Gerichte toegangsverlening in de zorg

Gerichte toegangsverlening zorgt ervoor dat direct bij de behandeling van een patiënt betrokken zorgverleners toegang kunnen krijgen tot medische gegevens, zónder dat gegevens breed beschikbaar hoeven worden gesteld voor andere groepen zorgverleners. Bij gerichte toegangsverlening stuurt een zorgverlener een link met daarin een autorisatiesleutel op naar een andere zorgverlener om deze toegang te geven tot het dossier van een patiënt. Naast de sleutel bevat de link lokalisatie- informatie. Hiermee weet de ontvanger direct waar de gegevens op te halen zijn. De sleutel geeft een extra beveiliging boven op de middelen (UZI/Dezi) die beschikbaar zijn in de zorg.

Een zorgverlener kan slim gebruik maken van bestaande zorgprocessen om gericht toegang te verlenen. Door een zorgproces zoals verwijzen te gebruiken, bestaat een context om een autorisatie-link te delen. Door het versturen van een autorisatie-link met een recept of een verwijsbrief krijgen alleen de juiste, bij de behandeling betrokken zorgaanbieders toegang. Welke gegevens toegankelijk zijn wordt decentraal (door de verzendende arts) bepaald en hangt af van de situatie. Een voorbeeld is actuele medicatieinformatie die op elk moment in een (verwijs)keten opgevraagd moet kunnen worden.

Hoe werkt gerichte toegangsverlening?

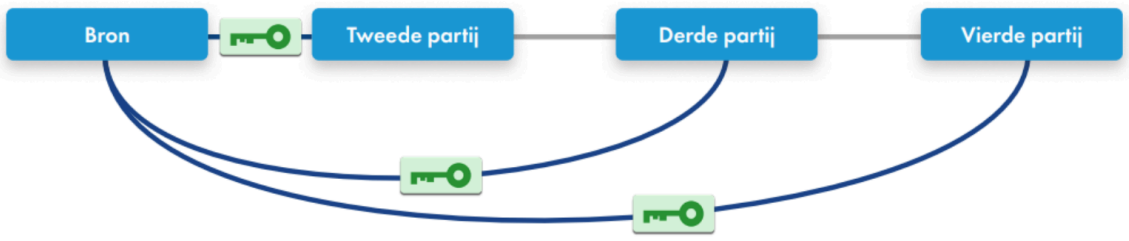
Gerichte toegangsverlening voorkomt dat grote groepen zorgverleners *op voorhand* toegang krijgen tot gegevens, zoals heden gebruikelijk is in de zorg. Daarbij is dan juridisch de eis dat zorgverleners alleen gegevens mogen inzien als zij een behandelrelatie met de patiënt hebben, terwijl technisch niet met zekerheid is vast te stellen dat een opvragende zorgverlener ook echt een behandelrelatie heeft. Omdat gerichte toegangsverlening gebruik maakt van werkprocessen zoals verwijzen om een autorisatie uit te geven aan specifieke behandelaren, is die zekerheid er wel. Hiermee sluit gerichte toegangsverlening op natuurlijke wijze aan bij de zorg. Gerichte toegangsverlening is vaak te gebruiken om gegevens onder *veronderstelde toestemming* beschikbaar te stellen aan medebehandelende zorgverleners. Door de beperkte toegangsverlening worden allerlei beveiligingsrisico's op voorhand effectief uitgesloten.

Data en regie aan de bron

De belangrijkste eigenschap van gerichte toegangsverlening is dat de toegangsverlening volledig door de bronhouder en de patiënt georganiseerd wordt – zij blijven regievoerder over wie toegang krijgt tot patiëntgegevens. Zorgverleners aan wie toegang is verleend vragen gegevens op bij de bron, waardoor actualiteit van de gegevens gewaarborgd wordt. Omdat de opvragende zorgverlener gegevens direct 'inlogt' bij de bron zijn traceerbaarheid van en controle over wie toegang krijgt optimaal gewaarborgd. Daarnaast wordt ook nog eens aan de hoogste eisen van beveiliging voldaan (end-to-end authenticatie en versleuteling).

Gerichte toegangsverlening in de zorgketen

Een belangrijke vorm van gerichte toegangsverlening is *keten-autorisatie.* Dit model wordt uitgewerkt in een standaard voor gerichte toegangsverlening van Decozo (zie bijlage). Hierbij wordt niet alleen een autorisatie-link van A naar B doorgezet, maar is het ook mogelijk voor B om een nieuwe autorisatie-link bij A op te halen die kan worden "doorgezet" naar een volgende zorgaanbieder in de keten.



