Versnellingsprogramma VIPP

# IT-audit en gegevensuitwisseling in de zorg

25 september 2020

Wilco Brouwers en Michiel Hopstaken

**Alle burgers in Nederland hebben volgens bestaande wetgeving het recht de eigen medische gegevens in te zien. In 2020 wordt dit recht door nieuwe wetgeving uitgebreid. Uitvoering blijkt in de praktijk voor de zorgsector niet zo eenvoudig, omdat zowel de wijze van uitwisselen van gegevens als de systemen en de processen hieromheen ingrijpend veranderen. De vraag is welke rol wij IT-auditors hierin kunnen spelen. Namens de kennisgroep ICT en Zorg van NOREA presenteren wij in dit artikel onze visie.**

We schetsen eerst kort de achtergrond van de veranderingen, vervolgens de huidige inzet van IT-audit en tot slot onze visie. In de tekst zijn links opgenomen naar verdiepende informatie over bepaalde onderwerpen. Dit als handreiking aan de lezer die (nog) niet in de zorgbranche actief is.

## Achtergrond ontwikkelingen digitale gegevensuitwisseling zorg

De Nederlandse zorg moet veranderen om de zorg en de vorm waarin deze wordt verleend beter af te stemmen op de cliënt. Dit kan door moderne en hoogwaardige zorg te bieden op de juiste momenten en er tegelijk voor te zorgen dat deze betaalbaar blijft. Digitalisering van de zorg is hier onvermijdelijk aan verbonden. Een aantal wetten en kaders liggen hieraan ten grondslag. We beperken ons in dit artikel tot de wetten en kaders, gericht op de ontsluiting van cliëntinformatie.

### Wettelijke ontwikkelingen ontsluiting cliëntinformatie

Vanaf 1 juli 2020 moeten alle zorgverleners aan burgers de gegevens over hun behandelingen beschikbaar stellen via een elektronisch uitwisselingssysteem. Dit nadat de zorgverlener heeft vastgesteld dat de burger, cliënt1 van een of meer zorgverleners daartoe uitdrukkelijk toestemming heeft gegeven. Deze toestemming kan via een eigen cliëntportaal of een landelijk beschikbare Persoonlijke Gezondheidsomgeving (PGO).

De informatieplicht volgt uit het tweede deel van de Wet cliëntenrechten bij elektronische verwerking van gegevens. Hierin staat welke gegevensuitwisseling digitaal moet gebeuren

en hoe deze gegevensuitwisseling eruit moet zien. Momenteel wordt gewerkt aan een nieuwe wet voor een volgende uitbreiding van de digitale gegevensuitwisseling, de Kaderwet elektronische gegevensuitwisseling in de zorg. Het wetsvoorstel wordt eind 2020 aan de Tweede Kamer aangeboden. Onze kennisgroep volgt deze ontwikkelingen en geeft waar nodig feedback aan de uitwerkende instanties. In juni van dit jaar heeft het bestuur van NOREA mede namens onze kennisgroep in de consultatieronde gereageerd op het conceptwetsvoorstel en verbetersuggesties aangedragen ten behoeve van de leden. Zie verder: bijlage A: Wettelijke ontwikkelingen in de ontsluiting van cliëntinformatie.

Op de beveiliging van de cliëntinformatie is uiteraard de privacywetgeving van toepassing. Een belangrijk deel van de eisen uit de AVG is verwerkt in de regelingen die in dit artikel zijn toegelicht, met name op het gebied van het ontsluiten en beveiligen van data. Aanvullende eisen uit de privacywetgeving, zoals organisatie en registratie van verwerkingen, zijn in andere sectorale kaders uitgewerkt. Zij vormen geen onderdeel van de regelingen behandeld in dit artikel.

