Protocol data, privacy en klachtenprocedure

Inhoudsopgave

1 Datalekken. 5

1.1.1 Wat zijn 'datalekken'? 5
1.1.2 Categorieën datalekken 5
1.1.3 Overwegingen 6

1.2 Interne verantwoordelijken melding datalekken 6

1.3 Interne melding bij ontdekking van een datalek 7

1.4 Onderzoek door interne verantwoordelijke 7

1.5 Bestrijding datalek 7

2 Medewerking verstrekking gegevens omtrent het datalek 8

2.1 Beschikbaarheid personeel na ontdekking datalek 8

2.2 Beslissing melding datalekken 9

2.3 Melding datalekken aan de autoriteit Persoonsgegevens en/of betrokkenen. 9

2.4 Gevolgen meldingen datalekken 10

3 Privacy en dataverkeer. 11

3.1 Privacyregeling 11
3.1.1 Wat gebeurt er met mijn gegevens? 11

4 Dataverkeer akkoordverklaring 13

5 Dataverkeer 15

5.1 Qurentis 15

5.2 E-mail en Zivver 15

5.3 Siillo 16

5.4 Telefoongesprekken 16

5.5 Website 16

5.6 Facebook 16

5.7 C-iris 16

5.8 Aanwezigheidsapp 16

5.9 Beveiligingssysteem 17

6 Documentenbeheersing 18

6.1 Documenten bij start zorgvraag deelnemer. *18*
6.1.1 Welke documenten dienen aanwezig te zijn? 18
6.2 Waar zijn deze documenten terug te vinden? *18*
6.3 Wie draagt de verantwoordelijkheid? *18*

7 Documentenbeheersing m.b.t. verslaglegging ziektebeeld. **19**
7.1 Welke documenten dienen aanwezig te zijn? *19*
7.2 Waar zijn deze documenten terug te vinden? *19*
7.3 Wie draagt de verantwoordelijkheid? *19*

8 Documentbeheersing m.b.t. Begeleidingsplan. **19**
8.1 Welke documenten dienen aanwezig te zijn? *19*
8.2 Waar zijn deze documenten terug te vinden? *19*
8.3 Wie draagt de verantwoordelijkheid? *19*

9 Documentbeheersing m.bt. Evaluaties. **20**
9.1 Welke documenten dienen aanwezig te zijn? *20*
9.2 Waar zijn deze documenten terug te vinden? *20*
9.3 Wie draagt de verantwoordelijkheid? *20*

10 Documentbeheersing m.b.t. Signaleringsplan. **20**
10.1 Welke documenten dienen aanwezig te zijn? *20*
10.2 Waar zijn deze documenten terug te vinden? *20*
10.3 Wie draagt de verantwoordelijkheid? *20*

11 Documentbeheersing m.b.t. Indicaties. **20**
11.1 Welke documenten dienen aanwezig te zijn? *20*
11.2 Waar zijn deze documenten terug te vinden? *20*
11.3 Wie draagt de verantwoordelijkheid? *21*

12 Documentbeheersing m.b.t. MIC en MIM meldingen. **21**
12.1 Welke documenten dienen aanwezig te zijn? *21*
12.2 Waar zijn deze documenten terug te vinden? *21*
12.3 Wie draagt de verantwoordelijkheid? *21*

13 Documentbeheersing m.b.t. klachten. **21**

13.1 Welke documenten dienen aanwezig te zijn? *21*
13.2 Waar zijn deze documenten terug te vinden? *21*
13.3 Wie draagt de verantwoordelijkheid? *21*

14 Documentbeheersing m.b.t. informatie medewerkers **21**
14.1 Welke documenten dienen aanwezig te zijn? *21*
14.2 Waar zijn deze documenten terug te vinden? *22*
14.3 Wie draagt de verantwoordelijkheid? *22*

15 Documentbeheersing mb.t. dossier medewerkers. **22**
15.1 Welke documenten dienen aanwezig te zijn? *22*
15.2 Waar zijn deze documenten terug te vinden? *23*
15.3 Wie draagt de verantwoordelijkheid? *23*

16 Checklist ..... Fout! Bladwijzer niet gedefinieerd.

1 Datalekken.

1.1.1 Wat zijn ‘datalekken’?

Het ongeoorloofd of onbedoeld toegang geven tot persoonsgegevens is een datalek. Oftewel het benoemen van namen of andere informatie (per ongeluk) delen met personen die hier geen recht of reden toe hebben. Ook ongewenst kwijtraken, vernietigen, verwijderen of wijzigen van gegevens, wordt bestempeld als een datalek. Betrokken personen kunnen hier namelijk schade van leiden.

