Een onderzoek naar de privacy van patiënten bij Altrecht Aventurijn

Bijlages

Student: Roos Hartings
Studentnummer: 2081668
Opleiding: Juridische Hogeschool Avans - Fontys

Stageverlener: Altrecht Aventurijn
Afstudeermentor: Mw. E. Doze

Eerste afstudeerdocent: Mw. M. Kok
Tweede afstudeerdocent: Mw. M. van Bree/ Mw. L. Berkel

Datum: 28 mei 2017
Afstudeerperiode: Februari 2017 – Juni 2017

Bijlages:

1. Interview 13 April 2017
2. Handleiding omgaan met cliëntgegevens, 2014
3. Toestemmingsverklaring Altrecht Aventurijn
4. Richtlijn Uniform Patiëntendossier (UPD), 2015
5. Toestemmingsformulier huisarts
6. Informatie delen met de gemeente, informatieblad
7. Protocol informatiebeveiliging
8. Protocol melden datalek

Interview

Datum: Donderdag 13 april

Interviewer: Roos Hartings (RH)

Participanten: Elsa Doze (ED), Joris van Nesselrooij (JN), Anne-Berit Harmsen(AH)

Doel: De protocollen en werkinstructies zijn doorgenomen, echter dat heeft nog wat vragen opgeroepen over het gevoerde beleid bij Altrecht Aventurijn. Door middel van deze interviews worden de resterende vragen over de praktijk beantwoord.

RH: Altrecht Aventurijn hanteert toestemmingsformulieren voordat persoonsgegevens worden gedeeld met andere partijen. Bij de formulieren worden de volgende partijen genoemd; huisarts, school, schoolarts, CIZ en Jeugdzorg, is dit volledig?
AH : Ja, dit zijn alle partijen waarbij wij om expliciete toestemming vragen.
RH: Wat is het CIZ?
JN: Het CIZ staat voor Centrum Indicatie Zorg. Het CIZ beoordeelt onafhankelijk of burgers recht hebben op zorg via de Wet langdurige zorg. Dit gebeurt op basis van uniforme en objectieve criteria, zodat de beoordeling overal in het land hetzelfde is. Deze criteria zijn een vertaling van de richtlijnen van het ministerie van VWS. Hiervoor hebben zij het zorgdossier nodig, om tot een goede indicatie te komen.

RH: Klopt het dat jullie de eventuele toestemming voor het delen van persoonsgegevens met naasten van patiënten niet schriftelijk vastleggen?
ED: Dit wordt vaak mondeling met de patiënt besproken en niet schriftelijk vastgelegd.

RH: Is iemand weleens zo verward, dat het niet mogelijk is om toestemming te vragen?
ED: Dit komt zelden voor. Wanneer iemand wordt opgenomen worden er geen gegevens gedeeld totdat iemand wel ‘’helder’’ genoeg is deze toestemming te verlenen.

RH: Zijn er verder nog partijen, waarmee persoonsgegevens worden gedeeld, maar die niet zijn opgenomen in de toestemmingsformulieren?
ED: De zorgverzekeraars, de gemeente (voor de financiering van de jeugd) en justitie.

RH: Wanneer worden de toestemmingsformulieren getekend?
AH: Bij het intakegesprek met de regiebehandelaar.
RH: Zijn er weleens gevallen waarbij er geen toestemmingsformulier wordt getekend?
ED: Bij mensen met een erg laag IQ (op de WIR afdeling), die niet onder curatele zijn gesteld. Wanneer mensen extreem in de war zijn, maar het essentieel is, dat persoonsgegevens worden gedeeld. Deze laatste situatie komt zelden voor.
RH: Bij de categorie die wel onder curatele is gesteld, tekent de wettelijk vertegenwoordiger?
JH: Ja, dat klopt.
RH: Heeft een groot aantal patiënten van de WIR afdeling geen wettelijk vertegenwoordiger?
JH: Ja

RH: Jullie hanteren verschillende informatiesystemen, die toegang verlenen voor medewerkers om bij patiëntengegevens te komen. Wanneer worden deze toegang gegeven?
JN: Nieuwe medewerkers krijgen wachtwoorden en gebruikersnaam. Alleen medewerkers die contact hebben met patiënten, krijgen toegang tot de zorgdossiers.
RH: Hiermee bedoel je het EPD? *(het dossier)*
JN: Ja

RH: Wat voor gegevens zitten er bijvoorbeeld in het EPD?
ED: laboratoriumuitslagen, medicatiegegevens en aantekeningen van psychiaters. Over de inhoud van de EPD in nog het één en ander te vinden in het kwaliteitsstatuut.

RH: Kan de patiënt hier zelf inkijken?
AH: Nee, alleen specialisten die betrekking hebben op de zorgverlening van die patiënt hebben inzage.

RH: Daarnaast hanteren jullie voor de medicatie een eigen informatiesysteem (EVS). Hoe werkt het feit dat apothekers hier ook toegang tot hebben?
AH: Zij kunnen hier meldingen in verwerken. Daarnaast zien zij welke medicatie onze specialisten voorschrijven, die zij dan moeten verstrekken. Zij voeren onze zorg uit.
RH: Hierbij hebben zij geen toegang tot andere zorginformatie behalve de medicatie?
AH: Dit is correct.

RH: Wanneer er geen toestemming wordt gegeven, geven de specialisten dan ook geen toestemming?
ED: Dit is ons beleid, en dat wordt ook gehandhaafd. Wanneer er geen toestemming is, delen we geen informatie met bijvoorbeeld de huisarts.

RH: Bij de intake met een eventuele nieuwe patiënt, worden er dan BSN-nummers geregistreerd?
AH: Ja dit klopt.

RH: Uit de protocollen, maak ik op dat er bij Altrecht Aventurijn geen functionaris voor gegevens bescherming werkzaam is, is dit correct?
ED: Dat klopt, wij hebben geen medewerker voor deze functie.

RH: Hoeveel medewerkers werken er bij Altrecht Aventurijn?
ED: Rond de 400 medewerkers.

RH: Jullie maken gebruik van EPD's, hiervoor geldt een bewaartermijn van 15 jaar. Uit jullie protocollen maak ik op dat jullie je hiervan bewust zijn. Is er al beleid over de vernietiging van EPD's?
ED: Wij hebben hiervoor nog geen beleid gemaakt.

RH: Wordt er gebruik gemaakt van de algemene voorwaarden door de SER?
JN: Ja, deze worden bij de intake aan patiënt overhandigd. Hierdoor kunnen zij een beeld vormen van de zorgverlening.

servicebedrijf Informatisering, afdeling InformatieBeheer.

Deze handleiding is een beknopte versie van het protocol Omgaan met Cliëntgegevens zoals dit door Altrecht is opgesteld en wordt gehanteerd. De volledige tekst van het protocol is te vinden op ManualMaster, Protocol Omgaan met Cliëntgegevens.

Inhoudsopgave

1 Rechten van de cliënt

1.1 Verzoek tot inzage of kopie door cliënt

actoren: centraal cliëntenarchief
(laatst bekende) hoofdbehandelaar of afdelingspsychiater
secretariaat (laatste bekende) hoofdbehandelaar of afdelingspsychiater

Cliënten hebben recht op inzage in hun dossier. Dat behelst zowel het papieren dossier (indien aanwezig), het elektronisch patiëntendossier (Psygis Quarant), maar ook gegevens die in andere systemen zijn opgeslagen, zoals ROM-gegevens (NetQ), Medicatie (EVS) en eHealth (MijnTherapie), al is deze laatste per definitie inzichtelijk voor de cliënt.

Enkele regels:

1. Het verzoek tot inzage tijdens de behandeling kan zonder schriftelijk verzoek en legitimatie rechtstreeks met de behandelaar worden afgestemd.
2. Het verzoek tot inzage na behandeling of voor het verkrijgen van een kopie van dossiermateriaal moet altijd schriftelijk worden gedaan.
3. Het verzoek moet altijd ondertekend worden door de cliënt of, indien van toepassing, zijn/haar wettelijk vertegenwoordiger.
4. Bij het verzoek moet een kopie van een legitimatiebewijs worden meegestuurd (om de ondertekening van het verzoek te kunnen controleren). Deze kopie mag niet in het EPD worden gehangen[1]

Werkwijze:
Cliënten die actueel in behandeling zijn, kunnen het verzoek rechtstreeks indienen bij hun behandelaar.
Cliënten die niet meer in behandeling zijn, kunnen hun verzoek richten tot het Centraal Cliënten Archief.
Wanneer de aanvraag bij een andere afdeling binnenkomt, moeten zij het verzoek naar het archief doorsturen.

Het Centraal Cliënten Archief
gaat na welke gegevens van de cliënt binnen Altrecht geregistreerd zijn (op papier/elektronisch) en verzamelt deze.
stuurt het verzamelde materiaal ter beoordeling en afhandeling naar de laatst bekende behandelaar (indien nog werkzaam bij Altrecht) of naar de afdelingspsychiater van de laatst bekende afdeling.

De behandelaar of afdelingspsychiater
bekijkt of het verzoek aan alle regels voldoet en bepaalt of het dossier inderdaad ingezien of gekopieerd mag worden (er zijn enkele gronden waarop het verzoek afgewezen kan worden: zie Protocol Omgaan met Cliëntgegevens).
In geval van een verzoek om inzage maakt de afdelingspsychiater of de laatst bekende behandelaar een afspraak voor inzage met de cliënt. Voor inzage in het EPD kan de noodknop worden gebruikt o.v.v. “Ter inzage voor cliënt”.
In geval van een verzoek om kopie draagt de afdelingspsychiater of laatst bekende behandelaar het verzoek ter afhandeling over aan het secretariaat van de afdelingspsychiater of behandelaar. Het printen van EPD-materiaal is een lastige en tijdrovende klus. Het is aan te raden om in overleg met cliënt en behandelaar een keuze te maken van welk deel de cliënt een print wil hebben.

Na het maken van een kopie of de inzage wordt het dossier en het originele verzoek retour gestuurd naar het Centraal Cliënten Archief.

[1] Zie 3.4 Pasfoto"s in het EPD"

Alle correspondentie en relevante stukken aangaande het verzoek tot inzage of kopie worden door het Centraal Cliënten Archief in het papieren dossier bewaard of ingescand in het EPD.

Vergoeding kopiekosten
Sinds juli 2011 is het zg. Tientjesbesluit (uit de guldentijd) afgeschaft. Cliënt wordt geen bedrag meer in rekening gebracht voor administratietijd, verzend- en kopieerkosten.

1.2 Recht op correctie/verwijdering en/of aanvulling door een cliënt[2]

actoren: behandelaar/afdelingspsychiater
centraal cliëntenarchief
servicebedrijf informatisering

Wanneer een cliënt nog in behandeling is kan de behandelaar ter plekke beoordelen en de gevraagde acties uitvoeren, eventueel met ondersteuning van de Servicedesk. Het verzoek van de cliënt moet ingescand worden in het EPD in map 7 om latere misverstanden te voorkomen.

Enkele regels:
1. Het verzoek tot correctie van dossiermateriaal moet altijd schriftelijk, ondertekend door de cliënt of diens vertegenwoordiger, worden ingediend, met een omschrijving van het deel waar het om gaat.
2. Het verzoek wordt ingescand in het EPD.
3. Bij het verzoek moet een kopie van een legitimatiebewijs worden meegestuurd.
4. Het verzoek moet worden gericht aan de betreffende behandelaar of, wanneer deze niet meer bij Altrecht werkt, de afdelingspsychiater van de laatst bekende afdeling. Deze vraagt indien van toepassing het papieren dossier op uit het centrale cliëntenarchief of gebruikt de noodknop om het EPD te benaderen o.v.v. “Beoordeling Verzoek om informatie van derden, om vernietiging, om Inzage, Kopie of Correctie, na uitschrijving”.

Werkwijze:
De behandelaar of afdelingspsychiater kijkt of het verzoek aan de regels voldoet. D.w.z. het te corrigeren/te verwijderen dossier- of tekstgedeelte moet daadwerkelijk feitelijke onwaarheden bevatten die correctie/verwijdering rechtvaardigen.

Correctie/aanvulling in een afgesloten papieren dossier:
de behandelaar of afdelingspsychiater voegt de correctie/aanvulling toe en stelt de cliënt er schriftelijk van op de hoogte dat aan het verzoek is voldaan. Indien niet aan het verzoek wordt voldaan zal de behandelaar of afdelingspsychiater dit schriftelijk aan cliënt onderbouwen[3]. Het originele verzoek, het bericht aan de cliënt over de uitvoering er van, worden tezamen met het dossier terug gestuurd aan het archief.

Vernietiging van een deel van een afgesloten papieren dossier:
de behandelaar of afdelingspsychiater verwijdert het te vernietigen dossierdeel en stelt de cliënt er schriftelijk van op de hoogte dan aan het verzoek is voldaan. Indien niet aan het verzoek wordt voldaan zal de behandelaar of afdelingspsychiater dit schriftelijk aan cliënt onderbouwen. Het originele verzoek en het eventueel te vernietigen materiaal worden tezamen met het dossier naar het centraal cliëntenarchief teruggestuurd. Het centraal Cliëntenarchief zorgt voor de vernietiging van de daarvoor aangeboden dossierstukken.

Correctie/verwijdering van een deel van een afgesloten EPD:

[2] Wanneer de cliënt nog in behandeling is kan de behandelaar ter plekke beoordelen en uitvoeren, eventueel met ondersteuning van de Servicedesk. Het verzoek van de cliënt moet ingescand worden in het EPD in map 7 om latere misverstanden te voorkomen.

[3] Indien de behandelaar of afdelingspsychiater het verzoek niet wenst in te willigen, kan de cliënt een klacht indienen volgens het geldende klachtenprotocol

de behandelaar of afdelingspsychiater stuurt het originele verzoek terug aan het archief met het bericht dat de correctie of verwijdering uitgevoerd kan worden. Het centraal cliëntenarchief voert de gevraagde aanpassing in het EPD uit in overleg met de servicedesk en stuurt de behandelaar of afdelingspsychiater een schriftelijke bevestiging met daarop datum en tijd van de correctie/verwijdering of aanvulling. Dit schrijven kan worden gebruikt om de cliënt in kennis te stellen dat aan diens wens voldaan is. Indien niet aan het verzoek wordt voldaan zal de behandelaar of afdelingspsychiater dit schriftelijk aan cliënt onderbouwen.

