

**Regionaal Elektronisch Patiënt Dossier Midden-Holland
Beveiliging tegen ongeoorloofd gebruik**



Inleiding

In het ontwikkelen, invoeren en toepassen van het Regionaal Elektronisch patiënt Dossier voor de regio Midden-Holland is het thema “beveiliging tegen ongeoorloofd gebruik” een uitermate belangrijk thema. “Zonder adequate beveiliging geen regionaal EPD”.

In dit document wordt compact beschreven waar het regionaal patiënt dossier uit bestaat. Vervolgens wordt weergegeven op welke manier de informatie die opgeslagen is in de verschillende informatiesystemen beveiligd is tegen ongeoorloofd gebruik. Hierbij worden achtereenvolgens worden de rollen van de patiënt, de zorgverlener, de techniek en de Regionale Beheer Organisatie beschreven.

Het Regionaal Elektronisch Patiënt Dossier

Het Regionaal Elektronisch Patiënt Dossier is in de kern de **inzage** in het elektronisch dossier van een patiënt zoals dat beheerd wordt door huisarts, apotheker en ziekenhuisapothek. Met deze inzage heeft de raadpleger toegang tot:

- de zgn. professionele samenvatting van het dossier zoals dat beheerd wordt door de huisarts, en
- het medicatie dossier zoals dat tot stand komt door het samenvoegen van gegevens m.b.t. uitgegeven medicatie zoals die vastgelegd zijn door:
 - ▶ apotheker en
 - ▶ ziekenhuisapothek.

Deze inzage in de dossiers van huisartsen en apothekers is al een bestaande toepassing. De apothekers kunnen op de Dienst Apotheek Midden-Holland (onderdeel van Spoedzorg Midden-Holland) gegevens inzien en toevoegen aan het systeem van een lokale apotheker. Dit is het huidige Waarneem Dossier Apothekers. (WDA)

De huisartsen kunnen op de Huis Artsen Post (onderdeel van Spoedzorg Midden-Holland) gegevens inzien en toevoegen aan het systeem van een individuele huisarts (die aangesloten is). Dit is het huidige Waarneem Dossier Apothekers dat voor ca 55% van de huisartsen in werking is. Eind 2007 hoopt men 85%-90% bereikt te hebben.

In de startfase hebben zorgverleners uit de volgende groepen toegang tot de dossiers van huisarts, apotheek en ziekenhuisapothek.

- ▶ Artsen en verpleegkundigen op de Spoedeisende Hulp van het Groene Hart Ziekenhuis (onderdeel van Spoedzorg Midden Holland)
- ▶ Specialistisch verpleegkundigen en Verpleegkundig specialisten actief in de transmurale zorg voor patiënten met Diabetes, COPD, Hartfalen, Wondzorg, Oncologisch aandoeningen, Palliatieve Zorg, Reuma, Incontinentie.
- ▶ Specialisten en verpleegkundigen in het circuit Volwassen van GGZ Midden-Holland
- ▶ Verpleeghuisartsen werkzaam bij de verpleeghuizen van Zorgpartners Midden-Holland

Later volgen de Medisch Specialisten in het Groene hart Ziekenhuis

In een later stadium worden mogelijk ook de dossiers ontsloten zoals die beheerd worden door Zorgpartners (Verpleeg en Verzorgingshuizen), Vierstroom (thuiszorg) Rivierduinen (GGZ-MH) en Groene hart Ziekenhuis. Inzage in het dossier is alleen voorbehouden aan zorgverleners die daartoe bevoegd zijn.



The screenshot shows the 'Zorgportaal' interface for a patient named M.K. Jansen van het Laar. The header includes the logo and navigation tabs: 'Patiëntdossiers', 'Patiëntportaal', 'Zorgportaal Beheer', and 'Patiëntportaal Beheer'. The patient's name and address are displayed, along with contact information for the practice (HP Borgele). There are tabs for 'Overzicht', 'Medicatie', and 'Deelcontacten'. The main content area is divided into 'Actuele Medicatie' and 'Historische Medicatie', both showing a list of Mercilon 25mg tablets with start and end dates. On the right, there are sections for 'Allergieën' (listing Amoxicilline and Peneciline), 'Contra-indicaties' (listing Diabetes Type 2), and 'Episodes' (listing Transpiratie problemen, Beenbreuk, and Keelontsteking).