De algemene verordening gegevensbescherming (AVG) spreekt niet over het begrip ‘datalek’. De wet spreekt over ‘inbreuk in verband met persoonsgegevens’.

1.1.2 Categorieën datalekken

- Inbreuk op de vertrouwelijkheid

Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.

- Inbreuk op de integriteit

Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.

- Inbreuk op de beschikbaarheid

Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Datalekken kunnen op de simpelste manieren ontstaan;

- Verliezen van een USB-stick die niet versleuteld is;
- Het computersysteem dat gehackt is;
- E-mail die niet versleuteld of naar de verkeerde is verzonden.

1.1.3 Overwegingen

Zorgcentrum Het Leefhuis hecht waarde aan een goede beveiliging van haar (elektronische) systemen waarin persoonsgegevens zijn opgeslagen en worden verwerkt. Het valt desalniettemin nooit volledig te voorkomen dat er een datalek zal plaatsvinden.

Zorgcentrum Het Leefhuis is op grond van de AVG wet verplicht om (ernstige) datalekken te melden aan de Autoriteit Persoonsgegevens en aan de betrokkenen. Zorgcentrum Het Leefhuis wenst aan haar wettelijke verplichtingen te voldoen. Zorgcentrum Het Leefhuis heeft daarom een beleid geformuleerd om zo adequaat mogelijk te handelen. Indien er onverhoopt toch een datalek plaatsvindt.

1.2 Interne verantwoordelijken melding datalekken

1. Zorgcentrum Het Leefhuis heeft interne verantwoordelijkheden voor de verwerking van datalekken aangesteld die verantwoordelijk zijn voor de melding van het datalek.

   Deze verantwoordelijkheden zijn:

   a. Nikki Jöris

      Telefoonnummer: 0651882675

      E-mail: zorgcentrumhetleefhuis@outlook.com

   b. Indien Nikki Jöris niet bereikbaar is vanwege ziekte of vakantie:

      Maartje Jansen

      Telefoonnummer: 0640414211

      E-mail: maartje.leefhuis@outlook.com

   (Hierna te noemen: ‘interne verantwoordelijke’).

1.3 Interne melding bij ontdekking van een datalek

1. Degene die een datalek bij Zorgcentrum Het Leefhuis ontdekt, meldt dit per omgaande aan de interne verantwoordelijke.

2. Indien mogelijk, zorgt degene die het lek ontdekt heeft, er gelijktijdig voor dat de gelekte gegevens meteen op afstand worden gewist of ontoegankelijk gemaakt.

Is er bij voorbeeld sprake van een e-mail, verstuurd naar het verkeerde adres, benader de ontvanger. Vraag de desbetreffende om de e-mail te verwijderen en vraag om het bewijs van verwijderen (ook uit de prullenbak, zodat de mail definitief verwijderd is).

1.4 Onderzoek door interne verantwoordelijke

De interne verantwoordelijke onderzoekt onder meer:

- Of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden;

- Wie of welke afdelingen binnen de organisatie betrokken zijn bij het datalek;

- Of er een verwerker betrokken is bij het incident.

Dit wordt gecommuniceerd met het management en indien nodig worden andere medewerkers ook op de hoogte gesteld. Het onderzoeksrapport wordt meegenomen en verwerkt in de jaarlijkse organisatiebeoordeling.

1.5 Bestrijding datalek

De interne verantwoordelijke stopt het datalek indien dat nog mogelijk is en neemt de noodzakelijke maatregelen om het datalek zo goed mogelijk te bestrijden.

Ook stelt de verantwoordelijke de gevolgen vast aan de hand van de aard en de omvang van de gegevens die gelekt zijn en stelt vast wat de nadelige gevolgen van de betrokkenen kan zijn.

