 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen;
1.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;
1.8 Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens ("**Datalek**"); 1.9 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens;

2A. Verwerken Persoonsgegevens

2.1A Personeel werkzaam op contractbasis bij de Marshoeve zal persoonsgegevens moeten verwerken voor de cliëntendossiers.

2.2A Cliëntendossiers mogen alleen volgende documenten bevatten; bsn nummer, Documentencode waarop het bsn is overgenomen, geboortedatum, woonadres vertegenwoordiger en cliënt, kopie zorgpas mits geen foto van de cliënt aanwezig is op deze pas.

2.3A Indien er foto's zichtbaar zijn dienen deze te worden afgedekt alvorens er een kopie wordt gemaakt.

2.4A Verwerken persoonsgegevens dient alleen te gebeuren met het getekende document; 3.2.2.2 verwerkersovereenkomst. Vertegenwoordiger en de Marshoeve dienen deze beiden te hebben ondertekend alvorens er documenten worden opgeslagen.

2B. Verwerken financiële administratie

2.1B Voor de verwerking van financiële administratie is er op de Marshoeve een boekhouder aangesteld. Deze samen met teamleider en directeur zijn gemachtigd financiële verwerkingsprogramma's en hulpmiddelen in te schakelen.

2.2B Het systeem dat wordt ingezet tot verwerking van de administratie is 'Snelstart'. Zowel het programma als online platform zijn beiden uitgerust met een wachtwoord.

2.3B Financiële administratie inclusief salarisadministratie worden door een derde partij gecontroleerd dan al niet opgesteld. Administratiekantoor Bleijenberg is aangesteld om deze functie uit te oefenen.

2.4B. Administratiekantoor Bleijenberg heeft toegang verkregen tot de administratie van de Marshoeve. Administratiekantoor Bleijenberg is enkel gemachtigd financiële gegevens te verzamelen en te verwerken met als doel het opstellen van salarisstroken, jaarcijfers en bijbehorende posten.

2.5B De Marshoeve kan hulp inschakelen voor financiële vraagstukken bij administratiekantoor Bleijenberg.

2.6B Gegevens verzameld vanuit de administratie omvatten NAW-gegevens. Deze worden gebruikt voor het verzenden van facturen.

2.7B Verzamelde gegevens van leveranciers omvatten NAW-gegevens ter verwerking van inkomende facturen.

2.8B Is er sprake van een rechtelijk vastgesteld bewindspersoon, dan zal de Marshoeve deze erkennen als wettelijk vertegenwoordiger van een cliënt. Facturen en overige financieel gegevens zullen enkel met deze persoon gecorrespondeerd worden. Ouders zijn in een dergelijke situatie niet gemachtigd om vanuit de Marshoeve financieel administratie omtrent de cliënt in te zien.

2C. Gebruik maken van digitale registratiesystemen.

2.1C digitaal systeem ONS van uitgever NEDAP is het programma waarin medewerkers van de Marshoeve hun werkzaamheden registreren. Daarnaast registreren zij de aanwezigheid van een cliënt. Deze gegevens worden door de boekhouder verzameld en financieel verwerkt.

2.2C ONS is inzichtelijk voor alle medewerkers op de Marshoeve. Uitzondering zijn vrijwilligers.

3. Opslaan en beveiliging persoonsgegevens.

3.1 het bestuur, noemende teamleider en directeur, dragen zorg voor een beveiligde online werkomgeving.

3.2. De online werkomgeving is vormgegeven middels een zakelijk mail account met bijpassende Cloud van waaruit gewerkt kan worden. Daarnaast zijn er laptops beschikbaar vanuit de Marshoeve en een externe opslag

(NAS) welke beveiligd is middels wachtwoord en virusscanner.
3.3 Persoonsgegevens dienen te worden gescand via scanner/printer op de Marshoeve. Het is niet mogelijk documenten thuis te scannen of op een dergelijke locatie. Documenten mogen niet de Marshoeve verlaten, tenzij schriftelijk anders overeengekomen tussen de Marshoeve en vertegenwoordiger cliënt.
3.4 Documenten worden opgeslagen op de NAS. Inloginstructies en wachtwoord tot deze externe schijf zijn door teamleider aangeboden aan het personeel.
3.5 Online is het mogelijk documenten te bewerken mits deze op de Cloud staan. Deze documenten mogen beslist niet naar privé mail e.d. worden verzonden.
3.6 Documenten welke online zijn bewerkt mogen alleen worden ingezien door collega's. Uitnodiging tot inzien mogen wederom alleen via werkmail worden verzonden.
3.7 USB-sticks waarop persoonsgegevens, van welke aard dan ook, worden opgeslagen dienen te zijn voorzien van een wachtwoord.
3.8 het is niet mogelijk documenten op privé computer of laptop op te slaan.

4. Exporteren Persoonsgegevens
4.1 Medewerker mag geen persoonsgegevens laten verwerken door andere personen en of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaand mijn toestemming te hebben verkregen van zorgvrager.
4.2 zorgvrager dient deze toestemming altijd schriftelijk aan te leveren. Toestemming via mail of papier zal beiden als rechtsgeldig worden bestempeld. Telefonische toestemming zal niet verwerkt worden door Zorgaanbieder.
4.3 Persoonsgegevens mogen zonder schriftelijke toestemming geen documenten verzenden naar andere instellingen van welke aard dan ook.
4.4 Dient een verzoek vanuit een overheidsinstantie zich om documentatie aan te leveren, dan dient wederom toestemming schriftelijk te worden aangeleverd mits dit rechtspraken e.d. niet hinderen.