Rol van de patiënt.

Passieve toestemming

De rol van de patiënt bestaat uit actief of passief toestemming geven voor inzage. NPCF heeft in haar “10 punten voor het EPD”¹ aangegeven dat zij voorstander is van actieve toestemming. Actieve toestemming wil zeggen dat aan elke patiënt toestemming gevraagd moet worden door elke zorgverlener die een elektronisch patiënt dossier van de patiënt beheert, om deze gegevens te delen met andere zorgverleners. Passieve toestemming gaat uit van het informeren van de patiënt die op grond daarvan de zorgverlener kan verzoeken het dossier of delen daarvan te blokkeren voor inzage door andere zorgverleners. Wettelijk voldoet deze benadering. Omwille van de uitvoerbaarheid van de toestemmingsverlening kiezen de gezamenlijke zorgaanbieders/zorgverleners voor de “passieve toestemming”. De belangrijkste reden hiervoor is dat het onhandig is als huisartsen, apothekers en het Groene Hart Ziekenhuis allen op hun eigen manier voorlichting en informatie gaan verstrekken over een zelfde onderwerp aan de zelfde groep patiënten/cliënten/burgers. In het kader van de passieve toestemming wordt dus een gezamenlijke informatiecampagne in de regio uitgevoerd. Deze zal in overleg met de patiënten/consumenten organisatie “ZORGBELANG” worden vorm gegeven.

Informatie afschermen

De patiënt kan aan de zorgverlener verzoeken om de gegevens af te schermen voor gebruik door anderen dan de “eigen” zorgverlener. (Dat geldt dan ook voor de SEH/SPOEDZORG) Hoe dat moet wordt beschreven onder het hoofdstuk [Regionale Beheer Organisatie SPITZ Midden-Holland](#).

Rol van de zorgverleners

De zorgverlener (huisarts / apotheker) heeft (afhankelijk van de mogelijkheden van het eigen informatiesysteem) de mogelijkheid om het dossier van de patiënt “dicht” te zetten dan wel delen (episodes) af te schermen.

Onvolledig Dossier

Indien door de zorgverlener op verzoek van de patiënt informatie afgeschermd wordt moet de patiënt geïnformeerd worden dat zijn/haar patiëntendossier onvolledig is indien het door anderen geraadpleegd wordt.

Deze wijze van afschermen is de 0-de beveiligingslaag

De technische beveiliging van het regionaal EPD

Naast het afschermen van het dossier door de beherend zorgverlener zelf, worden er een aantal technisch mogelijkheden toegepast die het onmogelijk maken om ongeoorloofd dossiers in te zien of onopgemerkt ongeoorloofd dossiers in te zien. Dat werk als volgt.

Beveiligde toegang

Ingelogd via het eigen informatiesysteem

Huisartsen en Apothekers kunnen, eenmaal ingelogd in hun eigen informatiesysteem van DAM en HAP relevante informatie opvragen bij collega's en informatie terug schrijven in de dossiers van de collega's. Identificatie vindt plaats op basis van de zgn. AGB-code.

Inloggen via UZI-pas / AGB-code

Andere zorgverleners krijgen toegang tot de dossiers via het Zorgportaal. Het Zorgportaal is een dienst die via het Internet werkt. Toegang tot de dossiers kan alleen verkregen worden als de

¹ NPCF; Het elektronisch patiëntendossier, De tien belangrijkste punten. November 2006

zorgverlener zich kan identificeren en authenticeren op het Zorgportaal. Hiervoor moet de zorgverlener beschikken over een UZI-pas, ofwel een Unieke Zorgverleners Identificatie Pas. Deze pas kan aangevraagd worden bij het UZI-register en wordt alleen verstrekt als de aanvrager

- werkzaam is bij een geregistreerde abonnee van het UZI-register² (bijvoorbeeld een ziekenhuis)
- zich kan legitimeren; via paspoort of rijbewijs
- een pasfoto verstrekt die voldoet aan de eisen uit de Wet op de Identificatieplicht
- ingeschreven is als in het zgn. BIG register³ (registratie van Beroepsbeoefenaren Individuele Gezondheidszorg)

De beheerder van het Zorgportaal registreert zorgverleners met hun UZI-gegevens of AGB-code. Indien een zorgverlener toegang zoekt tot het zorgportaal Worden de AGB-code of UZI gegevens met elkaar vergeleken. Bij een juiste “match” krijgt de zorgverlener toegang tot het Zorgportaal.