Na de correctie/aanvulling of verwijdering worden alle correspondentie en relevante stukken van cliënt en behandelaar aangaande het verzoek conform de wettelijke bewaartermijn in het centraal Cliëntenarchief archief bewaard c.q. door de archivaris ingescand in het EPD, map 7, Correspondentie.

1.3 Vernietigen van papieren en digitaal dossier, op verzoek van cliënt

actoren: centraal cliëntenarchief
psychiater-directeur
secretariaat psychiater-directeur
servicebedrijf informatisering

Enkele regels:

1. Het verzoek tot vernietigen van dossiermateriaal moet altijd schriftelijk worden gedaan.
2. Het verzoek moet altijd ondertekend worden door de cliënt of, indien van toepassing, zijn/haar wettelijk vertegenwoordiger. Dit verzoek wordt ingescand in het EPD.
3. Bij het verzoek moet een kopie van een legitimatiebewijs worden meegestuurd (om de ondertekening van het verzoek te kunnen controleren).

   NB: Deze kopie wordt door het Centraal Cliënten Archief in een aparte brandkast bewaard, tezamen met het verzoek om vernietiging. Een kopie van het WID mag niet in het EPD of papieren dossier worden opgeslagen (zie ook: Pasfoto"s in het EPD)..

Werkwijze:

Het verzoek kan door de cliënt rechtstreeks worden gestuurd naar het Centraal Cliënten Archief. Wanneer de aanvraag bij een andere afdeling binnenkomt moet deze de aanvraag naar het archief doorsturen.

Het Centraal Cliënten Archief
- gaat na welke gegevens van de cliënt bij Altrecht aanwezig zijn en verzamelt deze (incl. melding van evt. EPD).
- stuurt het verzamelde materiaal ter beoordeling naar de psychiater-directeur.
- wanneer cliënt geen gebruik maakte van het formulier van de Altrechtsite, wordt deze alsnog aan de cliënt toegestuurd, met het verzoek deze alsnog in te vullen en getekend terug te sturen[4].

De psychiater-directeur (van de divisie)
- laat de cliënt schriftelijk weten dat diens verzoek in behandeling genomen is.
- bekijkt of het verzoek aan alle regels voldoet en bepaalt of het dossier inderdaad vernietigd mag worden (er zijn enkele gronden waarop het verzoek afgewezen kan worden (zie Protocol Omgaan met Cliëntgegevens).
- bepaalt of het dossiermateriaal geheel of gedeeltelijk wordt vernietigd.

[4]Het formulier van de Altrechtsite bevat de tekst, dat cliënt bekend is met het feit dat de vernietiging van de gegevens een eventuele klachtbehandeling aanmerkelijk zal bemoeilijken. Wanneer de gegevens vernietigd zullen zijn kan de bewijslast in elk geval niet meer bij onze instelling c.q. bij een van onze medewerkers worden neergelegd. Dit geldt ook wanneer de cliënt een gerechtelijke procedure tegen ons zou aanspannen.

ondertekent onderaan het verzoek van cliënt of er wel of geen bezwaar bestaat om het materiaal te vernietigingen en stuurt het originele verzoek en de eventuele papieren dossier retour naar het Centraal Cliënten Archief.

Het Centraal Cliënten Archief zorgt vervolgens voor de daadwerkelijke vernietiging van het papieren dossier en vraagt de afdeling Informatiebeheer de in het registratiebestand en EPD aanwezige gegevens respectievelijk te anonimiseren en te verwijderen. Vernietiging kan alleen maar plaatsvinden indien alle administratieve en financiële handelingen zijn afgerond.

Het Servicebedrijf Informatisering (SBI)
- bepaalt of e.e.a. conform de regels mogelijk is (zie Protocol Omgaan met Cliëntgegevens) en voert het daarna uit.
- anonimiseert de aanwezige gegevens in het registratiebestand en verwijdert het EPD.
- stuurt na het anonimiseren/verwijderen een bevestiging hiervan per mail naar het Centraal Cliënten Archief.

Het secretariaat van de psychiater-directeur krijgt een schriftelijke bevestiging van het Centraal Cliënten Archief met daarop datum en tijd van de vernietiging. Een kopie van dit schrijven wordt naar het secretariaat van de psychiater-directeur gestuurd om cliënt van de vernietiging van het dossier op de hoogte te stellen.

Na de vernietiging worden alle correspondentie en relevante stukken aangaande het vernietigingsverzoek - conform de wettelijke bewaartermijn voor cliëntendossiers - in het Centraal Cliënten Archief bewaard.

1.4 Vernietigen van papieren en digitaal dossier na verstrijken van de bewaartermijn
actor: centraal cliëntenarchief

Door het Centraal Cliënten Archief worden alle dossiers verzameld die de bewaartermijn van 15 jaar (na het laatste behandelcontact) hebben overschreden. Ze worden verzameld in grote containers van het vernietigingsbedrijf en onder begeleiding en toezicht van een medewerker van het Centraal Cliënten Archief afgevoerd en vernietigd.

De wettelijke vernietigingstermijn is met ingang van 2006 gewijzigd van 10 naar 15 jaar[5]. In 2007 is Altrecht geheel overgegaan naar het EPD en werden er geen nieuwe papieren dossiers meer aangemaakt. Dit betekent dat het vraagstuk “vernietigen EPD"s” pas in 2021 gaat spelen.

Administratieve gegevens in Psygis Basis hebben een langere historie. De procedure voor het automatisch schonen hiervan is nog onderwerp van onderzoek.

[5] De bewaartermijn voor het BOPZ-dossier is 5 jaar: zie hoofdstuk 4

2 Informatie aan derden

2.1 Opvraag papieren dossier binnen Altrecht

Papieren dossier: de bij de behandeling betrokken medewerkers kunnen via het secretariaat het papieren dossier opvragen (archief@altrecht.nl). De dossiers worden daarna via de bekende rode tassen verzonden aan het secretariaat, dat over een sleuteltje beschikt. Het archief streeft ernaar om dossiers binnen twee werkdagen na aanvraag te leveren.

2.2 Inzagerecht van Klachtencommissie en/of PVP

Zie protocol Inzage dossier door Klachtencommissie en PVP voor:

Procedure opvragen dossiers van in behandeling zijnde cliënten
Procedure bij afgesloten en gearchiveerde dossiers
Procedure bij het indienen van een klacht na overlijden van de patient

2.3 Informatieverzoeken externe behandelaren of derden

actoren: centraal cliëntenarchief
laatst(e bekende) behandelaar of afdelingspsychiater
secretariaat laatst(e bekende) behandelaar of afdelingspsychiater

Informatieverzoeken van externe behandelaars: met enige regelmaat komen er verzoeken voor informatie van andere GGZ instellingen, ziekenhuizen of huisartsen.
Ook komen er informatieverzoeken van derden die niet betrokken zijn bij de behandeling of enigerlei medische zorg voor de cliënt, maar wel diens belangen behartigen, zoals bijvoorbeeld een advocaat of een verzekeringsmaatschappij.
Zulk een verzoek moeten altijd schriftelijk plaatsvinden en moet altijd vergezeld gaan met een door de cliënt of, indien van toepassing, zijn/haar wettelijk vertegenwoordiger ondertekende toestemmingverklaring. Bij het verzoek moet een kopie van een legitimatiebewijs of getekende machtiging worden meegestuurd (om de ondertekening van het verzoek te kunnen controleren).

De complete aanvraag wordt door de ontvanger naar het archief gestuurd. Hier worden alle (papieren) dossiers van cliënt bijeen gezocht en ter afhandeling van de aanvraag aan de laatste bekende behandelaar of de afdelingspsychiater van de laatst behandelende afdeling aangeboden.
De behandelaar of afdelingspsychiater dient eventueel de noodknop te gebruiken om te bekijken of er van de cliënt ook en EPD bestaat. De archivaris geeft dit in het overdrachtsformulier aan.

Afdelingen moeten dus niet op eigen initiatief gegevens over cliënten aan derden doorgeven omdat die gegevens mogelijk niet compleet zijn.

2.4 Vergoeding van kosten voor informatieverzoeken door derden

Het verstrekken van informatie aan externe behandelaars wordt gezien als een verlengde van de behandeling van de cliënt en hiervoor worden geen kosten in rekening gebracht bij de aanvrager.

Voor informatieverzoeken van niet-behandelaren, zoals een advocaat of verzekeringsmaatschappij, geldt een vast tarief („overig product", zie: http://www.nza.nl/regelgeving/tarieven). Om dit in rekening te kunnen brengen kan gebruik gemaakt worden van een notaopdracht van de FCI, financiële administratie. De notaopdracht kan ingevuld en ondertekend ter afhandeling aan de Financiële Administratie FCI worden gestuurd.

3 Psygis Quarant (EPD)

3.1 Indeling van het EPD

Het EPD is op een hiërarchische manier opgebouwd. U kunt het vergelijken met een ui met verschillende ringen. De buitenste en grootste ring is de laag “Cliëntgegevens”, op dit niveau kunt u cliënten in het EPD opzoeken en selecteren. De tweede laag bestaat uit één of meerdere inschrijvingsperiodes. U dient altijd vanuit de actuele inschrijvingsperiode te werken als u nieuwe gegevens toevoegt!

Wanneer u in de actuele inschrijvingsperiode zit, ziet u acht genummerde mappen. Onder de hoofdmappen hangen vaak nog meerdere submappen. De mappenstructuur van het EPD ziet er als volgt uit

1. Persoons- en aanmeldgegevens
2. Onderzoek en diagnostiek
3. Behandelplan en aanvullende plannen
4. Somatiek
5. Decursus / voortgangrapportage
6. Overplaatsing en afsluiting
7. Correspondentie
8. Juridische gegevens
9. Cliënt Online
10. ROM/Zorgpaden

Map 1 t/m 6 volgen het zorgproces van aanmelding tot ontslag of overplaatsing.
Map 7 bevat alle inkomende en uitgaande correspondentie.
Map 8 bevat gegevens omtrent de juridische situatie van de patiënt (BOPZ, Strafrechtelijke maatregelen).
Map 9 Cliënt online is onderdeel van Mijnaltrecht.nl. Vanuit deze map wordt informatie doorgesluisd aan het patiëntenportaal Mijnaltrecht.nl, een voor patiënten beveiligde website.
Map 10 bevat koppelingen naar ROM en Zorgpaden.

3.2 Alert functie in het EPD

In het EPD is een Alertfunctie beschikbaar. Met de Alertfunctie kan per cliënt aangegeven worden of er belangrijke waarschuwingen zijn omtrent deze cliënt.
Bijvoorbeeld:
heeft de cliënt een reanimatiebeleid,
is hij/zij allergisch, zo ja waarvoor,
of zijn er andere zaken die direct onder de aandacht gebracht moeten worden zodra een collega het dossier opent.

3.3 Ingescande documenten in het EPD

Het EPD behoort compleet te zijn, en alle cliëntgerelateerde informatie te bevatten. Ingekomen „post" dient ook opgenomen te worden in het EPD. Papieren documenten moeten worden gescand en in het dossier worden gehangen. De originelen documenten moeten worden vernietigd. Alleen in geval van juridische documenten moet echter de originele papieren versie 5 jaar bewaard worden in het BOPZ-dossier.

3.3.1 Naamgeving van (gescande) documenten

Richtlijn naamgeving documenten
JJ-MM-DD + bron + onderwerp. bijvoorbeeld: 2009-11-21 UMC Overdracht

Het EPD groeit met de dag en om ook in de toekomst documenten gemakkelijk terug te kunnen vinden, is het zaak dat de naam van een document zoveel mogelijk informatie geeft over de inhoud. Bovendien is het overzichtelijk als de naamgeving van alle documenten op dezelfde wijze is opgebouwd. Dit geldt voor ingescande documenten en alle MS Word documenten, bijvoorbeeld onder map 6 Overplaatsing en afsluiting en map 7 Correspondentie > Uitgaand.

3.3.2 Waar horen de ingescande documenten thuis?

Het EPD kent een aantal plekken waarop ingescande formulieren geplaatst moeten worden:

map	Omschrijving	Voorbeeld
1	Persoons- en aanmeldingsgegevens	Aanmeldformulier/verwijsbrief (ingescand).; verplicht item in het dossier
2	Onderzoek en diagnostiek	Intake- en crisisverslagen: systeemintake – genogram Overig/aanvullend onderzoek: onderzoek <onderwerp> Checklists en vragenlijsten: NIMH-LCM <onderwerp> vragenlijst
4	Somatiek / Somatische hulponderzoeken	Uitslagen van de somatische onderzoeken zoals ECG"s en Thorax foto"s.
4	Somatiek / Laboratorium	Uitslagen van Saltro
7	Correspondentie, inkomend	Alle ontvangen correspondentie van externe partijen, bijvoorbeeld: - CIZ-indicatie - medische brieven van derden - huisartsenjournaal van niet Altrecht huisarts

3.3.3 Inscannen van (mail)correspondentie met cliënten

Mailberichten met cliënten kunnen samengevat worden in de decursus en/of als PDF bewaard worden onder de map correspondentie.

3.3.4 Hoe in te scannen

Als er op de juiste manier ingescand wordt, dan is het mogelijk om later de tekst te doorzoeken. De documenten worden ingescand op de MFP scanner. Gebruik hiervoor altijd het logo: **EPD scan**. Alleen dán worden de documenten met behulp van speciale software ingescand, zodat de tekst doorzoekbaar is. Bovendien neemt het bestand veel minder geheugencapaciteit in.

3.4 Pasfoto's in het EPD

De werkgroep Wetgeving van GGZ Nederland meldt over het opnemen van een fotokopie van het WID: *"een identiteitsbewijs laten zien is iets anders dan er een kopie van maken en in het dossier stoppen, maar het is niet verboden*". De WPB doet geen expliciete uitspraak over opslaan van foto"s van cliënten, maar stelt in een voorbeeld over het bewaren van foto"s (voor toegangspasjes) van werknemers, dat het opslaan er van "onvermijdelijk moet zijn voor de identificatie".

Voor Altrecht is de stelling aangenomen: voor exceptionele gevallen moet het kunnen om een foto op te nemen in het dossier, maar dan een foto die je ter plekke neemt of ontvangt van de cliënt, voor dat doel ! Niet "stiekem" via een ID-kopie.
De cliënt moet schriftelijk toestemming geven voor het in het dossier opnemen van een foto: de cliënt heeft het recht om te weigeren om een foto in het EPD op te laten nemen.