Vaak is de huisarts, een vertrouwd beginpunt in veel zorgprocessen, de bron van autorisaties. Bij een verwijzing naar een specialist stuurt de huisarts een autorisatie-link mee, waarmee de specialist zelf patiëntgegevens kan ophalen bij de huisarts. Bij een doorverwijzing kan de specialist een nieuwe link ophalen die wordt doorgestuurd naar een volgende specialist of naar een apotheker. Dit kan voor de zorgverlener onzichtbaar gebeuren. Zo volgt gerichte toegangsverlening het reguliere zorgproces.

Gerichte toegangsverlening bij netwerkzorg

Gerichte toegangsverlening kan ook worden toegepast in de netwerkzorg. Bij netwerkzorg zijn meerdere zorgverleners tegelijkertijd betrokken bij de behandeling. Gerichte toegangsverlening bij netwerkzorg kan doordat bij het toevoegen van een nieuwe zorgverlener aan het zorgnetwerk door één van de leden van het bestaande netwerk, van elke partij in het netwerk een autorisatiesleutel wordt uitgereikt aan het nieuwe lid. Vervolgens kan de nieuwe partij autorisatiesleutels terugdelen met de oorspronkelijke partijen uit het netwerk[1]. Zo kunnen zorgaanbieders *gericht* aan het netwerk worden toegevoegd en gegevens uitwisselen met andere zorgverleners in het netwerk.

Gerichte toegangsverlening via de patiënt

Belangrijke eigenschap van gerichte toegangsverlening is dat de patiënt zelf ook een actieve rol kan nemen in het verlenen van toegang - zonder dat deze daarvoor per se zélf beheerder van zorginformatie wordt. De patiënt kan van de huisarts of een andere (eerstelijns) zorgverlener, bijvoorbeeld een verloskundige, een ***autorisatiecode*** krijgen, die hij of zij kan afgeven aan een zorgverlener naar keuze. Hiermee kan de zorgverlener een autorisatie-link *ophalen* waarmee deze toegang kan krijgen tot de gegevens uit één of meerdere brondossiers. Zie de bijlage voor uitleg.

Een autorisatiecode is landelijk en overal bruikbaar - toegang loopt via het web - en biedt de patiënt regie over wie toegang krijgt tot zijn gegevens. Dit biedt ook een oplossing voor onvoorziene situaties. Zo kunnen kwetsbare patiënten deze autorisatiecode afgeven bij een (spoed)opname buiten de eigen regio en desgewenst hun code in bewaring geven bij familie of mantelzorgers. Het systeem kan geïntegreerd worden door zorgaanbieders en kan ook internationaal werken in combinatie met de EHDS.

Kernwaarden verpakt in een eenvoudige standaard

De kerngedachte achter gerichte toegangsverlening is dat deze methodiek eenvoudig in bestaande zorgprocessen moet passen, zodat gegevensuitwisseling mogelijk wordt zónder ingewikkelde technische of juridische kunstgrepen (vaak het geval bij centrale systemen voor toegangsverlening). Kernwaarde is het behoud van het beroepsgeheim en een optimale bescherming van privacy van patiënten -- zónder de zorgverlening te hinderen. Deze aanpak geeft optimale controle en transparatie over gegevensdeling, zowel voor de patiënt als voor de zorgverlener.

Met gerichte toegangsverlening krijgen betrokken zorgverleners toegang tot benodigde informatie, zonder dat gegevens open moeten worden gezet voor een veelvoud van zorgverleners. Gerichte toegangsverlening voldoet aan de eisen van het beroepsgeheim (Wgbo) en biedt een privacybeschermend alternatief voor landelijke gegevensuitwisseling dat eenvoudig bruikbaar is voor zorgverleners. De methodiek kan eenvoudig náást centrale systemen voor gegevensuitwisseling[2] worden ingezet. Zo kunnen alle burgers bediend worden met adequate beschikbaarheid van hun data voor zorgverleners die hen behandelen – dus niet alleen patiënten die toestemming willen geven voor het gebruik van een EUS – met optimale transparantie en controle over toegang, en een strikte bescherming van patiëntprivacy en het beroepsgeheim.