## Sectorale noodzaak gegevensontsluiting

De Nederlandse zorgketen is verdeeld in zorgsectoren, zoals huisartsenzorg, medisch-specialistische zorg en geestelijke gezondheidszorg (ggz). Dit is logisch verklaarbaar, want iedere sector heeft zijn eigen specialisatie, dossiervereisten, financieringsafspraken en daarmee ook zijn eigen soort informatiesystemen. Deze organisatievorm heeft veel voordelen voor onze gezondheidszorg, maar qua gegevensuitwisseling ook diverse nadelen. Zo is informatie in silo's in verschillende bronsystemen opgeslagen. Bovendien is gegevensuitwisseling tussen zorgverleners vaak nog niet digitaal. Tussen zorgverleners uitgewisselde informatie wordt in diverse formaten aangeleverd, waarna de gegevens worden verwerkt in het eigen bronsysteem. Vaak gaat deze verwerking met de nodige vertalingen gepaard want er gelden nog geen centrale eisen voor het formaat van de basisgegevens.

De extra inspanningen en foutgevoeligheid van deze vertalingen leiden tot verminderde kwaliteit van de geleverde zorg en inefficiëntie in de zorgketen. Een ander nadeel is dat de cliënt zelf zijn gegevens niet kan inzien.

Dit leidt tot de volgende doelstellingen voor digitale gegevensontsluiting:

- Uitbannen van inefficiënties binnen de zorg door de vele dubbele registraties.
- Cliëntveiligheid door beschikbare en juiste en volledige medische gegevens.
- Overzicht, bewaking en regie bij de cliënt zelf.

Om dit te bereiken heeft de overheid wetten en subsidieregelingen vastgesteld. Zie bijlage A: Wettelijke ontwikkelingen in de ontsluiting van cliëntinformatie. Dit artikel gaat over een belangrijk programma waarbij de IT-auditor al actief betrokken is, het VIPP-programma.

## Het VIPP-programma

In 2017 is het subsidieprogramma 'Versnellingsprogramma Informatie-uitwisseling Cliënt en Professional' (VIPP) gelanceerd. Zie: bijlage B: De VIPP-regeling. Dit programma is in verschillende regelingen uitgerold en heeft als doel de benodigde informatiestandaarden te implementeren, waardoor informatie-uitwisseling mogelijk is conform de hiervoor genoemde doelstellingen.

Het gaat inhoudelijk om de gegevensuitwisseling met de cliënt en gegevensuitwisseling specifiek voor medicatie tussen professional en cliënt. De nieuwere VIPP-regelingen kennen ook onderdelen voor implementatie en opschaling van eHealth, zoals online-behandeling bij de ggz. Vanaf 2017 is mede dankzij de VIPP-subsidieprogramma's het aantal zorgportalen en persoonlijke gezondheidsomgevingen (zie hierna) enorm gegroeid.

Een zorginstelling kan subsidie krijgen voor de implementatie hiervan en wordt hier vervolgens via een IT-audit op getoetst. Via IT-audit verantwoordt de zorginstelling zich over het voldoen aan de programmadoelen.
Zie ook de NOREA-pagina 'Aandachtspunten VIPP-assessments'.

## MedMij afsprakenstelsel in zorg

De gegevensuitwisseling moet voldoen aan landelijke standaarden, zodat de gegevensstromen over de verschillende zorgsectoren heen uniform gaan lopen. VIPP ontwikkelt geen nieuwe standaarden, maar volgt bestaande landelijke standaarden zoals het landelijke MedMij afsprakenstelsel, en zorgt voor de implementatie daarvan.

MedMij is in 2018 gestart als een programma op initiatief van Patiëntenfederatie Nederland en het ministerie van VWS om landelijk de spelregels voor de gegevensontsluiting te bepalen en te bewaken. Op 31 december 2019 is het programma opgeheven en zijn de taken van het programma ondergebracht in de stichting MedMij.