Denk er aan, dat wanneer de foto van de cliënt op het scherm staat, hij/zij van enige afstand door een passant te herkennen is. De bescherming van de privacy van de cliënt kan in gevaar komen bij onnadenkendheid.

3.5 Werkaantekeningen (niet in EPD)

Persoonlijke werkaantekeningen die de hulpverlener voor korte duur als geheugensteuntje voor zichzelf maakt, zijn per definitie alleen voor eigen gebruik bestemd. Zowel voor de cliënt als collega"s zijn deze aantekeningen niet ter inzage. **Daarom mogen ze niet in het dossier voorkomen**.
Deze werkaantekeningen moeten in ieder geval bij afsluiting van het behandelcontact met de cliënt versnipperd of verwijderd worden van de persoonlijke schijf.
(NB: documenten met naar cliënten herleidbare gegevens mogen **nooit** op de X-schijf worden geplaatst!)

3.6 Autorisatie voor het EPD

3.6.1 Algemene regels

Tot welke dossiers u toegang hebt, welke formulieren gebruikt moeten worden en wat u wel of niet mag doen of lezen in Quarant, is afhankelijk van de inrichting van een drietal zaken:
1. Organisatorische Eenheid autorisatie en behandelrelatie bepalen welke patiënten u kunt zien.
2. EPD profielen bepalen welke onderdelen van het EPD u ziet en kunt bewerken.
3. Menu autorisatie bepaalt welke onderdelen in Quarant/Basis u kunt lezen of bewerken.

Bovenstaande punten worden nader toegelicht in het document "Autorisatie in Psygis Quarant"

3.6.2 Noodprocedure toegang EPD (buiten autorisatie).

Met betrekking tot de noodprocedure is het volgende opgenomen in de WBGO[6]

2.2.5.5 Noodprocedure
Bij spoedeisende zorg kan toegang tot patiëntgegevens worden verleend d.m.v. een „Noodprocedure".

Toelichting:
Bij spoedeisende zorg kan het voorkomen dat aan geen van de voorwaarden voor toegang tot

[6] "Modelrichtlijn Toegang tot patiëntengegevens", tot stand gekomen in het Implementatieprogramma WGBO

Alleen de digitale versie in het documentbeheerssysteem is een beheerst document.

patiëntengegevens kan worden voldaan omdat er geen wettelijke plicht is, geen rechtstreekse betrokkenheid, vervanging of vertegenwoordiging en de patiënt ook geen toestemming heeft gegeven. In dat geval kan de hulpverlener een Noodprocedure volgen, waarmee hij toch toegang krijgt tot de patiëntengegevens. De hulpverlener moet dan wel een protocol volgen/gebruiken. Tijdens de Noodprocedure wordt de toegang 'gelogd'. Hiermee kan worden geverifieerd of het echt noodzakelijk was de procedure te gebruiken. De logging van het gebruik van de Noodprocedure kan direct worden doorgegeven aan bijvoorbeeld de systeembeheerder of aan de directeur van de zorginstelling. Op deze manier wordt achteraf verantwoording afgelegd.
Een Noodprocedure is vereist om toegang te kunnen hebben tot patiëntengegevens in spoedeisende gevallen. Gebruik van de Noodprocedure moet altijd worden geregistreerd ('gelogd'), zodat de rechtmatigheid van toegang achteraf verifieerbaar is.

De beleidsverantwoordelijkheid voor het toepassen van de richtlijn ligt bij de Raad van Bestuur.

Zodra je een dossier opzoekt buiten autorisatie in Psygis Quarant dien je een geldige reden op te geven. Veel gebruikte redenen kun je uit een drop-down menu selecteren. Bijvoorbeeld: Crisisdienst, Geneeskundige verklaring inzake BOPZ, spoedopname etc. Daarnaast is het mogelijk om zelf een reden in te vullen waarom je een dossier buiten autorisatie wil inzien. De opgegeven reden wordt gelogd.

Controle buiten autorisatie gebruik
Altrecht is verplicht een aantoonbare controle op het gebruik van deze knop uit te voeren, in het kader van de privacybescherming van patiënten. Via Altris hebben kostenplaatsmanagers inzicht in: wie van hun medewerkers, welke dossiers heeft bekeken via buiten autorisatie. In principe kan de kostenplaatsmanagers dagelijks deze rapportages inzien, maar dient dit minimaal 1x per maand te bekijken. Bij constatering van onterecht gebruik van deze mogelijkheid in Psygis Quarant dient de manager proportioneel passende maatregelen nemen.

Daarnaast kan de (hoofd)behandelaar ten allen tijde, bij informatiebeheer een rapportage opvragen waaruit blijkt welke medewerkers van Altrecht via buiten autorisatie het dossier van een specifieke cliënt heeft ingezien. Bijvoorbeeld als een cliënt bang is dat zijn dossier ten onrechte is bekeken.

3.6.3 Autorisatie t.b.v. wetenschappelijk onderzoek

actoren: CWO (Commissie Wetenschappelijk Onderzoek)
afdelingspsychiater of BGD
centraal cliëntenarchief
servicebedrijf informatisering

Ter bescherming van de privacy van de patiënten is toegang tot het (elektronisch) dossier van patiënten beperkt tot de direct bij de behandeling betrokkenen. In geval van wetenschappelijk onderzoek beoordeelt de Commissie Wetenschappelijk Onderzoek alle voorwaarden voor het uit te voeren onderzoek, inclusief eventuele toegang tot dossiergegevens.
.
Als je als onderzoeker toegang krijgt tot medische gegevens, dien je hier buitengewoon zorgvuldig mee om te gaan. Hierbij geldt de volgende procedure:

Na akkoord van de CWO krijgt de onderzoeker eerst een Psygis Quarant (PQ) training. Bij succesvolle afronding ontvangt de onderzoeker een PQ account met (beperkte) inzage tot een aantal onderdelen van het EPD, maar nog geen directe toegang tot cliëntendossiers. Om toegang te krijgen voor de betreffende cliëntendossiers wordt gebruik gemaakt van de noodknop, met als reden: "Wetenschappelijk onderzoek". Deze inzage wordt gelogd en gerapporteerd aan de manager van de onderzoeker. Inzage in andere dossiers is niet toegestaan!

Wanneer de onderzoeker onvoldoende inzage heeft in het dossier of de omvang van de te onderzoeken patiëntengroep is te groot om dossiers via de noodknop te benaderen, kan via de manager van de onderzoeker bij informatiebeheer uitbreiding van de toegangsrechten worden aangevraagd (mail: Informatiebeheer@altrecht.nl).

Hierbij dient de volgende informatie te worden verstrekt:
- Naam manager waar de onderzoeker onder valt.
- Titel van het door de Commissie Wetenschappelijk Onderzoek goedgekeurde onderzoeksproject waarvoor de autorisatie-uitbreiding nodig is.
- Om welke autorisatie-uitbreiding het gaat:
  cliëntautorisatie, inzage zonder noodknop: dan aangeven voor welke organisatorische eenheden het onderzoek van toepassing is en of het gaat om actuele of niet actuele cliënten.
  bredere inzage in het dossier: dan aangeven welke gegevens ter inzage beschikbaar dienen te zijn.
- Over welke periode het onderzoek plaatsvindt.

Meer informatie over de procedures met betrekking tot wetenschappelijke onderzoeksprojecten: Altranet > interne services > Altrecht Science.

3.7 Substitueren cliëntgegevens

Wanneer een cliënt in het cliëntenbestand staat met een foutieve geboortedatum of de naam is verkeerd gespeld, moet er een zogenaamde “substitutie” van cliëntgegevens worden uitgevoerd. Zie: Substitutie van cliëntgegevens in Quarant/EPD.

Quarant en EPD zijn zo ingesteld, dat bij het intypen van de oude nummer de juiste cliënt met de juiste gegevens op het scherm verschijnt.
Controleer ook eventuele koppelingen naar gerelateerde applicaties die van het cliëntnummer van Psygis Quarant gebruik maken, zoals ROM, EVS en dergelijke.

Deze werkwijze geldt natuurlijk niet voor de dubbele cliënten die al in het systeem staan, maar zodra iemand ingeschreven moet worden die er dubbel in staat, moet wel eerst een substitutie uitgevoerd worden. Dubbele cliënten bij inschrijving graag melden bij de servicedesk@altrecht.nl

4 BOPZ-dossier

Na overleg met de BOPZ-secretariaten is besloten dat het papieren BOPZ-dossier blijft bestaan naast de digitale mogelijkheden van BOPZ-online en EPD. Het “meest essentiële BOPZ-materiaal” wordt door het BOPZ-secretariaat ingescand in het EPD.

Onder het “meest essentiële BOPZ-materiaal” wordt verstaan:
IBS of RM aanvragen/geneeskundige verklaring
Het proces-verbaal betreffende BOPZ-titels
De IBS of RM-beschikking
Brief rechtbank “Verzoek ingesteld”
Brief rechtbank “Zittingsdatum”
Aanvraag Onafhankelijke Beoordeling Dwangbehandeling
Artikel 38 en 39 Aanvang en Beëindiging + art. 40a
Evaluatie dwangbehandeling (van behandelend psychiater)
Bevindingen second opinion dwangbehandeling (onafhankelijke psychiater)

Schriftelijk bericht aan cliënt: continuering art. 38c lid 3 wet BOPZ
Einde IBS
Beëindigen / opheffen RM
Verklaring (voorwaardelijk) ontslag / verlof

De papieren dossiers worden na afsluiting bij het BOPZ-secretariaat bewaard met uitzondering van de reeds in het centraal archief geplaatste dossiers (tot 2012). Wanneer een nieuwe BOPZ-maatregel start, wordt een nieuw papieren BOPZ-dossier aangemaakt.

Bij tijdelijke overplaatsingen, bijvoorbeeld in geval van triage, wordt het BOPZ-dossier niet meegezonden met de cliënt naar de nieuwe afdeling. Het dossier en de verantwoordelijkheid blijft bij het BOPZ-secretariaat van de oude afdeling.
Bij definitieve overdracht van de behandeling aan een nieuwe afdeling gaat het BOPZ-dossier mee naar het BOPZ-secretariaat van de nieuwe afdeling, inclusief de verantwoordelijkheden hiervoor.
NB: Het M/M dossier gaat altijd mee met de cliënt, ook tijdens triage-periodes.

Vernietigen BOPZ-dossier
Voor BOPZ-materiaal geldt een afwijkende bewaartermijn van 5 jaar na het sluiten van de maatregelperiode. Het Centraal Cliëntenarchief zorgt na het verlopen van de bewaartermijn voor de vernietiging van het papieren materiaal wat zij in beheer heeft (tot 2012). Het bureau GD is verantwoordelijk voor het in het EPD ingescande of op overige manieren bewaarde BOPZ materiaal na verlopen van de bewaartermijn. De registratie van de BOPZ-periode blijft in Quarant gehandhaafd; alleen de inhoudelijke documenten in het EPD dienen te worden verwijderd.

5 BHT (BinnensHuisTherapie)

Hierbij gaat het om publiek bekende personen (VIP"s), collega"s en familie van collega"s die bij Altrecht in behandeling komen. Het kan voor de cliënt bezwaarlijk zijn wanneer een andere collega dan de behandelaar(s) inzage zou kunnen hebben in inhoudelijke onderzoeks- of behandelgegevens.

Indien een cliënt bezwaar maakt tegen dossiervorming in het EPD, worden alleen die administratieve gegevens in Quarant geregistreerd, die noodzakelijk zijn om de zorg te kunnen verantwoorden en te declareren. De inschrijving bevat administratieve gegevens, zoals de persoonsgegevens, maar ook de DSM-diagnose en de verstrekte activiteiten en verrichtingen. Om de behandeling correct te kunnen declareren is dit onvermijdelijk.

Voor de verplichte dossiervoering mag gebruik gemaakt worden van het aloude papieren dossier, zodat verder geen behandelinhoudelijke gegevens digitaal bereikbaar zijn. Zowel de betrokken behandelaren als het secretariaat moeten hierover geïnformeerd worden. Dit papieren dossier wordt na afsluiting van de behandeling in een gesloten envelop op naam aangeboden aan het centraal cliëntenarchief. Het dossier mag alleen maar gelicht worden na toestemming van de cliënt/collega.

Onder tabblad 1, Persoonsgegevens, moet een formulier ingevuld worden: *Geen elektronisch dossier: Over deze behandelepisode is op verzoek van cliënt geen elektronisch dossier aangemaakt, maar een afgeschermd papieren dossier. Cliënt is op de hoogte gesteld van eventuele risico's in geval van bijvoorbeeld een crisisopname..* Vermeld daarnaast in de Alert: Papieren Dossier zodat het voor iedereen direct duidelijk is dat deze cliënt een papieren dossier heeft.
Deze opmerking geeft voldoende duidelijkheid wanneer het dossier gezocht wordt voor bijvoorbeeld een onderzoek (van Inspectie GGZ) of een audit. In dat laatste geval zal een aanpassing in de steekproef moeten plaatsvinden.

6 Overige digitale gegevensbestanden (onder constructie)

Altrecht maakt ook buiten Psygis Quarant gebruik van diverse applicaties en bestanden waarin cliëntgegevens zijn opgeslagen, zoals Medicatiegegevens en ROM-gegevens. Voor elk van deze applicaties en bestanden moet beschreven zijn op welke wijze de privacy van deze gegevens wordt gewaarborgd.