Zorgportaal Uw praktijk op het internet

Inloggen met UZI-pas

Pincode

Inloggen

Hulp nodig?
Commodum poenicantibus
phaleris Aurora roseum
quatiens lacertum caelum
inequitabat.

© Protomics 2007 | Diabetes Praktijkondersteuning Prototype v0.01

Dit is de 1^e beveiligingslaag.

² Zie www.uziregister.nl

³ Zie www.ribiz.nl

Autorisatie

Vervolgens kan de zorgverlener alleen die dossier raadplegen waarvoor hij/zij geautoriseerd is. De Regionale Beheer Organisatie legt van elke zorgverlener of groep zorgverleners vast wat hun toegangsrechten zijn. De zorgverlener kan toegang hebben tot:

- Het medicatie dossier dat ontstaat door inzage in de verstrekte medicatie apotheker/apotheek houdend huisarts en ziekenhuisapotheek en/of
- De gedeeltelijke professionele samenvatting (= dossier zonder inzage in episodes) of
- De volledige professionele samenvatting van het dossier van de patiënt dat de huisarts heeft.

The screenshot shows the 'Zorgportaal' web application. The main header includes the logo and the text 'Uw praktijk op het internet'. Below the header, there are navigation tabs: 'Patiëntdossiers', 'Patiëntportaal', 'Zorgportaal Beheer', and 'Patiëntportaal Beheer'. The 'Zorgportaal Beheer' tab is active, and the page title is 'Zoekresultaten'. A table displays search results for care providers, with columns for 'Zorgverlener', 'Instantie', 'AGB-code', 'Plaats', 'Postcode', 'Huis nr.', 'Huisarts', 'Apotheek', and 'Regiobeheerder'. The table contains four rows of data, each with status indicators (green checkmarks and red minus signs) and a small icon in the final column.

Zorgverlener	Instantie	AGB-code	Plaats	Postcode	Huis nr.	Huisarts	Apotheek	Regiobeheerder
J Sanders	HP Sanders	0215478963	Deventer	7412 MR	44	✓	✗	✓
H Borgele	HP Borgele	859675123	Deventer	7412 MR	44	✗	✓	✗
J Sanders	HP Sanders	0215478963	Deventer	7412 MR	44	✓	✓	✗
G Borgele	HP Borgele	859675123	Deventer	7412 MR	44	✓	✓	✗

© Protomics 2007 | Zorgportaal Prototype v0.01

Dit is de 2^e beveiligingslaag

Behandelrelatie

Het college bescherming Persoonsgegevens heeft zich medio 2007 op het standpunt gesteld dat een voorwaarde voor het inzien van medische (en zorg) dossiers het hebben van een behandelrelatie is. In het Zorgportaal is dat als volgt geregeld.

We maken aan de gebruiker duidelijk dat het hebben van of het aangaan van een behandelrelatie een voorwaarde is om de gegevens te mogen inzien. Vanuit het gegeven dat vanuit de Regionale Beheer Organisatie niet te zien, weten en checken is of die behandelrelatie bestaat dit probleem opgelost vanuit de kant van de zorgverlener. Die moet weten dat het hebben of aangaan van een behandelrelatie voorwaarde is om bevoegd te zijn om informatie te raadplegen. En de zorgverlener moet weten dat het openen van de dossiers gelogd wordt.

Inmiddels is duidelijk dat ook zorgverleners geïnformeerd willen worden over:

- de voorwaarde van het hebben van de behandelrelatie,
- het loggen van de raadpleging en
- het feit dat ongeoorloofd raadplegen "strafbaar" is.

Dat helpt hen om goed met het Zorgportaal om te gaan. Dus in wordt hier een relatief simpele technische oplossing toegepast die professionals er aan herinnert om conform hun beroepscode(s) en de WBP en WGBO met patiënteninformatie om te gaan.