De spelregels worden beschreven in een *afsprakenstelsel* waaraan systeemleveranciers getoetst worden. Daarbij wordt onderscheid gemaakt tussen twee typen leveranciers:

1. **Leveranciers in het domein van de persoonlijke gezondheidsomgevingen (PGO)Een PGO** is een hulpmiddel voor de cliënt om relevante gezondheidsinformatie van de zorgverleners te verzamelen, te beheren en desgewenst met andere partijen te delen via gestandaardiseerde gegevensverzamelingen voor gezondheidsinformatie en geïntegreerde digitale zorgdiensten. Elke burger kan vrij kiezen uit verschillende landelijk aangeboden PGO's.
2. **Leveranciers in het zorgdomein, de 'dienstverleners zorgverlener' (DVZA)Een DVZA** levert rechtstreeks diensten aan zorginstellingen in de vorm van de primaire bronsystemen, gecombineerd met de gegevensuitwisseling tussen cliënt en instelling.

De systeemleveranciers in de zorg wisselen onder MedMij gegevens versleuteld met elkaar uit volgens de geldende standaarden. Ze kunnen zelf de informatie niet inzien. De set informatiestandaarden omvat gezondheidsgegevens zoals bloeddruk, longfunctie en laboratoriumuitslagen. De informatiestandaarden beschrijven welke informatie moet worden vastgelegd en hoe dat moet gebeuren. Ze worden ontwikkeld samen met marktpartijen zoals leveranciers van PGO's, leveranciers van zorginformatiesystemen en patiëntenorganisaties. Ook MedMij gebruikt zoveel mogelijk bestaande standaarden.

In aanvulling hierop bevat het stelsel afspraken over verschillende aspecten zoals juridisch, technisch en informatiebeveiliging. Leveranciers van systemen moeten aan dit hele stelsel voldoen en krijgen na een positief assessment door Nictiz het MedMij-label. Nictiz is een landelijke, onafhankelijke kennisorganisatie die zich inzet voor digitale informatie-uitwisseling in de zorg.

Zorgverleners moeten onder de VIPP-regeling aansluiten bij MedMij, door via een MedMij-goedgekeurd systeem op de afgesproken manier gegevens op te slaan en uit te wisselen (dit geldt voor de regelingen na de eerste regelingen VIPP1 en VIPP2). Zorgverleners kunnen daarbij zelf deelnemen aan het afsprakenstelsel of deelnemen via een dienstverlener die deelnemer is.

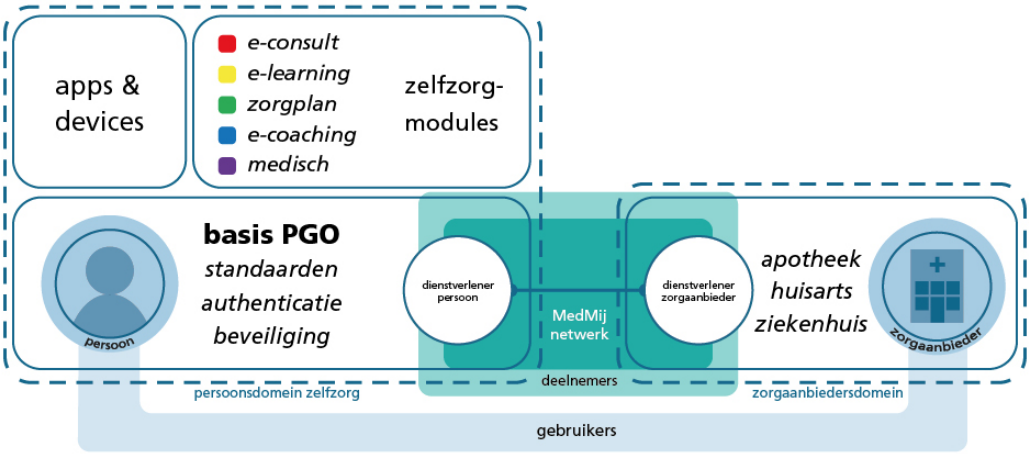
## Ontwikkeling systeemlandschap: van cliëntportaal naar PGO

In deze paragraaf schetsen we hoe de zorgsector momenteel de digitalisering vormgeeft. Mede door de hiervoor behandelde wetten en regelingen ontstaat geleidelijk een nieuw systeemlandschap.