Toestemmingsverklaring

Hierbij verklaart:

Naam cliënt :

Geboortedatum :

Ouder/verzorger 1 : Ouder/verzorger 2 :

Geboortedatum : Geboortedatum :

Ouderlijk gezag : ja/nee Ouderlijk gezag : ja/nee

Aan Altrecht toestemming te verlenen om

Informatie op te vragen bij *		**Informatie te verstrekken aan ***	
- Huisarts	ja/nee	- Huisarts	ja/nee
- Bureau Jeugdzorg	ja/nee	- Bureau Jeugdzorg	ja/nee
- School	ja/nee	- School	ja/nee
- Schoolarts	ja/nee	- Schoolarts	ja/nee
- Eerdere hulpverlenende instantie	ja/nee	- Eerdere hulpverlenende instantie	ja/nee
- Anders, namelijk		- Anders, namelijk	

**Graag doorhalen wat niet van toepassing is.*

Handtekening ouder:

Plaats:

Datum:

Handtekening jeugdige van 12 jaar of ouder:

Plaats:

Datum:

stafdienst financiën, control en informatievoorziening

Dolderseweg 164, 3734 BN Den Dolder
T 030 22 56 143 F 030 22 56 977

Altrecht geestelijke gezondheidszorg

Richtlijn Uniform Patiënten Dossier (UPD)

Auteur: G. Bongers
Versie: 4

Stafdienst FCI
ZIV

Inhoudsopgave

1 Inleiding

Waar is het archief voor ?
Het CCA (Centraal Cliënten Archief) dient er voor om afgesloten dossiers op een verantwoorde wijze te bewaren. Het archief bewaart dus alleen afgesloten dossiers. Lopende dossiers worden op de afdeling of op het afdelingssecretariaat bewaard. Het archief is gevestigd op de locatie Schearweijde Zeist. Alle dossiers worden gearchiveerd op geboortedatum aangezien dit een uniek kenmerk is. De volledige geboortedatum (dd-mm-jj) is noodzakelijk omdat deze in combinatie met de naam gebruikt word om te archiveren. Bij opvragen van een dossier dient dan ook altijd de volledige geboortedatum vermeld te worden.

Waarom op geboortedatum archiveren?
De geboortedatum is, in combinatie met de naam, de beste manier van archiveren omdat de combinatie een uniek geheel vormt. Archiveren op naam maakt het leveren van het juiste dossier een stuk moeilijker. Niet alleen de hoeveelheid cliënten met dezelfde naam geeft veel verwarring maar ook de verschillende schrijfwijze.

2 Soorten dossiers

Het cliëntendossier kan bestaan uit de volgende soorten dossiers:

1. Somatisch:	Hierin staan huisartsgegevens, externe onderzoeksgegevens. Voor dit onderdeel geldt een beperkte autorisatie.
2. Medisch:	Hierin staan de behandelgegevens, correspondentie ed. Geheel volgens de index UPD (bijlage 1.).
3. Ambulant/Poli:	Dit is het Medische dossier van een ambulante cliënt.
4. BOPZ:	Bevat rechterlijke machtigingen, juridische gegevens, middelen en maatregelen. In dit dossier komen de originele stukken. - Kopieën hiervan komen onder tab. 9 in het Medische dossier. - Bij afsluiting van het dossier dienen deze kopieën ter vernietiging aan het archief aangeboden te worden.
5. Verpleegkundig:	Deze gegevens komen in het Medische dossier onder tab. 5. Bij een te groot volume kan hier een aparte map/envelop aangelegd worden. Deze dient ook volledig genaamd en gestickerd te worden.

Aanmaken (nieuw) dossier
Sinds het gebruik van het EPD worden geen behandeldossiers meer aangemaakt.

3 Procedures

Kopie uit dossier
Zie procedure “Recht op inzage”.(zie Altranet voor volledige tekst).

Vernietiging dossier
Zie: “Protocol Vernietigen”.(zie Altranet voor volledige tekst).
Een beknopte handleiding te vinden op bijlage 4. Recht op correctie van dossier (vernietigen 1 dossierstuk) zie bijlage 5.

4 Overige archief items

Röntgenfoto's
Het beheer hiervan is geen taak van het CCA. Bij het afsluiten van een behandelcontact dienen aanwezige röntgenfoto's te worden teruggestuurd naar het algemene ziekenhuis die de foto heeft gemaakt. Steeds vaker komt het voor dat de cliënten zelf de foto's bewaren wat ook toegestaan is.

Microfiches
Andere dossiervormen naast het UPD en EPD zijn binnen Altrecht niet toegestaan. In het verleden geproduceerde dossiers op microfiches worden desgevraagd nog uitgeprint. Als de bewaartermijn verlopen is worden ook deze vernietigd.

5 Ontslagbrief of verwijsbrief

Ontslagbrief
Zie AO zorgproces – procesnummer 1.5 Afsluiting behandeling.
De behandelverantwoordelijke stelt een afsluitbrief op. Het secretariaat zorgt voor de verdere afwikkeling. De ontslagbrief wordt ingescand in het EPD.

Interne verwijzing / -brief
Bij een interne verwijzing dient het dossier, voorzien van een overplaatsingsbrief (verwijzing), de cliënt per ommegaande te volgen. De verwijzing wordt in het EPD verwerkt.

Samenvoegen/Splitsen
Meerdere papieren dossiers van dezelfde cliënt moeten worden samengevoegd om er weer één dossier van te maken. Het secretariaat die het dossier aanvraagt voegt de dossier delen samen. Na het samenvoegen dient de lege map retour archief gestuurd te worden met daarop de aanduiding "samengevoegd". Als de inhoud te groot wordt kan een dossier in meerdere blauwe mappen worden gesplitst. Ook dit is een taak van het secretariaat. Dossiers moeten worden gesplitst op datum/periode en niet op hoofdstuk. Op de buitenzijde komt dan te staan; Deel I t/m datum ..-..-.. Deel II vanaf datum ..-..-..

6 Afsluiten dossiers

A. Wanneer een dossier afgesloten word komt er in het EPD een ontslagbrief / uitschrijfformulier
B. Papieren dossiers dienen conform dit protocol aan het archief aangeboden te worden.

Bij beëindiging van de inschrijving kan het EPD worden afgesloten.
Indien de cliënt een interne verwijzing heeft, volgt het papieren dossier de cliënt.

Dossiers verlaten nimmer de instelling.

7 Verantwoording

Transport
Facilitair bedrijf/transportdienst is verantwoordelijk voor de veiligheid/beveiliging van de voor transport aangeboden post/dossiers en tijdens het transport hiervan, mits de dossiers in de voorgeschreven rode tas zit.

Lopende dossiers
Zolang dossiers op afdelingen zijn, bij behandelaars of secretariaten, is de afdelingleiding verantwoordelijk voor de juiste opslag, afhandeling en gebruik van de dossiers.

Archief
De archiefbeheerder van het CCA (Centrale Cliënten Archief) is verantwoordelijk voor de uitvoering van deze richtlijn. In geval er afwijkingen worden geconstateerd zal hij de betreffende afdelingen hierop aanspreken.

8 Toegangcontrole

Voor toegang tot het archief wordt een strak toegangsbeleid gevolgd.
Er worden periodieke controles uitgevoerd op het gebruik van uitgegeven elektronische sleutels.

9 Juridische zaken

BOPZ (Bijzondere Opname Psychiatrische Ziekenhuizen)
Een BOPZ dossier bevat;

1. IBS
2. Machtigingen
3. M en M (Middelen en Maatregelen)

Stukken betreffende deze onderdelen horen in het BOPZ dossier thuis
en niet in het “gewone” cliënten dossier.
Dit “lopend” dossier wordt beheerd door het secretariaat van de Geneesheer Directeur.
Het CCA is verantwoordelijk voor de afgesloten BOPZ dossiers die bij hen in bewaring zijn gegeven. Dit dossier dient 5 jaar na afloop laatste maatregel vernietigd te worden.

Overige juridische stukken
Strafdossierstukken dienen bij afloop van de termijn teruggestuurd te worden naar de aanmelder. Dit kan zijn de rechtbank, justitie of advocaat. Dit is een taak van het secretariaat van de betreffende (forensische) afdeling.

10 Verzenden dossiers

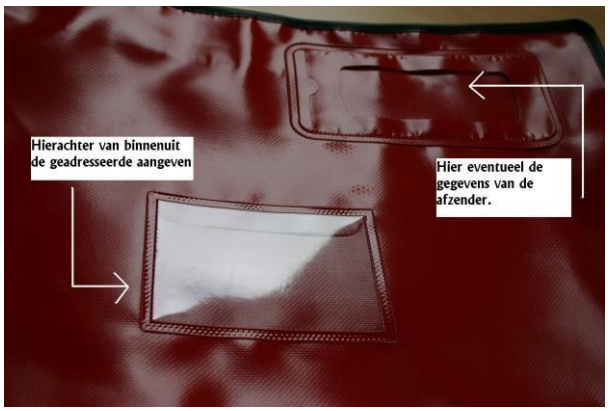
Het verzenden van de dossiers gebeurt met gebruik van rode dossiertassen (zie afb. I) en op geen enkele andere wijze (zoals de interne postenvelop).

Afbeelding I

Deze tassen zijn voorzien van een eenvoudig hangslotje (zie afb. J).

Afbeelding J

De dossiertassen worden afgesloten zoals hierboven te zien is. Sleutels voor dit hangslotje zijn aanwezig bij alle secretariaten. De dossiertassen met slotjes zijn verkrijgbaar bij het magazijn.
De dossiertassen mogen alleen worden gebruikt voor het transport van dossiers binnen de organisatie. De tassen worden door de interne post vervoerd. Bij verzenden van een dossiertas moet achter het plastic venster de geadresseerde worden aangegeven (zie afb. K).



Afbeelding K

11 Spelregels gebruik rode dossiertassen

Rode tassen gaan alleen van secretariaat naar secretariaat, nooit rechtstreeks naar de behandelaar
Rode tassen (dossiers) gaan **NOOIT** extern
Rode tassen gebruiken we alleen voor dossiertransport
Rode tassen worden afgesloten met het ABUS hangslotje, niet met het op de rits aanwezige slotje
Geen stickers of andere spullen op de tas plakken!
Adressering waar de tas heen moet **achter het PLASTIC** venster (van binnenuit te vullen). Hier kan het niet uitvallen.
Geef duidelijk aan naar wie het moet, alleen de locatie is niet voldoende want daar zitten meerdere secretariaten.
Afzender graag **IN** de tas niet **op** de tas om misverstanden in aflevering te voorkomen
Alle onbestelbare mappen worden bij het centraal cliënten archief afgegeven

12 Bewaartermijn

Altrecht houdt voor cliëntendossiers de bewaartermijn aan welke door de wet wordt opgelegd. Conform de wet dienen de medische dossiers per 01-01-06 tot 15 jaar na het laatste behandelcontact bewaard te worden. Voor 01-01-06 was deze termijn 10 jaar. Resultaat is dat alle dossiers waarvan het laatste behandelcontact lag vóór 1 januari 1996 zijn vernietigd.
BOPZ dossiers (juridische dossiers) worden tot 5 jaar na aflopen van de maatregel bewaard.

Bewaartermijn na afsluiting

A. In verband met de na te komen stukken en heraanmelding van cliënt dienen dossiers na uitschrijving **3 maanden** op de secretariaten bewaard te worden alvorens deze aan het archief aan te bieden.
B. BOPZ dossiers – totale bewaartermijn 5 jaar. (wetgeving WBP 01-04-1995)
Overige dossiers – totale bewaartermijn 10 jaar. (wetgeving WBP tot 01-01-2006)
– totale bewaartermijn 15 jaar. (wetgeving WBP vanaf 01-01-2006)

13 Overige dossier zaken

Uitleenadministratie
In het archief wordt een uitleenadministratie bijgehouden. Hierop staat o.a. aangegeven de uitleendatum, aan wie, wat en wanneer retour gekomen.

Groepsdossier
Van elk persoon dient een eigen dossier (aangelegd) te zijn. De groepsverslagen horen niet in het dossier thuis. In het dossier dient wel een verwijzing naar de groepsverslagen en/of groepsdossier aanwezig te zijn. Groepsverslagen worden door de behandelaar of secretariaat zelf beheerd. Deze dragen ook zorg voor tijdige vernietiging na verstrijken van de bewaartermijn.

Dossiervolgsysteem
Het archief ontvangt, archiveert en levert dossier(s) aan secretariaten. Waar het dossier na levering aan het secretariaat heen gaat is buiten het zichtveld van de archiefmedewerker.

Nagekomen stukken
In principe komen de meeste nagekomen stukken binnen tijdens de drie maanden bewaartijd op het secretariaat. Indien hierna nog stukken voor het dossier binnen komen moet het bijbehorende dossier wordt opgevraagd bij het archief door het secretariaat. Het secretariaat voegt de nagekomen stukken in. De archiefmedewerkers voeren **GEEN** dossierstukken in dossiers. Wanneer het archief “losse” stukken ontvangt, worden deze door het archief geretourneerd. Indien niet bekend wie de afzender is worden de losse stukken terzijde gelegd.

Naamswijziging
Bij naamswijziging van een cliënt of wijziging van het geslacht van een cliënt wordt de notering bij de Burgerlijke Stand gevolgd. Cliënten dienen dit bij de secretariaten aantoonbaar te maken. De secretariaten lichten de afdeling ZIV en het archief in.

Onderzoeken (studie)
Bij onderzoeken en studie's waar één of meerdere dossiers bij nodig zijn dienen de dossieraanvragen aangekondigd te worden. Hieronder wordt verstaan de studies van studenten, stagiaires en onderzoekers. Het archief heeft voor uitlevering van dossiers een toestemmingsverklaring nodig van het afdelingshoofd waar de onderzoek(st)er onder valt. Deze regelt o.a. geheimhouding e.d.

Faxen medische gegevens
Aangezien de risico's van het faxen van medische gegevens groot zijn, mogen er zowel intern als extern geen medische gegevens worden gefaxt.

Plaats dossier bij 2 gelijktijdige behandelingen
Zie hiervoor de werkinstructie "Kopiëren amb.dossiers t.b.v. klinische opname". (zie bijlage 3.).

14 Opvragen Dossiers

Opvraag rechten intern
De bij de behandeling betrokken medewerkers kunnen via het secretariaat dossiers opvragen.
Alle overigen (bijv. Klachtencommissie) dienen hun aanvraag te voorzien van een toestemmingsverklaring van de cliënt zelf.

Opvraag rechten extern
Met enige regelmaat komen er verzoeken voor informatie van andere GGZ instellingen, ziekenhuizen of huisartsen. Bij deze verzoeken moet altijd een getekende toestemmingsverklaring van de cliënt zitten. De complete aanvraag (en eventuele aanwezige dossiers van cliënt) wordt door de ontvanger naar het archief gestuurd. Hier worden alle dossiers van cliënt bijeen gezocht en ter afhandeling van de aanvraag aan het secretariaat geneesheer directeur aangeboden. Afdelingen mogen dus niet op eigen initiatief gegevens over cliënten aan derden doorgeven.