Noodgevallen

In noodgevallen kan inzage gewenst zijn terwijl nog geen behandelrelatie tussen arts en patiënt bestaat. Dit doet zich voor tijdens de ambulancerit en/of bij de Spoed Eisende Hulp in een ziekenhuis. Als de behandelrelatie er niet is, kan de melding overruled worden en het dossier toch geopend worden. Dat is met name gedaan om tegemoet te komen aan, waar de ontwikkeling van een (regionaal en landelijk) EPD toch ook voor bedoeld is; de Spoedzorg. Daar zijn professionals aan het werk die (nog) geen behandelrelatie met een cliënt hebben, maar die wel aan moeten gaan. In zulke gevallen wordt bijgehouden wie toegang heeft gevraagd, voor gericht toezicht achteraf.



Dit is de 3^e beveiligingslaag

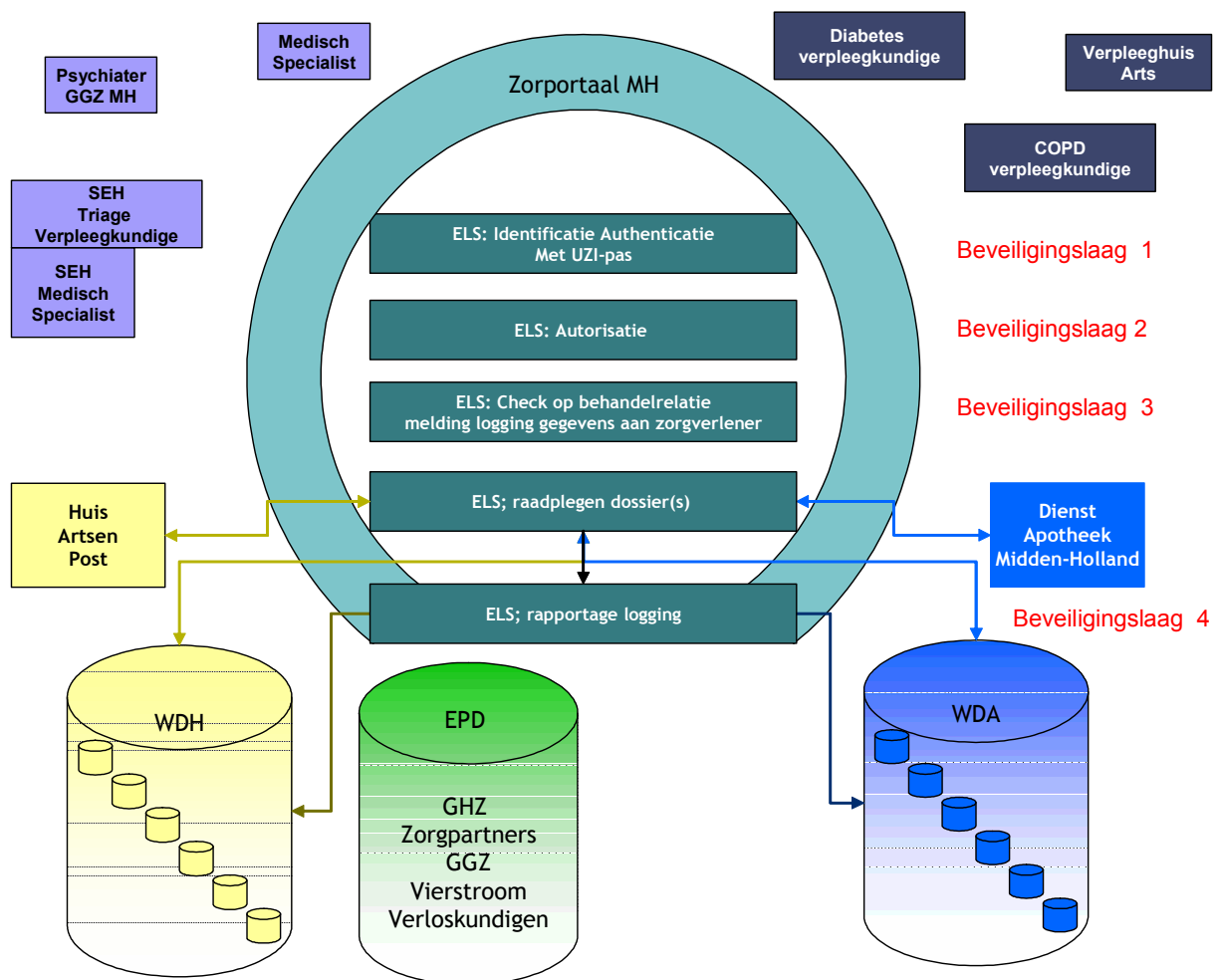
Logging

De raadpleging wordt gelogd (geregistreerd) en komt (via emailberichten) terecht bij de beheerder van het dossier huisarts en/of apothekers. Als die ziet dat bijvoorbeeld een triageverpleegkundige op de SEH een dossier geraadpleegd heeft van een patiënt die daar niet geweest is kan aan de bel betrokken worden bij de Regionale Beheer Organisatie.