In de eerste VIPP-regelingen hebben de zorgverleners – toen vooral ziekenhuizen – overwegend vanuit hun eigen systemen elk een cliëntportaal opgezet. De systeemleveranciers in de zorg hadden dergelijke portalen vaak al gebouwd en zagen in VIPP een kans om deze gesubsidieerd verder uit te rollen. Gevolg is dat er een verscheidenheid aan cliëntportalen in gebruik werd genomen. Het aantal portalen zal de komende jaren nog verder stijgen, gezien de lopende en aankomende VIPP-subsidies.

Het nadeel voor de cliënt is dat een veelheid aan portalen voor de verschillende zorgverleners ontstaat en dat de zorginformatie niet gebundeld bij elkaar komt te staan. Het ministerie van VWS stimuleert dan ook nadrukkelijk de aansluiting van zorgverleners op de persoonlijke gezondheidsomgeving PGO. Dit via een PGO-leverancier die – vaak in een regio of voor een specifieke doelgroep zoals diabetes- of COPD-patiënten – een systeem aanbiedt waarin de cliënt zelf de gegevens van de verschillende zorgverleners kan inladen in één PGO-omgeving. Vanuit het doel van regie bij de cliënt zelf is dit een zeer

gewenste richting. Bovenop zo'n PGO kunnen nog aanvullende toepassingen worden toegevoegd, zoals zelfzorgmdules en specifieke apps op devices als slimme horloges, die gegevens in een PGO kunnen inladen. De visualisering door MedMij van het geheel van persoonsdomeinen, zorgaanbiedersdomeinen en aanvullende toepassingen zoals apps en zelfzorgmodules weergegeven in figuur 1.




**Figuur 1:** Conceptueel model PGO. Bron MedMij

Een cliënt kiest dus zelf een PGO om medische gegevens van verschillende zorgverleners in te laden en, andersom, eigen gegevens aan de zorgverleners aan te bieden. Denk bij het laatste aan eigen metingen, dagboeken, sportinformatie et cetera. Deze door de cliënt aangeboden gegevens moet het bronsysteem van de zorgverlener ook weer kunnen verwerken.
Het is de vraag hoe aanbieders in het zorgaanbiedersdomein en het persoonsdomein zich op dit punt ontwikkelen, en wat de adoptiegraad van het PGO-concept wordt. Mede gestimuleerd door de MedMij-subsidiëring zijn er inmiddels zo'n dertig MedMij-erkende PGO-aanbieders in het persoonsdomein.

In het zorgaanbiedersdomein zien we per sector een beperkt aantal systeemleveranciers met een stevige klantbasis; sommige betreden de PGO-markt, andere leveren een specifiek portaal vanuit het bronsysteem dat de behoefte aan een PGO weer verkleint.
Regionale samenwerkingsorganen in de zorg denken na over een regio-PGO, maar ervaren dan vaak wel weerstand van de gevestigde leveranciers in het zorgaanbiedersdomein, die hun eigen systemen en portalen niet zomaar willen openstellen.

# Rol van de auditor

Duidelijk is dat medische gegevens door de bovenstaande ontwikkelingen vanuit de bronsystemen van de zorgverleners naar andere omgevingen worden verplaatst. Dat gebeurt vaak buiten het zicht en de beheersing van de zorgverleners. Hoewel het MedMij-afsprakenstelsel de betrouwbaarheid van de dienstaanbieders in het persoonsdomein (PGO) en in het zorgverlenersdomein in de basis borgt, worden hiermee niet alle nieuwe risico's voor de zorgsector afgedekt. Denk daarbij bijvoorbeeld aan de organisatorische en juridische vraagstukken over de gegevens en uitwisseling hiervan. Daar willen wij als kennisgroep een rol in spelen.