15 Opvraag / levertermijn

Dossiers dienen per E-mail opgevraagd te worden. Het e-mail adres:

archief@altrecht.nl

Het archief streeft ernaar om dossiers binnen 24 uur (werkdagen) na aanvraag te leveren.

16 EPD

Wat gebeurt er met voor het EPD ingescande documenten?
Deze worden aan de buitenkant voorzien van een rood, ingevuld, formulier.
In deze dossiers mag niets meer gewijzigd/toegevoegd worden, het dossier is alleen een inzage dossier geworden.

Bijlage 1.1.

Handleiding protocol recht op vernietiging

Deze handleiding is een beknopte versie van het protocol zoals dit door Altrecht is opgesteld en wordt gehanteerd. De volledige tekst van het protocol is te vinden op het intranet van Altrecht onder het hoofdstuk Info pagina's, Handboeken Kwaliteitszorg. Indien gewenst is een kopie ook op te vragen bij de afdeling zorgadministratie.

Enkele regels aangaande een verzoek tot vernietiging:
1. Een verzoek tot vernietiging van dossiermateriaal moet altijd schriftelijk worden ingediend.
2. Het verzoek moet altijd ondertekend worden door de cliënt of, indien van toepassing, zijn vertegenwoordiger.
3. Bij het verzoek moet een kopie van een legitimatiebewijs worden meegestuurd.
4. Het verzoek moet worden gericht aan de geneesheer directeur of aan de betreffende behandelaar.

Werkwijze:

Voor de leesbaarheid van het volgende worden geneesheer directeur en/of behandelaar verder als "ontvanger" aangegeven.

De ontvanger kijkt of het verzoek aan alle regels voldoet en bepaald of het dossier inderdaad vernietigd mag worden (er zijn enkele gronden waarop zij het verzoek kunnen afwijzen).
De ontvanger kan verzoeken het dossiermateriaal eerst in te zien alvorens het te vernietigen. Hiervoor vraagt hij het dossier op bij het medisch archief en/of EPD.
De ontvanger bepaald of het dossiermateriaal geheel of gedeeltelijk wordt vernietigd.
De ontvanger stuurt het originele verzoek (en eventueel het opgevraagde dossier) naar het medisch archief. Deze gaan na of er binnen de instelling verdere gegevens van de cliënt aanwezig zijn en verzamelen deze.
Met het doorsturen van het verzoek geeft de ontvanger aan geen bezwaar te hebben tegen de vernietiging.
Het medisch archief vraagt aan de zorgadministratie de in het patientenbestand aanwezige gegevens te anonimiseren.
De zorgadministratie bepaald of e.e.a. conform de regels mogelijk is en voert het daarna uit.
De zorgadministratie vraagt aan de helpdesk EPD de aanwezige gegevens te verwijderen en controleert de uitvoering hiervan.
Na het anonimiseren stuurt de zorgadministratie een bevestiging hiervan per mail naar het medisch archief.
Het medisch archief zorgt voor de daadwerkelijke vernietiging van het papieren dossier.
Na de vernietiging worden alle correspondentie en relevante stukken van zowel ontvanger als zorgadministratie aangaande het vernietigingsverzoek conform de wettelijke bewaartermijn cliëntendossier ter archivering in het medisch archief bewaard.
Na de vernietiging krijgt de ontvanger een schriftelijke bevestiging met daarop datum en tijd van de vernietiging. Dit schrijven kan worden gebruikt om de cliënt van de vernietiging van het dossier in kennis te stellen.

Bijlage 1.2

VERZOEK TOT VERNIETIGING MEDISCH DOSSIER:

Ondergetekende verklaart dat het zijn/haar uitdrukkelijke wens is dat tot vernietiging van op hem/haar betrekking hebbende medische gegevens wordt overgegaan.

Ondergetekende verklaart tevens dat hij/zij door Altrecht adequaat is geïnformeerd over de eventuele gevolgen en/of nadelige consequenties van de (voorgenomen) vernietiging.

Indien er een gerechtelijke procedure of een klachtenprocedure tegen Altrecht of een van onze medewerkers is aangespannen c.q. te verwachten is dat dit zal gaan gebeuren, kan er niet tot vernietiging worden overgegaan.

Met inachtneming van het bovenstaande verzoekt ondergetekende de stichting Altrecht te Den Dolder:

- Over te gaan tot vernietiging van het op hem/haar betrekking hebbende medische dossier.
- Het anonimiseren van zijn/haar de gegevens in het centrale cliëntensysteem.

Naam :

Geboortedatum :

Adres :

Woonplaats :

Laatste behandel locatie Altrecht :

Datum ondertekening :

Handtekening

:

Dit verzoek met een **kopie legitimatiebewijs** kunt u sturen naar:

Stichting Altrecht
Medisch Archief lokatie Zeist
Oude Arnhemseweg 260
3705 BK Zeist

Bijlage 2.1

Handleiding protocol recht op correctie

Deze handleiding is een beknopte versie van het protocol zoals dit door Altrecht is opgesteld en wordt gehanteerd. De volledige tekst van het protocol is te vinden op het intranet van Altrecht onder het hoofdstuk Info pagina's, Handboeken Kwaliteitszorg. Indien gewenst is een kopie ook op te vragen bij de afdeling zorgadministratie.

Enkele regels aangaande een verzoek tot correctie:

5. Een verzoek tot correctie van dossiermateriaal moet altijd schriftelijk worden ingediend.
6. Het verzoek moet altijd ondertekend worden door de cliënt of, indien van toepassing, zijn vertegenwoordiger.
7. Bij het verzoek moet een kopie van een legitimatiebewijs worden meegestuurd.
8. Het verzoek moet worden gericht aan de betreffende behandelaar.

Werkwijze:

Voor de leesbaarheid van het volgende wordt de behandelaar verder als "ontvanger" aangegeven.

De ontvanger kijkt of het verzoek aan alle regels voldoet. D.w.z. het te corrigeren (vernietigen) materiaal moet daadwerkelijk feitelijke onwaarheden bevatten die vernietiging ervan rechtvaardigen.
De ontvanger stuurt het originele verzoek en het betreffende materiaal naar het medisch archief.
Met het doorsturen van het verzoek geeft de ontvanger aan geen bezwaar te hebben tegen de correctie (vernietiging).
Het medisch archief bepaald of het verzoek aan alle regels voldoet.
Het medisch archief zorgt voor de daadwerkelijke vernietiging van de ter correctie aangeboden dossierstukken.
Na de vernietiging worden alle correspondentie en relevante stukken van ontvanger aangaande het correctieverzoek conform de wettelijke bewaartermijn cliëntendossier ter archivering in het medisch archief bewaard.
Na de correctie krijgt de ontvanger een schriftelijke bevestiging met daarop datum en tijd van de vernietiging. Dit schrijven kan worden gebruikt om de cliënt van de vernietiging van het dossier in kennis te stellen.

Bijlage 2.2

VERZOEK TOT CORRECTIE MEDISCH DOSSIER:

Ondergetekende verklaart dat het zijn/haar uitdrukkelijke wens is dat een of meerdere dossierstukken ter correctie worden vernietigd.

Ondergetekende verklaart tevens dat hij/zij door Altrecht adequaat is geïnformeerd over de eventuele gevolgen en/of nadelige consequenties van de (voorgenomen) correctie/vernietiging.

Met inachtneming van het bovenstaande verzoekt ondergetekende de stichting Altrecht te Den Dolder:

- Over te gaan tot vernietiging van het op hem/haar betrekking hebbende dossierstuk(ken), namelijk:
  (graag dossierstuk(ken) omschrijven d.m.v. kenmerken, datums, namen)

  ……
  ……
  ……
  ……

Naam	:
Geboortedatum	:
Adres	:
Woonplaats	:
Behandel locatie Altrecht	:
Datum ondertekening	:
Handtekening	:

Bijlage 3.1

Handleiding protocol recht op inzage of kopie

Deze handleiding is een beknopte versie van het protocol zoals dit door Altrecht is opgesteld en wordt gehanteerd. De volledige tekst van het protocol is te vinden in Manual Master – Handleiding omgaan met cliëntendossiers. Indien gewenst is een kopie ook op te vragen bij de afdeling Z.I.V. (zorg informatie voorziening.)

Enkele regels aangaande een verzoek tot inzage of kopie door cliënt(e):

9. Een verzoek tot inzage (kopie) van dossiermateriaal moet altijd schriftelijk worden ingediend.
10. Het verzoek moet altijd ondertekend worden door de cliënt of, indien van toepassing, zijn/haar wettelijk vertegenwoordiger.
11. Bij het verzoek moet een kopie van een legitimatiebewijs worden meegestuurd.

Werkwijze:

Het verzoek kan rechtstreeks worden gestuurd naar het medisch archief. In geval de aanvraag bij een andere afdeling binnenkomt moeten zij hem naar het archief doorsturen.
Het medisch archief gaat na of er binnen de instelling verdere gegevens van de cliënt aanwezig zijn en verzamelen deze.
Het medisch archief stuurt het verzamelde materiaal naar, indien nog werkzaam bij de instelling, de laatst bekende behandelaar. Anders gaat het naar de afdelingspsychiater.
De behandelaar of de afdelingspsychiater kijkt of het verzoek aan alle regels voldoet en bepaald of het dossier inderdaad ingezien mag worden (er zijn enkele gronden waarop zij het verzoek kunnen afwijzen).
De behandelaar of de afdelingspsychiater tekent onder het aanvraagformulier voor geen bezwaar en geeft het dossier en verzoek door aan het secretariaat ter afhandeling.
Indien het een gearchiveerde periode in het EPD betreft dan kan de helpdesk ZIS gevraagd worden deze tijdelijk open te stellen voor inzage of kopie.
Na het maken van een kopie (afdruk EPD) of de inzage wordt het dossier en het originele verzoek retour gestuurd naar het medisch archief.
Alle correspondentie en relevante stukken aangaande het verzoek wordt conform de wettelijke bewaartermijn cliëntendossier ter archivering in het medisch archief bewaard.

Bijlage 3.2

VERZOEK OPVRAGEN MEDISCH DOSSIER:

Ondergetekende verzoekt stichting Altrecht om een kopie van zijn/haar medisch dossier aan hem/haar beschikbaar te stellen.

Ondergetekende verklaart tevens dat hij/zij zich bewust is dat de verstrekte gegevens na ontvangst buiten de controle van Altrecht vallen v.w.b. de bewaartermijn en privacywetgeving.

Naam	:
Geboortedatum	:
Adres	:
Woonplaats	:
Laatste behandel locatie Altrecht	:
Datum ondertekening	:
Handtekening	:

Dit verzoek met een **kopie legitimatiebewijs** kunt u sturen naar:

Stichting Altrecht
Medisch Archief lokatie Zeist
Oude Arnhemseweg 260
3705 BK Zeist

Bijlage 4.1

VERZOEK OPVRAGEN MEDISCH DOSSIER OVERLEDENE:

Ondergetekende verzoekt stichting Altrecht om een kopie van het medische dossier van hieronder aangegeven cliënt(e) aan hem/haar beschikbaar te stellen. De relatie van ondergetekende t.a.v. overledene is de volgende:……..

Ondergetekende verklaart tevens dat hij/zij zich bewust is dat de verstrekte gegevens na ontvangst buiten de controle van Altrecht vallen v.w.b. de bewaartermijn en privacywetgeving.

Naam overledene	:
Geboortedatum overledene	:
Laatste behandel locatie Altrecht	:
Naam aanvrager	:
Adres aanvrager	:
Woonplaats aanvrager	:
Datum ondertekening	:
Handtekening aanvrager	:

Dit verzoek met een **kopie legitimatiebewijs (*) aanvrager en kopie overlijdensakte** kunt u sturen naar:

(*) *Let op, uit de kopie legitimatie moet de relatie tussen aanvrager en overledene te herleiden zijn. Indien dit niet het geval is zal ander "bewijs" moeten worden bijgesloten.*

Stichting Altrecht
Medisch Archief lokatie Zeist
Oude Arnhemseweg 260
3705 BK Zeist

Toestemmingsformulier om uw huisarts te informeren over uw behandeling

Geachte heer of mevrouw,

U bent door uw huisarts of medisch specialist naar Altrecht doorverwezen. Altrecht werkt altijd samen met de huisarts, omdat hij het overzicht heeft over alle aspecten van uw gezondheid en eerdere en andere behandelingen. Hij heeft een centrale rol om te zorgen voor een goede afstemming van verschillende behandelingen en we vinden het daarom van groot belang, dat hij ook op de hoogte is van de behandeling die u bij Altrecht krijgt. Hierover hebben wij met de huisartsen een samenwerkingsovereenkomst afgesloten. Eén van de onderdelen van deze overeenkomst is dat wij de huisarts betrekken bij en informeren over (het verloop van) uw behandeling. Daarvoor hebben wij echter wel uw toestemming nodig.

Wat houdt de informatievoorziening aan de huisarts in?
Wij sturen in ieder geval na de intake en na afsluiting van de behandeling een brief naar uw huisarts. Uw huisarts wordt minimaal één keer per jaar geïnformeerd of vaker als er belangrijke wijzigingen zijn in uw behandeling of gezondheidstoestand. Zo nodig overleggen wij met uw huisarts.

Als u bezwaar heeft tegen het feit dat wij uw huisarts informeren, dan kunt u dit kenbaar maken doormiddel van dit formulier. Altrecht zal de huisarts hiervan op de hoogte stellen en de huisarts alleen informeren bij start van de behandeling over welke behandelaar bij uw behandeling betrokken is en bij afsluiting van de behandeling. Deze berichten zullen geen zorginhoudelijke informatie bevatten.
N.B. In geval van risico's met sommige medicatie, denk aan bijvoorbeeld allergieën of nierproblemen, dan zal de hulpverlener de huisarts te allen tijde informeren. Ook in geval van ernstig gevaar, bijvoorbeeld bij een psychose of ernstige suïcidaliteit, kan de huisarts geïnformeerd worden.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

TOESTEMMINGSFORMULIER:

Ja, ik ga akkoord met het feit dat Altrecht mijn huisarts informeert over mijn behandeling bij Altrecht.

Nee, ik ga niet akkoord.

NAAM: ……

GEBOORTEDATUM:……

DATUM:……

HANDTEKENING:……

U kunt dit formulier ingevuld meenemen en overhandigen tijdens uw eerste gesprek.