2 Medewerking verstrekking gegevens omtrent het datalek

De ontdekker/melder van het datalek biedt alle medewerking aan de interne verantwoordelijke door zo snel en zo goed mogelijk (schriftelijk) antwoord te geven op de volgende vragen:

- Wat is er gebeurd? (Omschrijving van het incident)
- Was het lek incidenteel of is het met bedachte rade tot uitvoering gebracht (denk aan gehackte gegevens)?
- Wanneer heeft het incident plaats gevonden? (Datum en tijd)
- Wanneer is het incident ontdekt?
- Wat voor gegevens (registers) zijn gelekt?
- Zijn de gegevens versleuteld? (Zo ja, hoe?)
- Was het mogelijk gegevens op afstand te wissen of ontoegankelijk te maken en is dat gebeurd?
- Wat zijn mogelijke gevolgen voor betrokkenen?
- Welke groep(en) personen is/zijn hierdoor getroffen? (Deelnemers, ouders, medewerkers).
- Zijn er al organisatorische of technische maatregelen ingezet n.a.v. het incident? Zo ja, welke.

2.1 Beschikbaarheid personeel na ontdekking datalek

De verantwoordelijke van de afdeling vanuit waar het datalek heeft plaatsgevonden alsook de ontdekker van het datalek en iedereen die vanuit hun functie of kennis in staat is om organisatorische en/of technische maatregelen te treffen om de gevolgen van het datalek te beperken, houden zich de eerste 24 uur na ontdekking van het datalek beschikbaar voor overleg met de interne verantwoordelijke en eventueel door haar aangewezen experts en voor het indien nodig uitvoeren van opgedragen werkzaamheden als gevolg van het datalek.

2.2 Beslissing melding datalekken

1. De interne verantwoordelijke beslist z.s.m. doch in elk geval binnen 60 uur na het ontdekken van het datalek (al dan niet in overleg met degene die het datalek heeft ontdekt en/of aangewezen experts) of het datalek dient te worden gemeld aan de Autoriteit Persoonsgegevens en/of de betrokkenen.

2. Een datalek wordt in principe altijd gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen.

3. Melding van het datalek gaat gepaard met beantwoording van de vragen zoals omschreven in onderdeel 6.

4. Een datalek dat gemeld is aan de Autoriteit Persoonsgegevens wordt eveneens gemeld aan de betrokkenen indien het een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, tenzij inmiddels passende maatregelen zijn genomen dat het hoge risico heeft afgewend.

2.3 Melding datalekken aan de autoriteit Persoonsgegevens en/of betrokkenen.

1. De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of betrokkene(n).

2. Melding geschiedt z.s.m. na de ontdekking en uiterlijk binnen 72 uur na ontdekking van het datalek.

3. Enkel de interne verantwoordelijke meldt het datalek aan de Autoriteit Persoonsgegevens en/of betrokkenen.

4. Als een werknemer het niet eens is met de beslissing van de interne verantwoordelijke, kan hij dit kenbaar maken aan de andere interne verantwoordelijke.

5. Indien daartoe verzocht, verleent een werknemer alle medewerking aan de verantwoordelijke om de getroffen personen conform artikel 34 AVG te kunnen informeren omtrent het datalek.

2.4 Gevolgen meldingen datalekken

1. Indien het datalek negatieve gevolgen heeft voor betrokkenen, dan doet de interne verantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken.

2. Afhankelijk van de aard en omvang van het datalek voor betrokkenen bepaalt de interne verantwoordelijke.

    a. Op welke wijze betrokken worden geïnformeerd (waaronder in ieder geval de mededelingen worden gedaan, welke soorten personen getroffen zijn, wat de mogelijke gevolgen zijn, welke maatregelen Het Leefhuis opneemt en welke wijze betrokkenen zelf schade kunnen voorkomen of beperken).

    b. Welke nazorg betrokkenen krijgen.

    c. Welke acties in het belang van de organisatie noodzakelijk zijn.

3. Indien een datalek heeft plaatsgevonden, ongeacht of deze gemeld is of niet, worden zo spoedig mogelijk adequate maatregelen getroffen om toekomstige gelijksoortige datalekken te voorkomen.

4. De interne verantwoordelijke voegt het onderzoeksrapport toe aan de organisatiebeoordeling.

3 Privacy en dataverkeer.

3.1 Privacyregeling

3.1.1 Wat gebeurt er met mijn gegevens?

3.1.1.1 Waar worden mijn persoonlijke gegevens voor gebruikt?

Het Leefhuis maakt gebruik van persoonlijke gegevens om deelnemers aan te duiden en gebruikt deze informatie bij het bieden van de juiste zorg. De persoonlijke gegevens zijn nodig om te communiceren over deelnemers en de bevindingen of communicatie bij de juiste persoon te noteren. Tevens dienen de persoonlijke gegevens ervoor om contacten te leggen en te onderhouden. Persoonlijke gegevens worden ook gebruikt voor betalingen, communicatie met de gemeente, SVB en het CIZ. De persoonlijke gegevens worden niet aan derden verstrekt. De deelnemer dient in alle zaken zelf zijn eigen gegevens aan derden te verstrekken, wanneer hiernaar gevraagd wordt. Het Leefhuis stelt zich niet verantwoordelijk voor de gegevens afkomstig van Het Leefhuis verstrekt aan derden door de deelnemer.