Grote vraag voor veel zorginstellingen is hoe je een dergelijke gegevensuitwisseling samen met alle partijen in de keten kunt beheren en veilig houden – goedkeuring van systemen door MedMij is slechts een van de te regelen aspecten. Hoe houd je als individuele zorginstelling zonder gespecialiseerd personeel overzicht en grip op risico's? Wie is nu eigenaar van de gegevens? Voor zorgprofessionals ontstaat een andere manier van samenwerken en gegevens uitwisselen. Dit wordt steeds vaker regionaal ingericht. In Nederland zijn hiervoor reeds tien regionale ICT-uitvoeringsorganen voor zorgverleners opgericht, de Regionale Samenwerkings Organisaties. Deze RSO's zullen een nog grotere rol gaan spelen in de gegevensuitwisseling in de regio en het ondersteunen van de zorgverleners bij inrichting en beheer van de benodigde infrastructuur en systemen.

De kennisgroep heeft hierover contact met de landelijke vereniging van RSO's, RSO Nederland. Daarbij wil de kennisgroep zich meer gaan richten op grote veranderingen die nieuwe risico's voor de zorgverleners en cliënten introduceren en waar wij als IT-auditors een belangrijke rol bij kunnen spelen. We noemen er twee: groei in SaaS-oplossingen en organiseren in samenwerking met zorgverleners in een regio.

## Groei in SaaS-oplossingen

De zorgverlener kan vanuit het eigen bronsysteem een cliëntportaal van de systeemleverancier afnemen. Dit is een Software as a Service (SaaS) oplossing. Dit past bij de trend dat IT-faciliteiten worden uitbesteed, wat zeker voor de kleinere zorginstellingen geldt. Overigens is dit vaak noodzaak, omdat bepaalde oplossingen uitsluitend als online variant beschikbaar zijn. Gevolg is dat bij zorginstelling het karakter van het interne IT-beheer verandert van beheer van de eigen systemen in regievoering over externe systemen.

Bij het aansluiten op de landelijk beschikbare PGO's gaat deze verandering in het beheer van systemen nog een stap verder. Een PGO is in beheer bij de PGO-leverancier, en dat is een partij waar de zorgverlener geen relatie mee heeft. In die situatie is het IT-beheer geen verantwoordelijkheid van de zorgverlener, terwijl de zorgverlener wel de gegevens moet kunnen aanbieden aan het PGO, en de zorgverlener ervoor verantwoordelijk is dat dit alleen gebeurt met toestemming van de eigenaar van de data, de cliënt. Over de kwaliteit

van het beheer van het PGO zal de zorgverlener vragen hebben die een IT-auditor kan helpen beantwoorden.

### Organiseren in samenwerking met zorgverleners in een regio

Een PGO wordt per definitie gekoppeld aan verschillende zorgverleners en daarmee vaak in een regio georganiseerd. Dit gebeurt om twee redenen. Ten eerste omdat de overheid naar meer regionale samenwerking wil en bijvoorbeeld ook de financiering voor infrastructuur hierop zal aanpassen. Ten tweede ook omdat het simpelweg voor een instelling bedrijfseconomisch niet haalbaar is een eigen PGO te organiseren, daarmee zelf systeemleverancier te worden, en dus ook andere zorgverleners te moeten aansluiten. Ook ontstaan hierdoor regionale cliëntportalen, zodat de kennis en financiële middelen in een regio worden gebundeld. Gevolg hiervan is dat regionale samenwerkingen op het gebied van ICT ontstaan en zorgverleners worstelen met de inrichting en het beheer van dergelijke 'hubs'. Bij de bijbehorende inrichtingsvraagstukken en het vergroten van het vertrouwen in systemen en organisaties kan de IT auditor een nuttige rol vervullen.