Informatie voor kinderen, jongeren en hun ouder(s) / verzorger(s)

Informatie delen met de gemeente

Waarom geeft Altrecht informatie over kinderen en jongeren aan de gemeente?

Alle behandelingen in de geestelijke gezondheidszorg aan kinderen en jongeren tot 18 jaar worden sinds 1 januari 2015 betaald door de gemeente waarin de ouders wonen. De gemeente heeft daarom informatie nodig over de behandeling van kinderen en jongeren tot 18 jaar. De gemeente kan anders de gegeven zorg niet aan de zorginstelling betalen. In de Regeling Jeugdwet (augustus 2015) staat wettelijk vastgelegd welke informatie zorginstellingen moeten geven aan gemeenten. Ook Altrecht moet dus informatie geven aan de gemeente.

Welke informatie geeft Altrecht aan de gemeente?

- Algemene informatie, zoals burgerservicenummer, geboortedatum, geslacht, naam, postcode en huisnummer.
- Informatie over de zorg, zoals begindatum behandeling, einddatum behandeling, verwijsdatum, gegevens verwijzer, hoeveelheid bestede tijd en de hoofddiagnose.

Goed om te weten: Altrecht geeft geen informatie over de inhoud van de behandeling tenzij u[1] daar duidelijke toestemming voor heeft gegeven.

Moet de gemeente ook weten wat er aan de hand is (hoofddiagnose)?

Het kan zijn dat u echt niet wilt dat de gemeente de hoofdiagnose weet. Wanneer u de **privacyverklaring** in deze informatiemap invult, hoeft Altrecht de hoofddiagnose niet door te geven aan de gemeente. Hiernaast staat wat u daarvoor moet doen:

- Vul de privacyverklaring in en zet een handtekening op het formulier.
  - Bij kinderen onder 12 jaar tekent een van de ouders.
  - Bij kinderen van 12 tot 16 jaar tekent een ouder én het kind.
  - Jongeren vanaf 16 jaar tekenen zelf óf een ouder ondertekent de privacyverklaring. Een handtekening van een ouder is niet nodig voor jongeren vanaf 16 jaar.
- Het is belangrijk dat wij de privacyverklaring zo snel mogelijk naar de gemeente kunnen sturen. Altrecht kan pas een rekening naar de gemeente sturen voor de gegeven zorg, als de gemeente de privacyverklaring in haar bezit heeft.
- Neem daarom de ingevulde privacyverklaring mee naar het eerste (intake)gesprek. De behandelaar zorgt dat het formulier verder wordt ingevuld. Altrecht verstuurt de privacyverklaring naar de gemeente.

Goed om te weten: Als u het niet erg vindt dat de gemeente informatie krijgt over de hoofddiagnose, hoeft u niets te doen.

Hoe gaat de gemeente om met de gegevens?

Gemeenten moeten zorgvuldig omgaan met persoonlijke gegevens die zij ontvangen van zorginstellingen. Het kan zijn dat u daar vragen over heeft. U kunt dan zelf contact opnemen met uw gemeente voor meer informatie over het privacybeleid (het omgaan met persoonlijke gegevens).

Met vragen over de privacyverklaring en/of de behandeling kunt u terecht bij de behandelaar tijdens een behandelafspraak.

[1] U/jij en uw/jouw in de tekst leest niet gemakkelijk. We hebben daarom gekozen voor alleen de u-vorm.

Informatiebeveiligingsbeleid Altrecht

Datum: 25-01-2017
Versie: 1

Revisiehistorie

Datum	Versie	Omschrijving	Auteur
02-08-2016	0.1	Eerste opzet	Ralph Wagter
10-08-2016	0.2	Incl. commentaar HvK	
12-08-2016	0.3	Feedback verwerkt, organigrammen toegevoegd	Ralph Wagter
14-10-2016	0.7	Feedback verwerkt	Ralph Wagter / Bart Jan Schuit
25-11-2016	0.8	Functionaris voor gegevensbescher-ming toegevoegd	Bart Jan Schuit
8-12-2016	0.91	Verduidelijking termen en plaatsen se-curity officers	Ralph Wagter / Bart Jan Schuit
9-12-2016	0.92	Verduidelijking afbeeldingen	Bart Jan Schuit
12-12-2016	0.93	Feedback verwerkt	Naomi Meier
14-12-2016	0.94	Afbeeldingen aangepast Feedback verwerkt	Bart Jan Schuit Naomi Meier
25-01-2017	1	Feedback van RvB, LG B&OO en CAZ verwerkt	Naomi Meier

Formele reviewhistorie

Datum	Versie	Aandachtspunten	Reviewer

Inhoudsopgave

Voorwoord Raad van Bestuur

De veiligheid van informatie wordt steeds belangrijker in onze de samenleving. Niet alleen in onze samenleving maar ook binnen Altrecht. Toenemende uitwisseling van (patiënt)gegevens, digitalisering van onze werkzaamheden, maar ook interne en externe ontwikkelingen als bijvoorbeeld wijkgericht werken en aangescherpte privacy wetgeving, maken dat wij als Altrecht in het belang van verantwoorde zorg aan onze patiënten en een gezonde bedrijfsvoering aan informatieveiligheid gehoor willen geven.

Informatieveiligheid is de verantwoording van ons allemaal! Er wordt vaak gedacht dat informatieveiligheid de verantwoordelijkheid van het team ICT is, maar zij kunnen echter niet meer doen dan (on)zichtbare en voelbare ICT-maatregelen toepassen in de geautomatiseerde ondersteuning van al onze zorg- en bedrijfsprocessen. Informatieveiligheid valt en staat namelijk hoe de organisatie met de geautomatiseerde systemen en daarbij behorende processen omgaat. Ofwel: informatieveiligheid is een continue proces met bijbehorende procedures, richtlijnen en gedragingen. Het is een volwaardig onderdeel van ons kwaliteits- en veiligheidsmanagementsysteem.

Het document wat voor je ligt, beschrijft het informatiebeveiligingsbeleid van Altrecht zoals wij als organisatie invulling willen geven aan informatieveiligheid. Dat wij ons nog meer bewust gaan worden wat onze kritische zorg- en bedrijfsprocessen zijn, dat wij zicht hebben op de risico's die daarbij kunnen optreden, dat wij bewuste keuzes maken welke risico's aanvaardbaar zijn en welke risico's met maatregelen verminderd moeten worden. Het voorkomen van incidenten en als die toch plaatsvinden met verbetervoorstellen het risico tot een aanvaardbaar niveau (terug)brengen.

Alle leidinggevenden dienen naar aanleiding van dit document binnen hun eigen eenheid zelf invulling te geven aan genoemde taken, verantwoordelijkheden en bevoegdheden. Het is voor de eenheden belangrijk zelf na te gaan of en in welke mate zij zich hebben voorbereid op de effecten van mogelijke risico's op het gebied van informatieveiligheid.

Januari 2017

Raad van Bestuur Altrecht GGZ,

Mevr. Drs. R.H.M. Vernimmen Dhr. A.C de Grunt

1 Definitie en doelstelling Informatiebeveiliging Altrecht

Het informatiebeveiligingsbeleid is van toepassing op Altrecht als totale organisatie met alle onderdelen die nodig zijn om de behandeling van mensen met een ernstige en complexe psychiatrische aandoening, te garanderen. Het informatiebeveiligingsbeleid is tevens van toepassing op de gegevensuitwisseling van Altrecht met de patiënt, andere organisaties en de maatschappij. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie.

1.1 *Definitie van informatiebeveiliging*

Informatiebeveiliging wordt als volgt gedefinieerd:
Het treffen en onderhouden van een controleerbaar samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die nodig is om onze bedrijfs- en zorgcontinuïteit binnen gestelde wet- en regelgeving te garanderen.

Dit betekent dat verschillende maatregelen samen de informatiebeveiliging vormen en niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Ook betreft het maatregelen die procedureel, organisatorisch en technisch van aard zijn.

Het stelsel van beveiligingsmaatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren en transparant over informatiebeveiliging *te kunnen rapporteren*. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd.

Informatiebeveiliging is gericht op het realiseren van een *optimaal niveau van beveiliging.* Dit wordt bereikt door een zorgvuldige afweging van kosten/baten en beschikbaarheid versus vertrouwelijkheid. Het is met dit beleid niet de bedoeling te streven naar 100% veiligheid maar zorgvuldige keuzes te maken rondom de beveiliging van onze informatie.

1.2 *Waarom informatiebeveiliging*

Het opstellen van het informatiebeveiligingsbeleid en hieraan uitvoering geven, is noodzakelijk omdat:
- informatie waarde heeft. Beschikbaarheid, integriteit en vertrouwelijkheid van onze informatie is zeer belangrijk voor de zorgverlening aan onze patiënten en voor onze bedrijfsvoering.
- onze informatie en informatiesystemen altijd beschermd moeten worden.
- onze patiënten er van uit moeten kunnen gaan dat wij hun (persoons)gegevens beschermen.
- wet- en regelgeving[1] ons verplichten passende technische, organisatorische en procedurele maatregelen te treffen om te voldoen aan het beveiligen van gevoelige en waardevolle gegevens.

1.3 *Doelstelling informatiebeveiliging*

Informatiebeveiliging richt zich op de volgende drie aspecten van de informatievoorziening:
- *Beschikbaarheid*
  de informatie moet op de gewenste momenten beschikbaar zijn;
- *Integriteit*
  de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- *Vertrouwelijkheid*
  de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

[1] Bijvoorbeeld: wet bescherming persoonsgegevens, gebruik BSN nummers, NEN 7510, NEN 7512, 7513.

Altrecht heeft met informatiebeveiliging als doel:
- Het vergroten van het bewustzijn en de –wording bij medewerkers van het belang van beveiligingsmaatregelen en hun eigen handelen ter bescherming van gevoelige en waardevolle (persoons) gegevens.
- Het in stand houden van een organisatorische en technische infrastructuur die stabiel en betrouwbaar is voor wat betreft de informatieveiligheid.
- Continue inspelen en meebewegen op de steeds strengere wet- en regelgeving met betrekking tot informatieveiligheid/-beveiliging.

1.4 *Verantwoordelijkheid informatiebeveiligingsbeleid en maatregelen*

Informatiebeveiliging is de taak van iedereen die bij Altrecht werkzaam is. Patiënten en ketenpartners verstrekken hun (gevoelige) informatie aan ons omdat wij die informatie nodig hebben om ons werk te doen. Naast alle technische maatregelen met betrekking tot onze systemen en processen is het de verantwoordelijkheid van de medewerkers integer en vertrouwelijk met die gegevens om te gaan. Om dit te realiseren wordt van iedere medewerker een actieve bijdrage verwacht aan de veiligheid van onze geautomatiseerde systemen en de daarin opgeslagen informatie.

Een verdere uitwerking van taken en verantwoordelijkheden is beschreven in hoofdstuk 3.

1.5 *Beleidsproces en ondersteunende documentatie voor informatiebeveiliging*

Het maken van beleid, vertalen naar concrete plannen, evalueren en bijstellen van de plannen en het beleid, is onderdeel van de reguliere PDCA-cyclus die ook in het AO/IC-proces gehanteerd wordt. Het informatiebeveiligingsbeleid wordt ondersteund door procedures en inrichtingsdocumenten. Alle inhoudelijke documentatie is vindbaar op Altraplein, onder de functie Altrapedia en op de samenwerkingspagina Informatieveiligheid[2].

Minimaal de volgende documentatie dient aanwezig te zijn:
- Context waarbinnen Altrecht opereert
- Gedragscode computer- en internetgebruik
- Privacy beleid
- Verwijzing naar het informatiebeleidsplan omdat hier ook elementen van informatiebeveiliging in zijn opgenomen
- Risicoanalyse- en dataclassificatie-methode

Alle documenten behorende tot informatiebeveiliging worden opgenomen in het informatiesysteem (Information Security Management Systeem (ISMS)) dat onderdeel is van het kwaliteits- en veiligheidsmanagementsysteem van Altrecht.

[2] Samenwerkingspagina is nog onder constructie.

2 Informatiebeveiliging Altrecht

2.1 *Risicobeoordeling en afweging*

De aanpak van informatiebeveiliging binnen Altrecht is 'risk based'. Risico's worden beoordeeld en er vinden risicoafwegingen plaats.

De risicoafweging betreft een beoordeling van de mate van impact/schade die risico's kunnen hebben voor patiënten en/of Altrecht. Zo wordt gekeken naar zorginhoudelijke, juridische of commerciele schade, omdat bijvoorbeeld bijzondere persoonsgegevens of bedrijfsgevoelig geclassificeerde informatie onrechtmatig verwerkt[3] wordt, er specifieke dreigingen bestaan, de integriteit van informatie niet kan worden gegarandeerd of hogere beschikbaarheidseisen worden gesteld dan worden behaald.

Altrecht kan op meerdere manieren omgaan met (rest)risico's:
- risicodragend
- risiconeutraal
- risicomijdend

Risicodragend wil zeggen dat risico's geaccepteerd worden. Dat kan zijn omdat de kosten van de beveiligingsmaatregelen de mogelijke schade overstijgen. Maar de Raad van Bestuur en de leidinggevenden kunnen ook besluiten om niets te doen, ondanks dat de kosten niet hoger zijn dan de schade die kan optreden. De beveiligingsmaatregelen die hierbij worden genomen zijn veelal van repressieve aard.
Onder **risiconeutraal** wordt verstaan dat er dusdanige beveiligingsmaatregelen worden genomen dat dreigingen óf niet meer manifest worden óf, wanneer de dreiging wel manifest wordt, de schade als gevolg hiervan geminimaliseerd is. De meeste beveiligingsmaatregelen die hierbij voorkomen zijn een combinatie van preventieve, detectieve en repressieve maatregelen.
Onder **risicomijdend** wordt verstaan dat er zodanige maatregelen worden genomen dat de dreigingen zo veel mogelijk worden geneutraliseerd, zodat de dreiging niet meer tot een incident leidt. Veel van de maatregelen binnen deze strategie hebben een preventief karakter.

Altrecht kiest voor **risicomijdend** bij de maatregelen vanuit informatiebeveiliging op de zorgprocessen en **risiconeutraal** bij het treffen van maatregelen bij de processen van de ondersteunende diensten. Indien in bepaalde gevallen (of bij bepaalde organisatie-eenheden) gekozen wordt voor risicodragend[4] dan is dat is dit een bewuste keuze van de leidinggevende waarvan de gevolgen gedragen dienen te worden. Uiteraard blijven we ook bij deze keuze voldoen aan de relevante wet- en regelgeving.