3.1.1.2 Waarom worden mijn persoonlijke gegevens gebruikt?

Om te kunnen communiceren over deelnemers op Het Leefhuis en de juiste zorg te kunnen bieden, is het gebruik van persoonlijke gegevens noodzakelijk. Deze gegevens worden ingezet om een dossier aan te maken en persoonlijke groei of stagnaties te kunnen noteren. Daarnaast worden persoonlijke gegevens gebruikt om betalingen te kunnen doen en te communiceren over de zorg die geboden wordt .

3.1.1.3 Hoe wordt er rekening gehouden met mijn privacy?

Er wordt rekening gehouden met de privacy van onze deelnemers doordat wij een code gebruiken om deelnemers aan te duiden. Er zal dus geen naam genoteerd of geschreven worden, maar een code gebruikt worden tijdens mail- en whatsappverkeer. Het Leefhuis heeft een beveiligd rapportage systeem dat een eigen privacy beleid in zich draagt. Hierin worden namen voluit geschreven zodat alle werknemers weten over welke persoon het gaat en zijn de gegevens binnen dit systeem beschermd. Het Leefhuis maakt gebruik van de Siillo app. Een app met een eigen beschermingsmechanisme, die berichten na 30 dagen automatisch verwijdert. Tevens dient deze app met een code of vingerafdruk geopend te worden en kunnen alleen werknemers deze app openen. In de aanwezigheidsapp wordt de volledige naam gebruikt om de aanwezigheid van de deelnemer te registreren. Op deze manier is bekend wie er aanwezig zijn tijdens eventuele calamiteiten en kunnen medewerkers iedere deelnemer die aanwezig is in veiligheid stellen. De aanwezigheidsapp heeft iedere werknemer op zijn of haar telefoon waarmee ingelogd wordt met persoonlijke inloggegevens. In de C-iris app worden de anonimiseringscodes van de deelnemers gebruikt om werknemers in te kunnen plannen bij individuele begeleiding. Deze app wordt alleen gebruikt door de

werknemers en is beveiligd met een persoonlijk wachtwoord. Het beveiligingssysteem is inzichtelijk voor de werknemers op de tablet die opgeborgen ligt op het kantoor. Het kantoor is tijdens de diensten dicht en op slot. Deze app kan geopend worden met een code die alleen de werknemers weten. De beelden van de camera's worden na iedere dienst verwijderd.

3.1.1.3.1 Waar ligt mijn eigen verantwoordelijkheid?

Wanneer er gegevens aan derden worden verstrekt, draagt de deelnemer of de verantwoordelijke van de deelnemer hier de verantwoording voor. Het Leefhuis verstrekt alleen op aanvraag van deelnemers of verantwoordelijke van de deelnemers, informatie met betrekking tot de deelnemer.

Naam: Handtekening:

Datum:

Wanneer u een handtekening plaatst gaat u akkoord met het regelement van Het Leefhuis omtrent het gebruik van persoonlijke gegevens. Te allen tijde kan deze toestemming opgeheven worden.

4 Dataverkeer akkoordverklaring

Wanneer u een handtekening plaatst, gaat u akkoord met het gebruiken van de beschreven gegevens voor het kunnen leveren van de juiste zorg. Wanneer u geen akkoord geeft, kan er geen zorg geleverd.

Persoonsgegevens	Handtekening voor akkoord
Persoonlijke gegevens doorgeven aan werknemers.	
Persoonlijke gegevens doorgeven aan SVB.	
Persoonlijke gegevens doorgeven aan CIZ.	
Persoonlijke gegevens doorgeven voor betalingen.	
Persoonlijke gegevens gebruikt in Qurentis.	
Persoonlijke gegevens doorgeven via mailverkeer middels een beveiligingscode.	
Persoonlijke gegevens doorgeven via telefoongesprekken middels een anonimiseringscode.	
Persoonlijke gegevens doorgeven aan werknemers.	
Foto's die gebruikt worden voor PR materiaal.	
Foto's die gebruikt worden voor Social Media.	
Video's die gebruikt worden voor PR Materiaal	
Video's die gebruikt worden voor Social Media.	