## Voorbeelden huidige toetsende rol IT-auditor

Het IT-auditberoep heeft de afgelopen jaren een belangrijke rol gespeeld in de bovengeschetste ontwikkelingen. Zo waren IT-auditors, vertegenwoordigd door onze kennisgroep, betrokken bij de totstandkoming van de standaarden en het afsprakenstelsel en de diverse handboekentoetsing. Een zorginstelling is voor elke VIPP-subsidie verplicht via een eindtoets door een RE aan te tonen dat de doelstellingen van die subsidie zijn behaald. De RE toetst of de uitgevoerde activiteiten geleid hebben tot het behalen van het functionele doel, dat wil zeggen:

- Werkende gegevensontsluiting naar de cliënt.
- Gebruik van de gegevensontsluiting door cliënten.
- Interoperabiliteit tussen verschillende zorgaanbieders.

De kennisgroep ontwikkelt toetshandreikingen voor de IT-auditor. Ook is samen met relevante belangenorganisaties als de Nederlandse Vereniging van Ziekenhuizen, Zelfstandige Klinieken Nederland en GGZ Nederland, een FAQ met nadere duiding voor auditors beschikbaar gesteld en zijn er diverse auditorsbijeenkomsten georganiseerd voor de leden van NOREA.

Deze toetsingen borgen dat aanbieders van systemen een kwalitatief goede oplossing bieden die de zorgverleners op de juiste wijze in hun zorgprocessen kunnen implementeren. Kúnnen implementeren, want de daadwerkelijke implementatie en de randvoorwaardelijke algemene IT-beheerprocessen liggen niet binnen de scope van deze toetsen. Ook maken we de kanttekening dat VIPP nu nog vooral gericht is op het

kunnen *downloaden* door de cliënt van gegevens van zorgverleners in het eigen portaal. Pas de komende jaren wordt de focus verlegd op het zelf uploaden van eigen gegevens door de cliënt in een persoonlijk dossier en dit door laten zetten naar de zorgverlener. Toetsmethodiek en handreikingen moeten dan ook de komende jaren door de kennisgroep worden doorontwikkeld.

In aanvulling hierop voert de IT-auditor uiteraard ook toetsingen uit bij SaaS-leveranciers voor *third party assurance*. Hiermee wordt al langere tijd voorzien in de behoefte van zorginstellingen om zekerheid te krijgen over de kwaliteit van IT-beheerprocessen bij de externe leveranciers.

Ten slotte voeren IT-auditors al geruime tijd bij de instellingen in de zorgsector NEN 7510 en ISO 27001 toetsingen uit op managementsystemen voor informatiebeveiliging en op getroffen maatregelen. Ook worden privacy-onderzoeken uitgevoerd op basis van tools die de NOREA-kennisgroep Privacy heeft aangereikt. In breder verband wordt dus al langer gekeken naar informatiebeveiliging, privacy, en bijvoorbeeld leveranciersmanagement. Deze normeringen zijn volop in ontwikkeling, waarbij de in dit artikel geschetste veranderingen worden meegenomen. Bij NEN liggen momenteel tal van normontwerpen voor de zorg op tafel. Ook hierin zorgt de kennisgroep voor betrokkenheid en kwaliteit.

## Visie kennisgroep op toekomstige rol IT-auditor

Hierna beschrijven we aan welke toekomstige rol van de auditor de kennisgroep werkt.

### Eenduidigheid bij implementatie van standaarden

De kennisgroep vindt het belangrijk dat, los van marktpolitiek, de basisstandaardisering en beveiliging eenduidig ingeregeld worden. In theorie is dit door het MedMij afsprakenstelsel altijd gewaarborgd. Maar de gewenste ontwikkeling naar het PGO wordt niet bereikt wanneer de MedMij afspraken door systeemleveranciers verschillend worden geïnterpreteerd en geïmplementeerd. De kennisgroep overlegt hierover met de diverse zorgkoepelorganisaties en leveranciersverenigingen en wijst daarbij op de mogelijke risico's van bepaalde uitwerkingen.