2.2 *Uitgangspunten*

Bij de toepassing van informatiebeveiliging worden de volgende uitgangspunten gehanteerd:
1. Altrecht streeft ernaar aantoonbaar te voldoen aan de eisen gesteld in het toetsingsreglement van de norm NEN7510, Informatiebeveiliging in de zorg.
2. Altrecht voldoet aan alle van toepassing zijnde wet- en regelgeving op gebied van informatiebeveiliging.
3. Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Alle organisatie-eenheden van Altrecht hebben hiertoe verantwoordelijkheden voor informa-

[3] Het woord 'verwerkt' is in brede zin genoemd. Dit houdt o.a. in het opslaan, inzien, vernietigen, transporteren van data, zo ook het verlies van data.
[4] Afwijken kan pas na afstemming met de Functionaris Gegevensbescherming/commissie Informatieveiligheid en na toestemming van de Raad van Bestuur.

tiebeveiliging toegewezen en vastgelegd. De in hoofdstuk 3 beschreven organisatie van informatiebeveiliging vormt hierbij de leidraad.

4. Altrecht stelt voldoende mensen en middelen beschikbaar om haar informatie te kunnen beveiligen volgens de wijze die volgt uit dit beleid.
5. Wanneer (onderdelen van) Altrecht samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging indien van toepassing. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
6. De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van Altrecht zijn geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
7. Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van maatregelen die volgen uit het realiseren van het informatiebeveiligingsbeleid.
8. Altrecht voert een actief beleid om het beveiligingsbewustzijn van leidinggevenden en medewerkers te stimuleren, dit geldt ook voor ingehuurd en tijdelijke medewerkers evenals vrijwilligers.
9. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de Raad van Bestuur een sanctie opleggen conform hetgeen hierover met betrekking tot op non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in de CAO GGZ of beëindiging van de inhuurovereenkomst cq. vrijwilligersovereenkomst.
10. Altrecht heeft voldoende maatregelen getroffen voor de fysieke beveiliging van ruimtes en de digitale verwerking van gegevens.
11. Altrecht heeft maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
12. Bij de ontwikkeling en aanschaf van informatiesystemen wordt in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht besteed aan informatiebeveiliging.
13. Altrecht heeft adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden (vastgesteld in de risicoanalyse). Er is een continuïteitsplan ICT aanwezig passend bij de dienstverlening van Altrecht.
14. Als onderdeel van het beleidsproces voor informatiebeveiliging wordt binnen Altrecht door interne (Functionaris voor Gegevensbescherming (FG)) en externe partijen (accountant) toegezien op de naleving van het informatiebeveiligingsbeleid.
15. Altrecht beschikt over middelen voor het melden en afhandelen van informatiebeveiligingsincidenten. Alle gemelde beveiligingsincidenten worden naast de registratie geëvalueerd met de eigenaar van de betreffende informatie ter verbetering van informatiebeveiliging.

3 Organisatie van informatiebeveiliging

In dit hoofdstuk wordt de organisatie van informatiebeveiliging binnen Altrecht beschreven. Het is van belang dat de taken, verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze zijn toegewezen. Het beschrijven en vastleggen van taken en verantwoordelijkheden met betrekking tot informatiebeveiliging maakt het mogelijk dat medewerkers in de uitvoer van hun werkzaamheden makkelijker rekening kunnen houden met informatieveiligheid en indien nodig door hun leidinggevende hierop aangesproken kunnen worden.

3.1 *Betrokkenen informatiebeveiliging*

Binnen informatiebeveiliging is een aantal generieke rollen te onderscheiden. Zie onderstaande tabel. Een groot deel van de rollen is binnen de eenheid Informatisering & Zorgadministratie belegd. De verschillende betrokkenen maken met systeem- en proceseigenaren afspraken over de uitvoering van de (beveiliging)taken. De systeem- en proceseigenaren zijn namelijk verantwoordelijk voor het bepalen van het risicoprofiel en de daarbij behorende set aan maatregelen om het risico tot een acceptabel niveau te brengen.

Tabel 1: Generieke rollen voor informatiebeveiliging:

Rol	Verantwoordelijkheden
Verantwoordelijke (systeemeigenaar)[5]	Beslissingsrecht voor het informatiesysteem, c.q. de gegevensverzameling Bepalen van de beveiligingseisen
Ontwikkelaar / Leverancier	Ontwikkelt en onderhoudt het informatiesysteem conform de (beveiliging)eisen die door Altrecht zijn gesteld Denkt actief mee over de realisatie en de beveiliging van het informatiesysteem, c.q. de gegevensverzameling
Functioneel beheerder / Databasebeheerder	Ondersteunen van de verantwoordelijke bij het bepalen van de beveiligingseisen Operationele instandhouding van het informatiesysteem Ziet toe op een juiste werking van het informatiesysteem
Technisch beheerder	Exploitatie van de technische infrastructuur Ziet toe op een juiste technische werking van de technische infrastructuur
Gebruiker/medewerker	Gebruik van het informatiesysteem Naleving van beveiligingsrichtlijnen en –procedures

De *medewerker* van Altrecht heeft allereerst zelf de verantwoordelijkheid te werken volgens de gemaakte afspraken en maatregelen die zijn gedefinieerd als voortvloeisel van het informatiebeveiligingsbeleid. De *teamleiders* en *leidinggevenden* zijn verantwoordelijk voor het toezien op het juiste gebruik en om eventuele ongewenste werkwijzen en handelingen op het gebied van informatiebeveiliging en privacy te signaleren en binnen het eigen team of de eigen eenheid te verhelpen. Hierbij kunnen zij worden ondersteund door een *aandachtsfunctionaris informatieveiligheid*.

Vanuit de eenheid *Informatisering & Zorgadministratie* (I&ZA)worden alle informatiesysteem en –infrastructuren ondersteund. De eisen van systeem- en proceseigenaar, de geldende wet- en regelgeving en de technische mogelijkheden bepalen met name de inrichting van de informatiebeveiliging van Altrecht. Gezien de rol en betrokkenheid van I&ZA bij het invulling geven aan relevante

[5] Nog niet ieder systeem heeft een eigenaar, maar op dit moment worden de systemen en processen in kaart gebracht door I&ZA om vervolgens waar dat nog nodig is eigenaren aan systemen en processen te koppelen. Een voorbeeld van een systeem en een eigenaar is het EPD waar de EPD commissie eigenaar van is.

wet- en regelgeving op het gebied van informatieveiligheid is de rol aandachtsfunctionaris informatieveiligheid uitgebreid naar de rol van *Information Security Officer* (ISO) binnen de eenheid.

Vanuit de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywetgeving, stelt Altrecht een *Functionaris Gegevensbescherming* (FG)[6] aan om de privacy te bewaken en te zorgen dat Altrecht voldoet aan deze wetgeving. Naast concrete eigen werkzaamheden ondersteunt de FG in samenwerking met *commissie Informatieveiligheid* de organisatie. Binnen de commissie Informatieveiligheid is de rol van privacy functionaris belegd. De commissie houdt zich in die hoedanigheid bezig met de gemelde informatebeveiligingsincidenten in het kader van de wet datalekken.

De *Raad van Bestuur* is eindverantwoordelijk voor informatieveiligheid en daarmee voor het informatiebeveiligingsbeleid. Het beleid wordt minimaal 1x per 2 jaar geëvalueerd. Per trimester wordt er door alle eenheden en de functionaris Gegevensbescherming aan de Raad van Bestuur gerapporteerd over:
- Informatiebeveiligingsincidenten en hoe deze zijn afgehandeld.
- Adviesaanvragen op het gebied van informatiebeveiliging.
- Status van de implementatie van het informatiebeveiligingsplan.

3.2 *Rollen en functies voor informatiebeveiliging*

Veel onderdelen binnen onze organisatie zijn bij informatiebeveiliging betrokken. Een hiërarchisch en functioneel organigram is op pagina 14 te vinden. In dit informatiebeveiligingsbeleid worden de verantwoordelijkheden van de volgende functies en rollen beschreven:
- Raad van Bestuur (Portefeuillehouder informatiebeveiliging)
- Functionaris voor de gegevensbescherming (FG)
- Leidinggevenden eenheden
- Leidinggevende I&ZA
- Leidinggevende HRM
- Aandachtsfunctionaris Informatieveiligheid
- Information Security Officer (ISO)

Raad van Bestuur (Portefeuillehouder informatiebeveiliging)

De Raad van Bestuur is eindverantwoordelijk voor alle activiteiten binnen Altrecht en dus ook voor informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging omvat:
- het vaststellen van het informatiebeveiligingsbeleid en daaruit voortvloeiende richtlijnen
- het toezien op de naleving van het informatiebeveiligingsbeleid door de organisatie-eenheden
- het evalueren van de toepassing en werking van het informatiebeveiligingsbeleid op basis van rapportages over informatiebeveiliging
- risicoanalyse uit laten voeren en vaststellen

Functionaris voor de gegevensbescherming (FG)

Privacy hangt nauw samen met informatiebeveiliging. Vanuit de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywetgeving, dient Altrecht een FG aan te stellen om de privacy te bewaken en te zorgen dat Altrecht voldoet aan deze wetgeving. Onderdeel van deze wet is het uitvoeren van gegevensbescherming effectbeoordeling (ofwel Privacy Impact Assessment, PIA) voor nieuwe en bestaande systemen met persoonsgegevens, het informeren van patiënten en medewerkers over gegevensverwerkingen en het hebben van passende maatregelen voor gegevensbescherming. De FG is zodoende verantwoordelijk voor:
- het adviseren van de Raad van Bestuur en andere leidinggevenden over informatiebeveiliging en adviseren en informeren van medewerkers en patiënten rondom persoonsgegevensverwerkingen.

[6] Het voornemen is om deze functie binnen de eenheid Bestuur- en Organisatieondersteuning te positioneren.

- opstellen meerjarenplan rondom informatiebeveiliging en bevorderen informatiebeveiligingsparagraaf in de reguliere jaarplannen van de eenheden binnen Altrecht.
- opstellen jaarverslag rondom informatiebeveiliging en privacy met hierin de incidenten, voortgang over het meerjarenplan en toe te wijzen middelen voor het komende jaar.
- toezicht houden op de naleving van informatiebeveiligingsmaatregelen, de uitwerking van de NEN7510 binnen Altrecht.
- coördineren van de interne audit en bijhouden van de resultaten.
- m.b.t. Wet Bescherming persoonsgegevens/AVG juridische aanbevelingen voor een betere bescherming van verwerkingen van persoonsgegevens.
- het op kennis brengen en houden van bewustzijn rondom gegevensbescherming in de organisatie.
- het bijhouden van een register van alle persoonsgegevensverwerkingen.
- adviseren bij en controleren van PIA's.
- het verzamelen van informatie over en het centraal registreren van (potentiële) informatiebeveiligingsincidenten en beveiligingslekken.

De FG heeft veelal een coördinerende rol in deze verantwoordelijkheden, waarbij de uitvoering veelal ligt bij de leidinggevenden en de commissie Informatieveiligheid. De FG rapporteert direct aan de Raad van Bestuur en geniet rechten vergelijkbaar met een ondernemingsraad, zoals het onafhankelijk uitvoeren van zijn taak en ontslagbescherming.

Leidinggevenden van de eenheden

De activiteiten met betrekking tot informatiebeveiliging worden binnen Altrecht bewaakt door de leidinggevenden. De leidinggevenden zijn verantwoordelijk voor de ondersteuning en bewaking van de realisatie en naleving van het informatiebeveiligingsbeleid en de bijbehorende richtlijnen inclusief het doorvoeren van maatregelen in de eigen eenheid. Dit houdt, binnen de eigen eenheid, de verantwoordelijkheid in voor:

- de naleving van de Wet Bescherming persoonsgegevens en aanpalende wetgeving.
- positieve en actieve houding ten aanzien van informatiebeveiliging.
- fungeren als voorbeeldfunctie.
- toezicht houden op de naleving van informatiebeveiligingsmaatregelen.
- opstellen van verbeterplannen voor de eigen teams, uitvoer van deze plannen.
- autoriseren van medewerkers: standaardautorisatie op basis van de functie in het systeem.
- informatiebeveiliging behandelen in werkoverleg, jaargesprekken, etc.
- afhandelen van vertrouwelijke informatiebeveiligingsincidenten.
- rapporteren van informatiebeveiligingsincidenten via de meldingen in Topdesk.
- controle en registratie, het bewaken van het niveau van informatiebeveiliging.
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn bij alle medewerkers.

Leidinggevende Informatisering & Zorgadministratie

Naast de beschreven verantwoordelijkheden voor de leidinggevenden van de eenheden is de leidinggevende I&ZA verantwoordelijk voor de instandhouding van de centrale geautomatiseerde informatievoorziening. Dit heeft op vele onderdelen raakvlakken met informatiebeveiliging. Dit leidt tot de volgende verantwoordelijkheden:

- verantwoordelijk voor de inrichting en uitvoering van de informatiebeveiligingsprocessen binnen de ICT-processen.
- verantwoordelijk voor de inrichting en beveiliging van de centrale ICT-infrastructuur.
- inrichten en rapporteren over de kwetsbaarheden van de ICT-infrastructuur, zowel de interne infrastructuur als de systemen die vanaf het internet benaderbaar zijn.
- bijhouden van de informatiestromen vanuit het applicatielandschap en het (laten) uitvoeren van een risicoanalyse op deze informatiestromen met de eigenaren van de informatie(systemen).

Leidinggevende HRM

Naast de beschreven verantwoordelijkheden voor de leidinggevenden van de eenheden is de leidinggevende HRM verantwoordelijk voor het personeelsbeleid van Altrecht. De uitvoering hiervan vindt gedeeltelijk centraal en gedeeltelijk decentraal plaats. Er is een relatie tussen personeelsbeleid en informatiebeveiliging, onder andere daar waar het de selectie en het ontslag van personeel betreft. Dit dient op een zorgvuldige manier te geschieden met de waarborging van een goede informatiebeveiliging. Hiertoe bewaakt de leidinggevende HRM de samenhang tussen personeelsbeleid en informatiebeveiliging en is verantwoordelijk voor:

- het borgen van het indiensttredingsproces, de doorstroom van medewerkers en het uitdiensttredingsproces.
- het zorgdragen voor het voldoen aan de gestelde eisen van contracten van interne en externe medewerkers met betrekking tot informatiebeveiliging.
- het opstellen van het sanctiebeleid vanuit de aspecten van informatiebeveiliging en rapporteren over de handhaving hiervan.