Informatieverstrekking voor opdrachten/werkstukken van stagiaires. Omschreven als deelnemer X.	
Video's voor opdrachten/werkstukken van stagiaires. Waarin de deelnemer te zien is.	
Foto's voor opdrachten/werkstukken van stagiaires. Waarin de deelnemer te zien is.	
Het gebruiken van voor en achternaam op aanwezigheidslijst i.v.m. calamiteitenplan en veiligheid.	
Het gebruiken van voor- en achternaam voor noodkaarten en cliëntenkaarten om snel contact op te kunnen nemen met de verantwoordelijke van de deelnemer.	
Er wordt akkoord gegeven om de volledige naam van de deelnemer in de aanwezigheidsapp te gebruiken.	
Het wordt akkoord gegeven om de volledige naam van de deelnemer in de c-iris app te gebruiken.	
Er wordt akkoord gegeven dat de deelnemer in beeld komt bij het beveiligingssysteem en deze beelden worden opgeslagen.	

Wanneer u een handtekening plaatst gaat u akkoord met het regelement van Het Leefhuis omtrent het gebruik van persoonlijke gegevens. Te allen tijde kan deze toestemming opgeheven worden.

5 Dataverkeer

Dataverkeer binnen Het Leefhuis met andere instanties, organisaties, verantwoordelijke van deelnemers of betrokkenen.
Binnen welke programma's vindt er dataverkeer plaats:

- Qurentis
- E-mail en Zivver
- Siillo
- Telefoongesprekken
- Website
- Facebook
- C-iris
- Aanwezigheidsapp
- Beveiligingssysteem

5.1 Qurentis

Via Qurentis worden alle ontwikkelingen per deelnemer bijgehouden. Qurentis heeft een eigen veiligheidssysteem die bijdraagt aan de regels van de nieuwe AVG wet. Persoonsgegevens worden in Qurentis genoteerd en kunnen ingezien worden door alle werknemers bij Het Leefhuis en de verantwoordelijke die een licentie hebben gekregen tot het inzien van hun gegevens. Binnen dit systeem worden ook documenten bewaard die informatie bevatten over de betreffende deelnemers, deze kunnen ook alleen ingezien worden door werknemers van Het Leefhuis en de verantwoordelijke met een licentie.

5.2 E-mail en Zivver

Via de email worden contacten gerealiseerd met de verantwoordelijke, gemeentes, instanties, organisaties en andere betrokkenen. E-mails met persoonlijke informatie worden verstuurd middels beveiligd programma Zivver, betrokkenen ontvangen per sms en/of email een code waarmee zij het bericht kunnen openen. Deze code is 5 minuten geldig en kan maar eenmaal gebruikt worden. Medewerkers hebben ieder een eigen inlogcode en wachtwoord vanuit Zivver, zij ontvangen daarnaast een sms met code om in te kunnen loggen. Tevens gebruikt Het Leefhuis de eerste letter van de voornaam en de eerste letter van de achternaam om deelnemers te anonimiseren.

5.3 Siillo
Siillo is een app die communicatie tussen werknemers mogelijk maakt. Siillo voldoet aan de privacy normen vanwege het feit dat berichten automatisch na 30 dagen worden verwijderd. Er kunnen geen schermopnames worden gemaakt van gesprekken en gegevens blijven niet bewaard.

5.4 Telefoongesprekken
Tijdens telefoongesprekken over deelnemers wordt er ook gebruik gemaakt van het benoemen van de eerste letter van de voornaam en de eerste letter van de achternaam om deelnemers te anonimiseren. Het Leefhuis werkt met een map algemeen, binnen deze map staan persoonsgegevens van deelnemers. De map is vergrendeld met een code en deze code wordt elk half jaar vernieuwd. De lijst met benoemingen per deelnemer is binnen deze map te vinden.

5.5 Website
Via de website kunnen de verantwoordelijke contact opnemen met Het Leefhuis via contactformulieren. De verantwoordelijkheid voor het benoemen van een naam ligt bij de verantwoordelijke. Verder staan er geen persoonsgegevens op de website vermeld.