De verwachtingen in de markt zijn dat een hybride omgeving ontstaat met een mix van instelling-specifieke portalen en PGO-omgevingen. De meeste zorginstellingen kiezen voor aansluiting bij een extern geleverde SaaS-portaalomgeving, in de vorm van een cliëntportaal of PGO. Er ontstaan ook initiatieven voor een regionaal opgezet PGO. Er wordt daarbij steeds vaker een koppeling gemaakt vanuit de eigen software naar een leverancier van andere software buiten de eigen netwerken.

## Vertrouwen in de keten door integraliteit van certificeringen

Iedere betrokken partij binnen de zorginfrastructuur en de keten van gegevensuitwisseling heeft een verantwoordelijkheid om cliëntinformatie te beveiligen. Dus de leverancier van het bronsysteem bij de zorginstelling, het dataknooppunt, de portaalomgeving et cetera. Elke schakel zal zijn eigen vorm van verantwoording moeten afgeven, idealiter in de vorm van assurance.

Voor de gebruikers van de data is het vaak ondoorzichtig hoe de gegevensuitwisseling in de keten verloopt en of alle verantwoordelijkheden goed zijn afgedekt. Voor zorgverleners en cliënten is de veiligheid van de totale keten echter van essentieel belang. Hetzelfde geldt voor beleidsmakers.

De IT-auditor heeft een belangrijke rol om inzicht in deze keten en risico's te geven. Onze kennisgroep deelt de visie binnen de zorgsector dat moet worden toegewerkt naar een standaardcertificering voor de totale zorgketen. Een certificering die marktpartijen, beleidsmakers en de cliënt het vertrouwen geeft dat beveiliging, privacy en andere relevante aspecten goed geregeld zijn. Er dreigt nu nog een meervoud aan deelcertificeringen te ontstaan. Denk hierbij aan MedMij-labels, NEN 7510-certificaten, DigiD-audits et cetera.

Nu zal iedere schakel in de keten binnen de zorginfrastructuur andere veiligheidsrisico's lopen en dus ook moeten voldoen aan andere normen. Tenslotte heeft een eHealth-leverancier bijvoorbeeld een ander risicoprofiel dan een leverancier van een elektronisch cliëntendossier. De nog te ontwikkelen visie op eenduidige certificering ziet de kennisgroep dan ook als een kader waarin eenduidig is afgesproken wat de deelonderwerpen zijn, wat deze inhouden en welke onderwerpen voor elke schakel in de keten van toepassing zijn. En om te bewaken of alle partijen voldoen aan de certificeringsplicht.

NOREA zou hier de door de relevante veldpartijen voorgestelde inhoud van de (deel) certificering moeten toetsen. Te denken valt aan het normenkader en de auditkaders en ook aan een concreet beschreven auditproces met welomschreven terugkoppeling van resultaten aan alle stakeholders. De leden van NOREA zijn de uitvoerders van de audits. De kennisgroep is al betrokken bij een aantal initiatieven en heeft zich aangesloten bij partijen die zich deze richting op bewegen. Dat NOREA in de consultatieronde over het wetsvoorstel Elektronische gegevensuitwisseling in de zorg heeft gereageerd, past in deze benadering.

## Normenkaders meer helpend en minder dirigerend

Om ruimte te houden voor innovatie heeft de zorgsector behoefte om te werken in lerende (regionale) netwerken. Daarbij passen normenkaders niet op elk moment even goed; het wringt bijvoorbeeld in de pilotfase van een innovatie. Daarvan moeten wij ons als beroepsgroep bewust zijn, terwijl we vaak geneigd zijn juist een meer rigide toetskader te hanteren. Ook toezichthouders zullen hierin moeten meebewegen.

In de pilotfase zien we vooral een rol voor de IT-auditor om duidelijkheid te scheppen in het groeiende woud aan kaders: wat is het specifieke doel van elk normenkader en past de invulling die de zorgverlener of keten kiest daar wel bij? Daar waar je diversiteit en ruimte toestaat, passend bij een keten of regio, krijg je betere oplossingen. Om ruimte te krijgen voor maatwerk zijn wel altijd risicoanalyses nodig. Op basis van zo'n analyse en de *risk appetite* in de keten kunnen dan passende kaders voor handhaving en toetsing worden gekozen.