Aandachtsfunctionaris Informatieveiligheid

Om de continuïteit van informatiebeveiliging op alle niveaus binnen Altrecht te borgen en ter ondersteuning van leidinggevenden en teamleiders dient de rol aandachtfunctionaris Informatiebeveiliging te worden beleggen binnen de teams of de eenheid. De aandachtsfunctionaris is aanspreekpunt voor de medewerkers op het gebied van Informatieveiligheid en –beveiliging. Concreet:

- De aandachtsfunctionaris is vraagbaak en draagt zorg dat er met regelmaat binnen het team/de teams aandacht is voor het onderwerp. Bijvoorbeeld in het werkoverleg of op de teampagina op Altraplein.
- De aandachtsfunctionaris heeft een signalerende rol bij het handelen rondom informatieveiligheid. Waar nodig spreekt hij/zij collega's aan en/of bespreekt de mogelijke risico's met teamleider of leidinggevende.
- De aandachtsfunctionaris is aanspreekpunt voor de FG (functionaris gegevensbescherming) en de commissie Informatieveiligheid om bijvoorbeeld aandacht aan nieuwe ontwikkelingen te besteden of indien nodig bij informatiebeveiligingsincidenten en/of verbetervoorstellen die hieruit komen.

Information Security Officer (ISO) binnen de eenheid I&ZA[7]

Gezien de rol en betrokkenheid van de eenheid Informatisering & Zorgadministratie (I&ZA) bij het invulling geven aan relevante wet- en regelgeving op het gebied van informatieveiligheid en -beveiliging is de rol aandachtsfunctionaris informatieveiligheid uitgebreid naar de rol van Information Security Officer (ISO) binnen deze eenheid. De ISO coördineert en ondersteunt het documentenbeheer, de risicoanalyses en het doorvoeren van maatregelen in de eigen eenheid, daarbij rekening houdend met het informatiebeveiligingsbeleid en de bijbehorende richtlijnen. De ISO is verantwoordelijk voor:

- het adviseren van de leiding van de eenheid over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen de eenheid.
- het analyseren en beoordelen van de aard, omvang en oorzaak van informatiebeveiligingsincidenten waarbij de eenheid betrokken is.
- het organiseren van de evaluatie van de afhandeling van informatiebeveiligingsincidenten.
- het adviseren van de leiding van de eenheid over de te nemen preventieve en herstelacties bij informatiebeveiligingsincidenten.
- het coördineren van de uitvoering van preventieve en herstelacties.

[7] Er moet nog worden nagegaan of de eenheden HRM en V&F voldoende hebben aan een aandachtsfunctionaris of de rol ISO ook voor deze eenheden van toepassing is. Dit gezien de rol en betrokkenheid van deze eenheden m.b.t. invulling geven aan relevante wet- en regelgeving op het gebied van Informatieveiligheid en –beveiliging.

- rapporteren aan de FG/commissie Informatieveiligheid over de implementatiegraad van de maatregelen die uit de risicoanalyse voor de eenheid zijn opgesteld.
- uitvoeren van de interne audit ter toetsing of de eenheid voldoet aan NEN 7510.
- het coördineren van het documentenbeheer m.b.t. informatieveiligheid en –beveiliging binnen de eenheid.
- het onderhoud en beheer van de informatiesysteem (ISMS).

Commissie Informatieveiligheid

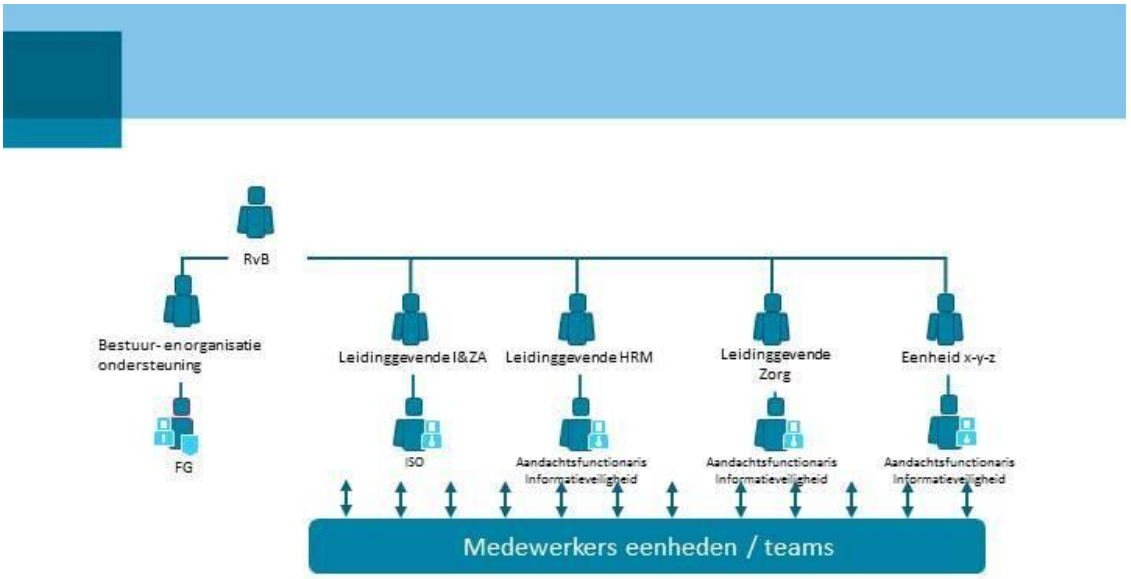
De commissie Informatieveiligheid[8] ondersteunt de organisatie:

- het analyseren en beoordelen van de aard, omvang en oorzaak van informatiebeveiligingsincidenten.
- het organiseren van de evaluatie van de afhandeling van informatiebeveiligingsincidenten.
- het adviseren van de organisatie over de te nemen preventieve en herstelacties bij informatiebeveiligingsincidenten.
- het centraal informeren van gebruikers over (potentiële) informatiebeveiligingsincidenten.
- het coördineren van de uitvoering van preventieve en herstelacties.
- in het opstellen en monitoren meerjarenplan.
- in het opstellen van het jaarverslag.
- In het toetsen en actualiseren informatiebeveiligingsbeleid.

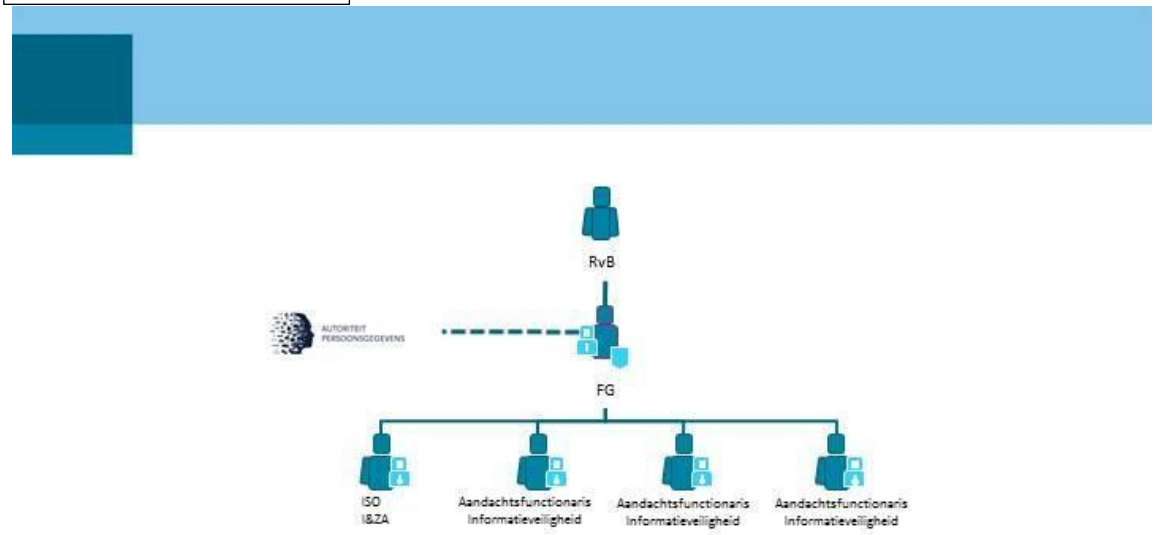
[8] Commissie Informatieveiligheid vervangt de commissie datalekken en zal breder gaan functioneren dan enkel onderzoeken informatiebeveiligingsincidenten Voorzitter van de commissie is de Functionaris gegevensbescherming (FG). Commissieleden: I&ZA, HRM, V&F(??) Zorg .

Bijlage: Organigram

Hiërarchisch:



Functioneel:



Protocol melden datalek

De Wet bescherming persoonsgegevens is sinds 1 januari 2016 uitgebreid met een artikel over datalekken. Vanaf 1 april 2016 is het wettelijk verplicht om een datalek te melden. Zowel grootschalige inbraak als ieder kwijtraken, diefstal of onbevoegd gebruik van persoonsgegevens[1] telt als een datalek. Wie gegevens laat lekken of persoonsgegevens verwerkt zonder zich netjes aan de wet te houden, loopt kans op boetes die kunnen oplopen tot € 820.000,- . Tevens verplicht de wet tot het treffen van maatregelen voor het voorkomen, herkennen en het beperken van de gevolgen van datalekken.

Wat is een datalek?
Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek.

Het risico op datalekken is binnen Altrecht steeds groter omdat persoonsgegevens in onze systemen en/of op draagbare media (telefoon, laptop, USB-stick) zijn opgeslagen. Wanneer deze persoonsgegevens onrechtmatig worden verwerkt of verloren raken, is er sprake van een datalek.

Onrechtmatige verwerking
Aanpassen/veranderen van persoonsgegevens, onbevoegde toegang tot, afgifte van persoonsgegevens.

Verloren raken
Definitief verlies persoonsgegevens terwijl daarvan geen back-up bestaat.

Voorbeelden van een datalek zijn:
- het laten liggen, kwijt raken of gestolen worden laptops, telefoons of USB-sticks,
- het kwijt raken van wachtwoorden die toegang geven tot een gegevensbestand,
- een serverhack waarbij gegevens worden 'gestolen',
- een printje met privacygevoelige informatie laten liggen op de printer of je bureau,
- sturen van een mailing met adressen in het CC-veld i.p.v. in het BCC-veld
- het doorgeven van persoonsgegevens aan een persoon of organisatie die het niet had moeten hebben.
- het verlies van gegevens zoals bij een brand terwijl er geen back up beschikbaar is.

Doel van de wet datalekken
Het doel van het melden van datalekken is het beter beschermen van de persoonsgegevens in de systemen van de organisatie.

Wanneer een datalek melden?
Ieder incident waarbij persoonsgegevens onrechtmatig worden verwerkt of verloren raken, dient zonder onnodige vertraging te worden gemeld bij de leidinggevende en via Self Servicedesk Informatisering & Zorgadministratie bij de Privacy functionaris[2].

Of de melding ook gemeld moet worden bij de Autoriteit Persoonsgegevens[3] dient Altrecht zelf te bepalen aan de hand van de volgende vragen:
1. Is er sprake van een datalek?

[1] Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
[2] Deze rol is bij de Veiligheidskundige belegd.
[3] Voorheen College Bescherming Persoonsgegevens

2. Zijn de verwerkte persoonsgegevens daardoor blootgesteld aan verlies of onrechtmatige verwerking?
3. Heeft deze blootstelling geleid tot ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens of de privacy van de betrokkenen?

Indien alle 3 de vragen positief worden beantwoord, dient een melding bij de Autoriteit Persoonsgegevens te worden gedaan.

Wanneer een datalek ongunstige gevolgen (bijvoorbeeld identiteitsfraude, discriminatie of reputatieschade) heeft voor betrokkenen dient naast een melding aan de Autoriteit Persoonsgegevens ook de betrokkene(n) geïnformeerd te worden.

Indien de gelekte gegevens onleesbaar zijn door versleuteling of het mogelijk is gestolen gegevens op afstand aantoonbaar succesvol te verwijderen dan hoeven getroffen personen niet geïnformeerd te worden.

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker die direct of indirect kennis draagt of krijgt van een datalek is verplicht dit direct te melden via Self Servicedesk Informatisering & Zorgadministratie en ook kenbaar te maken bij zijn leidinggevende.
2. De Privacy functionaris is verantwoordelijk voor het (laten) onderzoeken van het incident, het indien nodig melden bij Autoriteit Persoonsgegevens en het indien nodig informeren van de betrokkenen om wiens persoonsgegevens het gaat.
3. De Privacy commissie[4] ondersteunt de Privacy functionaris bij het onderzoeken, het rapporteren en doen van verbetervoorstellen.
4. De leidinggevende is verantwoordelijk voor het ondernemen van preventieve en repressieve acties en mede uitvoer te geven aan verbeterplan/-advies.
5. Op basis van de, gedurende een jaar, ontvangen meldingen analyseert de Privacy functionaris en stelt een verbeterplan of –advies op. Dit plan of advies wordt opgenomen in de jaarlijkse systeembeoordeling en de jaarrapportage.
6. Minimaal jaarlijks beoordeelt de Privacy functionaris of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

Melden datalek

1. De medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens meldt dit direct via Self Servicedesk Informatisering & Zorgadministratie en meldt dit aan zijn/haar leidinggevende.
2. De Privacy functionaris, in samenwerking met de privacy commissie onderzoekt het incident. Hierbij is aandacht voor de volgende aspecten:
    a. Wat is de aard van de datalek
    b. Wat is de oorzaak dat dit incident heeft plaatsgevonden
    c. Is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures
    d. Is de organisatie verwijtbaar
    e. Van het incident wordt een verslag gemaakt en vastgelegd
3. De Privacy functionaris meldt indien nodig via het webformulier het incident bij de Autoriteit Persoonsgegevens.

[4] Bestaat uit functionarissen uit meerdere geledingen binnen Altrecht. O.a. Jurist, HRM, Informatisering & Zorgadministratie en zorg.