

- **Toegang tot persoonsgegevens:**

Hier wordt benoemd welke gebruikers, andere personen, of instanties toegang hebben.

Toepassing vindt plaats op basis van de *Algemene Toegangsregeling*:

Overeenkomstig artikel 9 van het reglement hebben, onverminderd eventuele wettelijke voorschriften ter zake, slechts toegang tot de persoonsgegevens de beroepsbeoefenaar die deze gegevens heeft verzameld of diens waarnemer.

Ook anderen werkzaam binnen Amarant dienen toegang te hebben tot persoonsgegevens opgesteld door een andere beroepsbeoefenaar, indien zij deze persoonsgegevens nodig hebben voor het uitoefenen van hun taak. De Raad van Bestuur is als verantwoordelijke geen gebruiker in de zin van het reglement. Een bestuurder heeft alleen toegang tot de registratie indien dit gezien zijn verantwoordelijkheid noodzakelijk is. Slechts bij een interne verstrekking kan aan Amarant niet-herleidbare persoonsgegevens worden verstrekt, bijvoorbeeld om de kwaliteit van de zorg te toetsen. Het verschaffen van herleidbare persoonsgegevens is alleen mogelijk met toestemming van de betrokkene.

Beheerders die niet als directe beroepsbeoefenaar zijn aan te merken hebben uitsluitend toegang tot de betrokkene persoonsgegevens voor zover dit binnen beheer noodzakelijk is. Stagiaires zijn geen gebruiker in de zin van het reglement. Zij mogen alleen, na toestemming van de werk- c.q. stagebegeleider, het deeldossier raadplegen dat betrekking heeft op de opleiding waartoe de stagiaire wordt opgeleid.

- **Gebruiker(s):**

Gebruikers zijn verantwoordelijk voor een juiste verslaglegging en raadpleging. En ook voor het bewaren van dossiers die zij in verband met hun taakuitoefening aanleggen. Zij gebruiken de registratie voor de omschreven doelen.

- **Bevoegdheid per gebruiker:**

Gegevens kunnen geraadpleegd worden door betrokkenen voor zover van belang in de beroepsuitoefening van deze, dit ter beoordeling van de beheerder. Géén toestemming hoeven clustermanager, districtmanager en klachtencommissie. Autorisaties als invoeren, muteren, corrigeren, aanvullen en vernietigen, gebeurt onder verantwoordelijkheid van de beheerder. Per bevoegdheid worden de verschillende gebruikers vermeld.

Voor hen kunnen de volgende twee bevoegdheden van toepassing zijn:

Bevoegdheid 1: raadplegen, invoeren (schrijven), wijzigen (corrigeren, muteren), toevoegen en verwijderen en vernietigen);

Bevoegdheid 2: raadplegen (inzien, lezen).

- **Inzage derde(n):**

Vastgelegd is wie recht op inzage heeft in het dossier of onderdeel, bijvoorbeeld overheid en anderen voor zover hierop een wettelijke verplichting rust.

- **Looptijd:**

Voor onbepaalde tijd.

- **Bewaartermijn(en):**

Conform hoofdstuk XI reglement

- **Beveiliging:**

Registratie dient beveiligd te zijn.

Beveiliging geautomatiseerde registraties: het hoofd cliëntenadministratie ziet toe op het handhaven van de beveiligingsprocedures voor het geautomatiseerde deel en treedt op als contactpersoon.

Beveiliging *niet* geautomatiseerde registraties: de clustermanager ziet toe op het handhaven van de beveiligingsprocedures voor het niet-geautomatiseerde deel van de registratie. Deze registraties worden in een afsluitbare, brandwerende (dossier)kast bewaard in een afsluitbare ruimte. De bewaarplaats dient te worden aangegeven.

- **Wijzigingsdatum:**

Dit is het moment dat dit onderdeeloverzicht is bijgesteld, geactualiseerd en opnieuw is vastgesteld.

- **Houder van de registratie:**

De Raad van Bestuur is houder van de registratie en heeft geen toegang tot de registratie, tenzij dit noodzakelijk is binnen zijn eindverantwoordelijkheid als houder.