Dit is de 4^e beveiligingslaag

Overzicht

Beveiliging van medische dossiers is vormgegeven in 4 lagen, waarvan de 1^e en de 2^e laag technisch geregeld zijn (UZI en autorisatie), de 3^e via een feed-forward principe (informer/attenderen) werkt, en de 4^e een combinatie is van techniek (loggen) en feedback geven (als handhavingmechanisme).



De Regionale Beheer Organisatie

Voor het beheer van het regionale EPD wordt een daartoe bestemde rechtspersoon opgericht, de regionale beheer organisatie. Deze organisatie heeft als werktitel SPITZ-MH meegekregen; Schakel Punt Informatie Transmurale Zorg Midden-Holland.

SPITZ-MH is het geheel van technische, organisatorische en bestuurlijke afspraken en activiteiten die als doel hebben het schakelpunt te laten functioneren en de werking duurzaam te verankeren in de regio.

Het doel van SPITZ-MH

Het doel van SPITZ voor de korte termijn is:

- ▶ Het ontwikkelen van regionale infrastructuur. (ontwikkeling)
- ▶ het bieden van veilig toegang tot authentieke bronnen (bronsystemen) die medische, patiëntgebonden informatie bieden. (beheer)

Wat moet er beheerd worden?

Het beheer betreft

- ELS-platform
- Zorgportaal

De beheerstaken die in het kader van beveiliging vervuld moeten worden zijn:

- Functioneel beheer voeren over ELS en Zorgportaal o.b.v. de uitkomst van bovenstaande functies.
- Beleid ontwikkelen ten aanzien van beveiliging en autorisaties.
- Beleid uitvoeren ten aanzien van beveiliging en autorisaties.

Dit leidt tot de volgende concrete taken.

1. Voorbereiden en uitvoeren van de publiekscampagne regionaal EPD in het kader de passieve toestemming.
Er is mogelijk samenwerking te realiseren tussen Zorgbelang (RPCP) en SPITZ inzake de publieks campagne. Daarnaast wordt verkend in hoeverre Zorgbelang kan fungeren als aanspreekpunt voor patiënten en consumenten aangaande het afschermen van gegevens uit het dossier. Het voordeel van deze constructie is:
 - ▶ Zorgbelang kan de patiënt/consumenten vanuit het patiëntperspectief informeren en wijzen op rechten en verplichtingen.
 - ▶ Zorgbelang kan de verzoeken tot afscherming doorleiden naar SPITZ-MH. Dit zal gedaan worden op een wijze waarbij Zorgbelang een formulier van SPITZ MH zendt naar de cliënt die zijn/haar gegevens afgeschermd wil hebben. Daarin kan door de client worden aangegeven wat de client (niet) wil en voorzien worden van een handtekening.
2. Het vastleggen en registreren van verzoeken van patiënten/consumenten tot afscherming van informatie.
 - 2.1. Het uitvoeren van afscherming van gegevens;
 - ▶ door berichtgeving naar de beheerder van het dossier
 - ▶ door instelling / wijziging van autorisaties in het Zorgportaal
 - 2.2. Het controleren of de gegevens conform de wens van de patiënt afgeschermd zijn
3. Het instellen en onderhouden van de autorisaties voor zorgverleners of groepen van zorgverleners.
4. Het inzien en bewaken van de logging
 - 4.1. Het checken van ongebruikelijke raadplegingen
 - ▶ Hetzij gemeld door de beheerder van een informatiesysteem (huisarts / apotheker)
 - ▶ Hetzij gesignaleerd door eigen bewaking
 - 4.2. Het aanspreken van zorgprofessionals op ongeoorloofde raadpleging van patiëntdossiers