5.6 Facebook
Het Leefhuis noteert geen namen bij berichten op Facebook.

5.7 C-iris
De c-iris app is een app voor de werknemers om het rooster digitaal in te kunnen zien zodat zij weten wanneer zij op welke dienst ingepland staan. De codenaam van de deelnemer wordt hierbij geregistreerd voor de ambulante en individuele begeleiding. De werknemer klokt bij iedere dienst in en uit. Zowel op de dagbesteding als bij ambulante- en individuele begeleiding.

5.8 Aanwezigheidsapp
De aanwezigheidsapp wordt gebruikt door de werknemers om de aanwezigheid van de deelnemers op de dagbesteding en ambulante- en individuele begeleiding te registreren. De aanwezigheidsapp maakt het mogelijk dat de aanwezigheid terug te zien is voor de administratie. In de app worden de volledige namen van de deelnemers gebruikt.

5.9 Beveiligingssysteem

Het beveiligingssysteem is een systeem met camera's en sloten op de deuren en ramen. Op deze manier kunnen wij de beveiliging waarborgen. De camera's hebben een bewegingssensor die alle bewegingen vastlegt. De medewerker krijgt hiervan een melding op de tablet en telefoon. Na iedere dienst worden de beelden verwijderd.

6 Documentenbeheersing

6.1 Documenten bij start zorgvraag deelnemer.

6.1.1 Welke documenten dienen aanwezig te zijn?

- Zorgovereenkomst.
- Voorwaarden Zorgcentrum Het Leefhuis.
- Medicatiebeleid.
- BEM formulier.
- Begeleidingsplan.
- Evaluatie begeleidingsplan.
- Machtiging medicatie.
- Privacyregeling.
- Dataverkeer.
- Privacyverklaring.
- Agressieprotocol
- RI&E
- Klachtenregeling
- Apothekerslijst
- Akkoord C-iris
- Akkoord Aanwezigheidsapp
- Akkoord beveiligingssysteem.

6.2 Waar zijn deze documenten terug te vinden?

Het dossier van de deelnemer staat in het softwareprogramma Qurentis en in de netwerk verbonden opslaglocatie Nas.

6.3 Wie draagt de verantwoordelijkheid?

Mentor draagt samen met ouders/verzorgers of de deelnemer de verantwoording voor het compleet maken van het dossier.

7 Documentenbeheersing m.b.t. verslaglegging ziektebeeld.

7.1 Welke documenten dienen aanwezig te zijn?

Alle verslagen die betrekking hebben op het ziektebeeld, eerdere zorgverlening of nieuwe inzichten.

7.2 Waar zijn deze documenten terug te vinden?

Dossier van de deelnemer in het softwareprogramma Qurentis en in de netwerk verbonden opslaglocatie Nas.

7.3 Wie draagt de verantwoordelijkheid?

Mentor draagt samen met ouders/verzorgers of de deelnemer de verantwoording voor het compleet maken van het dossier.

8 Documentenbeheersing m.b.t. verslaglegging ziektebeeld.

8.1 Welke documenten dienen aanwezig te zijn?

Starterspakket bij de aanmelding.

8.2 Waar zijn deze documenten terug te vinden?

Dossier van de deelnemer in het softwareprogramma Qurentis en in de netwerk verbonden opslaglocatie Nas.

8.3 Wie draagt de verantwoordelijkheid?

Mentor draagt samen met ouders/verzorgers of de deelnemer de verantwoording voor het compleet maken van het starterspakket.

9 Documentbeheersing m.b.t. Begeleidingsplan.

9.1 Welke documenten dienen aanwezig te zijn?

- Begeleidingsplan deelnemer ondertekend.

9.2 Waar zijn deze documenten terug te vinden?

Dossier van de deelnemer in het softwareprogramma Qurentis en de netwerk verbonden opslaglocatie Nas.

9.3 Wie draagt de verantwoordelijkheid?

Mentor draagt samen met ouders/verzorgers of de deelnemer de verantwoording voor het compleet maken van het dossier.

10 Documentbeheersing m.bt. Evaluaties.

10.1 Welke documenten dienen aanwezig te zijn?

- Evaluatie deelnemer ondertekend.

10.2 Waar zijn deze documenten terug te vinden?

Dossier van de deelnemer in het softwareprogramma Qurentis en de netwerk verbonden opslaglocatie Nas.