---

[1] In de NEN norm Lokalisatie 7519 worden in bijlage C scenario's voor het delen van lokalisatiegegevens (linkjes) beschreven, waaronder bij netwerkzorg. In de NEN werkgroep Toestemming (7517) wordt het toepassen van veronderstelde toestemming voor uitwisseling van gegevens via decentrale principes uitgewerkt.

[2] De methodiek van gerichte toegangsbeveiliging kwalificeert niet als Elektronisch Uitwisselingssysteem conform de Wabvpz en voldoet aan artikel 1.4 lid 5 van de Wegiz. Het is vaak in te zetten onder veronderstelde toestemming (zie NEN norm 7517).

Bijlage
Gerichte toegangsverlening volgens Decozo
De push autorisatie methode – een technisch perspectief

Push autorisatie (PA) is een **privacy-vriendelijke methode** om patiëntgegevens gericht uit te wisselen binnen het zorgproces. In tegenstelling tot traditionele 'pull' systemen, waarbij gegevens vaak ongericht en breed beschikbaar worden gesteld, zorgt push autorisatie ervoor dat informatie alleen gericht toegankelijk wordt gesteld aan specifieke personen of organisaties die direct bij de behandeling betrokken zijn.

Decentrale controle

Bij push autorisatie blijven de data én de controle **decentraal bij de bron**, er zijn dus géén centrale registers met (lokalisatie)gegeven van de patiënt nodig. Lokalisatie en autorisatiegevens worden decentraal uitgewisseld - dit sluit aan bij de NEN-norm lokalisatie. De behandelend arts en de patiënt behouden het laatste woord over wie toegang krijgt, wat essentieel is voor de vertrouwelijkheid van de arts-patiëntrelatie.

De kern: gericht en veilig referenties doorgeven binnen het zorgproces

Het fundament van deze methode is een unieke referentie naar een specifiek brondossier die zowel de autorisatie als de lokalisatie van de gegevens bevat. Deze *push autorisatie URL* (PA-link) bevat informatie over welk type document opgevraagd kan worden, de geldigheidsduur en de beveiligingseigenschappen.

Een cruciaal veiligheidselement is **binding**: het proces waarbij een PA-link wordt gekoppeld aan de identiteit van een specifieke gebruiker of organisatie die deze URL mag gebruiken. Een PA-link kan van tevoren gebonden zijn aan een specifieke gebruiker, of bij het eerste gebruik. Door gebruik te maken van identificatiemiddelen op hoog niveau (zoals een UZI of Dezi middel) in combinatie met binding wordt gewaarborgd dat alleen de geautoriseerde ontvanger de gegevens kan inzien. Naast identificatie kan een aanvullende **6- of 7-cijferige autorisatiecode** nodig zijn om te binden, als extra factor die beschermt tegen onrechtmatig oprvragen van de gegevens.

Flexibiliteit door doorautoriseren en autorisatiecodes

Een autorisatiecode biedt naast beveiliging ook flexibiliteit, doordat deze op vele manieren kan worden getransporteerd (meegenomen, doorgestuurd) door de patiënt of een arts.

Een PA-link kan eenvoudig worden opgenomen in een digitale verwijsbrief, een recept, maar een autorisatiecode kan ook op papier of zelfs telefonisch worden doorgegeven. Het inzien van gegevens kan niet alleen via een zorginformatiesysteem maar ook met een web-browser plaatsvinden, zodat het systeem vrijwel in elke situatie ingezet kan worden.

Een unieke eigenschap van push autorisatie is het vermogen om de zorgketen te volgen via doorautoriseren. Een zorgverlener die zelf een autorisatie-link heeft ontvangen, kan bij de bron een nieuwe PA-link aanvragen voor een volgende partij in de keten. Bijvoorbeeld als een specialist medicatiegegevens van de apotheek beschikbaar wil stellen aan de volgende partij in de keten.

Eenvoud en standaardisatie

De push autorisatie standaard maakt gebruik van bestaande web-technologieën. Dit bevordert de interoperabiliteit en schaalbaarheid, omdat elke programmeur met deze standaard kan werken en deze in vrijwel elke applicatie te integreren zijn. *Push autorisatie* is de naam van de standaard voor gerichte gegevensuitwisseling die door Whitebox Systems is bedacht en die in 2024 is overgedragen aan de stichting Decentrale communicatie in de zorg (Decozo) ten behoeve van het beheer als open standaard. De stichting bewaakt de privacy-beschermende eigenschappen en het governance-model van deze technologie op de lange termijn.