5. Datalekken
5.1 Dient zich een datalek voor dan zal medewerker dit onmiddellijk melden bij werkgever of teamleider.
5.2 Werknemer dient een FOBO op te stellen waarin dienst handelen in detail worden vermeld. Ook moet er vermeld worden welke documentatie is gelekt en naar welke instanties of personen.
5.3 Werkgever/leidinggevende zal binnen 24 uur na een lek contact opnemen met vertegenwoordiger van de cliënt om aan te geven wat is er gebeurd. Daarnaast zal er vermeld worden dat er een FOBO is opgesteld en zijn vertegenwoordigers gemachtigd deze op te vragen.
5.4 na een datalek is er altijd een gesprek met de leidinggevende zodat herhaling op dergelijke situaties tot het minimum beperkt wordt.

6. Geheimhouding
6.1 Werknemer zal de door zorgvrager verstrekte gegevens geheimhouden, tenzij dit middels wettelijke verplichtingen niet mogelijk is.
6.2 Documenten dienen te worden opgeslagen zoals beschreven in paragraaf 3 of dienen te worden opgeslagen in de dossierkast.
6.3 Stagiaires en vrijwilligers zijn niet gemachtigd om in dergelijke documenten te kijken zonder voorafgaande toestemming van vertegenwoordiger.
6.4 Gegevens van zowel personeel als cliënten

vallen onder geheimhoudingsplicht. Het is daarom niet mogelijk contact te hebben met derden over de gegevens van eventuele cliënten of collega's.
6.5 worden er middels wettelijke brieven documenten omtrent een cliënt of werknemer opgevraagd dan zal de Marshoeve deze verlenen ongeacht de toestemming die eventueel niet verleend zal worden.
6.6 Alle gegevens omtrent een persoon die zorg ontvangt vallen onder de geheimhoudingsplicht. Het is mogelijk dergelijke informatie in te zetten als voorbeeld waarin personen aanwezig zijn buiten de Marshoeve om.

7. Aansprakelijkheid
8.1 Zorgaanbieder wordt verantwoordelijk gesteld indien de hiervoor beschreven afspraken niet of niet juist gehanteerd worden.
8.2 Zorgvrager en of budgethouder, zijn niet aansprakelijk voor aanspraken van betrokkenen of andere personen en organisaties waar zorgaanbieder de samenwerking mee is aangegaan of waarvan jij persoonsgegevens verwerkt, als dit het gevolg is van de zorgaanbieders onrechtmatig nalatig handelen.

8. Teruggave Persoonsgegevens en bewaartermijn.
9.1 Zorgdocumenten en dossier worden hebben een bewaartermijn van 15 jaren.
9.2 Persoonsgegevens zullen in deze periode in het dossier aanwezig blijven tenzij anders schriftelijk overeengekomen.
9.3 Zorgaanbieder zal persoonsgegevens vernietigen op het moment dat deze termijn is verstreken.
9.4 Op verzoek van zorgvragen kan zorgaanbieder documenten eerder vernietigen. Mocht hierna sprake zijn dat gegevens niet correct kunnen worden aangeleverd door de zorgaanbieder, dan is de zorgvrager hier verantwoordelijk voor.
9.5. In geval van een vroegtijdige vernietiging van documentatie vanuit de zorgaanbieder dient de zorgvrager hiervoor schriftelijk toestemmingen hebben gegeven, daarnaast ontvangt de zorgvrager een kopie van alle gegevens uit het dossier wanneer zij deze geschied te ontvangen. Uitzondering zijn documenten de wettelijke verplichting hebben tot een bewaartermijn van 15 jaar.

9. Bijlage en overige documentatie
10.1 Bijlage betreffende het protocol omvat het verwerkingsregister. Documentnummer; 3.2.2.4. Dit betreft een overzicht van verzamelde gegevens, het doeleinde en de wettelijke grondslag om gegevens op te slaan.
10.2 Bijlage betreffende verwerkersovereenkomst. Deze bijlage ontvangen vertegenwoordigers van ouders. Zij zullen ons machtigen middels dit formulier om documenten op de slaan en te verwerken. Documentnummer; 3.2.2.2.
Het social mediabeleid is beschreven in het protocol internet gebruik, documentnummer; 3.2.2.5.

Technische beveiligingsmaatregelen

☒ Up to date virusscanner

☒ Beveiligde USB- stick

☒ Unieke inlogcode computer

☒ Unieke inlogcode rapportagesysteem

☒ Tweetraps beveiliging email

☒ Versleutelde back up/harde schijf

☒ Geen documenten op privé computer

Organisatorische beveiligingsmaatregelen

☒ Clean desk policy

☒ Laptop niet onbemand achterlaten

☒ Verklaring omtrent gedrag medewerkers

☒ Juiste vernietiging oude documenten

☒ Protocol persoonsgegevens