10.3 Wie draagt de verantwoordelijkheid?

Mentor draagt samen met ouders/verzorgers of de deelnemer de verantwoording voor het compleet maken van het dossier.

11 Documentbeheersing m.b.t. Signaleringsplan.

11.1 Welke documenten dienen aanwezig te zijn?

- Signaleringsplan (indien aanwezig) deelnemer ondertekend.

11.2 Waar zijn deze documenten terug te vinden?

Dossier van de deelnemer in het softwareprogramma Qurentis en de netwerk verbonden opslaglocatie Nas.

11.3 Wie draagt de verantwoordelijkheid?

Mentor draagt samen met ouders/verzorgers of de deelnemer de verantwoording voor het compleet maken van het dossier.

12 Documentbeheersing m.b.t. Indicaties.

12.1 Welke documenten dienen aanwezig te zijn?

- Indicatiestelling.
- Toewijzing indicatie vanuit gemeente of PGB.

12.2 Waar zijn deze documenten terug te vinden?

Dossier van de deelnemer in het softwareprogramma Qurentis en de netwerk verbonden opslaglocatie Nas.

12.3 Wie draagt de verantwoordelijkheid?
Mentor draagt samen met ouders/verzorgers of de deelnemer de verantwoording voor het compleet maken van het dossier.

13 Documentbeheersing m.b.t. MIC en MIM meldingen.
13.1 Welke documenten dienen aanwezig te zijn?
- MIC meldingen.
- MIM meldingen.
- Bijna incidenten.

13.2 Waar zijn deze documenten terug te vinden?
In het dossier van de deelnemer of medewerker (kan ook beiden) binnen het softwareprogramma Qurentis en binnen Solopartners bij een ernstig incident.

13.3 Wie draagt de verantwoordelijkheid?
De begeleider waarbij het betreffende incident heeft plaatsgevonden draagt volledige verantwoordelijkheid voor de beschrijving en aanmelding van het incident. Het management is verantwoordelijk voor het bespreken van het incident en het ondernemen van actie.

14 Documentbeheersing m.b.t. klachten.
14.1 Welke documenten dienen aanwezig te zijn?
- Klachtenmeldingen vanuit deelnemers, ouders of verzorgers.

14.2 Waar zijn deze documenten terug te vinden?
Op de website van Zorgcentrum Het Leefhuis, bij de knop ‘klacht indienen’.

14.3 Wie draagt de verantwoordelijkheid?
Het management draagt alle verantwoordelijkheid voor de klachten m.b.t. Zorgcentrum Het Leefhuis.

15 Documentbeheersing m.b.t. informatie medewerkers.
15.1 Welke documenten dienen aanwezig te zijn?
- Protocollen
- Artikelen

- CAO gehandicaptenzorg
- Draaiboeken
- Medicatiebeleid
- Meldcode huiselijk geweld
- Protocol seksueel grensoverschrijdend gedrag
- Werkvoorwaarden
- Functieprofiel
- Begeleidingsprofiel
- Tevredenheidsmeting
- Verantwoordelijkheden
- Aan te leveren gegevens
- Wat te doen bij een klacht
- Wat te doen bij agressie

15.2 Waar zijn deze documenten terug te vinden?

De documenten zijn terug te vinden in het mapje ‘medewerkers’ in het NAS en er is een map gemaakt met belangrijke protocollen en begeleidingsrichtlijnen.

15.3 Wie draagt de verantwoordelijkheid?

De medewerkers dragen zelf de verantwoordelijkheid om op de hoogte te blijven van de werkwijze, nieuwe inzichten en veranderingen binnen Zorgcentrum Het Leefhuis. Binnen de vergadering worden vernieuwingen steeds besproken en behandeld.

16 Documentbeheersing mb.t. dossier medewerkers.

16.1 Welke documenten dienen aanwezig te zijn?

- VOG
- Diploma’s
- Cursussen
- Functieprofiel
- Begeleidingsprofiel
- BHV diploma
- Contract
- Functioneringsgespreksverslag
- Functioneringsformulier
- SKJ-pas indien aanwezig

16.2 Waar zijn deze documenten terug te vinden?

De documenten zijn terug te vinden in het dossier van de medewerker in het softwareprogramma Qurentis en in de netwerk verbonden opslaglocatie Nas.

16.3 Wie draagt de verantwoordelijkheid?

De medewerkers dragen samen met het management de verantwoordelijkheid voor het compleet maken van het dossier en in het Nas.