We beseffen dat als je ruimte geeft voor leren, het toezicht complexer wordt. Gelukkig groeit ook de zorgsector zelf in volwassenheid en zal die zich terecht meer bemoeien met de invulling van toezicht. Het is een interessante bredere ontwikkeling in ons beroepsveld van meer focussen op uitkomsten dan op regels, die wij als kennisgroep ook in de zorgsector komende periode nader zullen verkennen.

Hier past tot slot wel de kanttekening dat de zorgsector niet sterk is in het voldoen aan kaders, ook al zijn deze wettelijk verplicht zoals de NEN 7510. Er zijn nog maar een handvol aanbieders die aantoonbaar aan de NEN 7510 voldoen, terwijl het doel informatiebeveiliging evident is.

### NOREA en de adviserende rol van de IT-auditor

Naast de assurance-rol die dicht bij huis ligt, zien we als kennisgroep ook een toenemende vraag naar de adviesrol van de IT-auditor in dit veranderende landschap. Met een open blik naar de toekomst kijkend streeft de kennisgroep ernaar, namens NOREA meer aan de voorkant mee te helpen bij de ontwikkelingen zoals in dit artikel geschetst. Daarbij willen we ook breder kijken dan alleen de kwaliteit van gegevens (de focus van dit artikel). We willen ons nadrukkelijk ook richten op het gebied van zorginnovatie en het gebruik van ICT daarbij. De kennisgroep ontvangt vanuit diverse gremia steeds meer vragen over beheersingsvraagstukken in brede zin, zoals portfoliomanagement, kwaliteit van systeemontwikkeling en leveranciersmanagement. De kennisgroep gaat hier meer aandacht aan besteden.

## Tot slot

Het moge duidelijk zijn dat de gegevensontsluiting in de zorgsector veel uitdagingen kent, maar ook een groot maatschappelijk belang dient. Er wordt hard gewerkt en vooruitgang geboekt, gedreven door wet, subsidie en noodzaak. Het beheersen van (nieuwe) risico's en het sturen op normontwikkeling en toezicht blijft vaak onderbelicht. De kennisgroep ICT en zorg van NOREA zal hier aandacht aan blijven besteden en de rol van de IT-auditor hierin bepleitten.

## NOOT

[1] Binnen de zorg wordt gesproken over patiënt en cliënt. Er zijn verschillende definities in omloop. Voor de leesbaarheid van dit artikel houden we cliënt aan, waarbij we zowel patiënt als cliënt bedoelen.


### Drs. W.J.M. (Wilco) Brouwers RE | Senior Manager IT Advisory bij Baker Tilly IT Advisory

Wilco Brouwers is senior manager bij IT Advisory van Baker Tilly. Hij is ruim twintig jaar werkzaam als adviseur en IT-auditor. Wilco heeft veel audit- en advieswerkzaamheden uitgevoerd bij zorgorganisaties, onder andere op het gebied van strategievorming, informatiebeveiliging en beheersing. Wilco is lid van de kennisgroep ICT en Zorg van NOREA.

### Ing. M.A.W.V. (Michiel) Hopstaken MSc RE CISA CISM | Senior Manager IT Risk Assurance bij BDO

Michiel heeft tien jaar ervaring op het gebied van IT, risicomanagement en audit. Hij heeft zich binnen BDO gespecialiseerd in de zorgsector en vanuit die specialisatie is hij lid van de BDO branchegroep Healthcare.
Hij is namens BDO betrokken bij diverse IT Risk Assurance opdrachten in de zorg (data-analyse, VIPP, horizontaal toezicht, cybersecurity en IT-implementaties). Tevens is hij lid van de NOREA kennisgroep ICT en Zorg.