Naar een te verantwoorden, veilige en transparante gegevensuitwisseling in de zorg

Hugo de Vos Maart 2023

In opdracht van Stichting KDVP en Platform Burgerrechten

Voswiz
Innovation in place

Inhoud

Naar een te verantwoorden, veilige en transparante gegevensuitwisseling in de zorg

Hugo de Vos (Voswiz)

In opdracht van Stichting KDVP en Platform Burgerrechten

Maart 2023

Samenvatting

Het voorliggend visiedocument presenteert de wenselijkheid om vanwege verschillende redenen decentrale berichtenuitwisseling in de zorg te ontwikkelen en voluit te steunen. Het Nederlandse Zorgstelsel rust op het vertrouwen dat bestaat tussen (het netwerk van) zorgverleners en patiënt, is beschermd door het beroepsgeheim en valt onder de AVG. Een ICT-stelsel dat de ontwikkeling in netwerkzorg ondersteunt moet daarom flexibel zich kunnen aanpassen aan vereisten van ontwikkelingen in de zorg, moet veilig zijn en moet ten allen tijden de privacy van de patiënt en het beroepsgeheim in stand houden. (hoofdstuk 1)

Het huidige centrale georganiseerde ICT-stelsel loopt tegen hardnekkige problemen aan die bij doorontwikkeling zullen leiden tot voortdurend hoge kosten, veiligheidsproblemen, het opgeven van belangrijke privacy-rechten, ondoorzichtigheid van betrokkenen, onmogelijke belegging van verantwoording en zelfs tot opheffing van beroepsgeheim en de roep tot herschrijven van de WGBO. De huidige weg is duidelijk een techniek-gedreven oplossing die gebruikers en de samenleving vraagt zich maar te schikken naar de ICT. De ICT-oplossing en enorme huidige uitgaven wordt hierbij gepresenteerd als een noodzakelijkheid omdat "*het immers niet anders kan*". Deze weg zal ongetwijfeld leiden tot meer problemen en aanhoudende discussie rond privacy, veiligheid en verantwoordelijkheid. (hoofdstuk 2)

Bij ICT en privacy vraagstukken dient altijd de vraag te worden gesteld of – naast de wettelijke grondslag- de voorgestelde ICT oplossing precies doet wat nodig is (noodzakelijkheid), of het doel de middelen heiligt (proportionaliteit) en of er geen minder zwaar middel is om hetzelfde doel te bereiken (subsidiariteit).

Een decentrale oplossing (*het kan wel anders*) gaat uit van goede afspraken en protocollen waar de berichtenuitwisseling aan moet voldoen en implementeert die in de context van de plek waar de uitwisseling start en de wens voor gegevensdeling zich voordoet; in de zorgverlenerspraktijk. De decentrale optie is een zorgvolgend proces, waarbij ICT zich aanpast aan de processen van het dagelijkse zorgproces van zorgverleners en patiënt. Decentrale uitwisseling is niet alleen door de voortdurende ontwikkeling in het ICT-veld mogelijk, het is nu al bewezen technologie in verschillende *use cases*. (hoofdstuk 3)

Een decentrale aanpak is veiliger, goedkoper en transparanter. Bovenal is het een veel eenvoudiger oplossing voor gegevensdeling, die het mogelijk maakt aan de privacy-eisen en de WGBO te voldoen en minder invasief is. Er hoeven geen ingewikkelde beheersorganisaties en samenwerkingsverbanden te worden opgezet en de WGBO kan volledig overeind blijven. Het maakt het bovendien een oplossing die – met de nodige ondersteuning- vlot geïmplementeerd kan worden. De privacy wetgevingseisen geven aanleiding om de decentrale opzet nu door te zetten en het verder investeren in grote complexe ondoorzichtige dure systemen - met de gepaard gaande aantasting van veiligheid en privacy - te staken. De Nederlandse - nu kwetsbare - kritische centrale infrastructuur van medische gegevensuitwisseling moet dringend worden heroverwogen. De zorg verdient ICT die het zorgproces volgt, flexibiliteit en snelle doorontwikkeling mogelijk maakt en de vertrouwensrelatie kan garanderen, in plaats van zich in bochten te moeten wringen om een centralistisch georganiseerde ICT te kunnen blijven gebruiken. (hoofdstuk 4)

1 Inleiding : de ontwikkeling van gegevensdeling in de zorg

Het Nederlands Zorgstelsel is de laatste jaren steeds complexer geworden waarbij zorg niet meer alleen op 1 locatie wordt gegeven, maar steeds meer in netwerken van zorgverleners plaatsvindt. Netwerkzorg vereist dat een goede uitwisseling van medische gegevens de zorg kan ondersteunen.

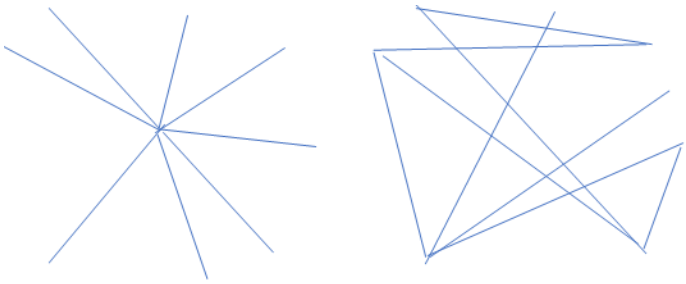
De verwachtingen van ICT zijn ook in de zorgsector torenhoog. Al vroeg in de jaren 2000 werd ingezet op het verbinden van de systemen via een landelijk knooppunt, het EPD, wat later het LSP is gaan heten. Het systeem is gebaseerd op het idee van 'een centraal knooppunt' of 'centrale as' die toegang faciliteert voor de verschillende systemen in het land. Hoewel de toepassing in 2011 zich beperkte tot huisartsenwaarneming en medicatie sprak het College Bescherming Persoonsgegevens in 2011 van " ***grootschalige, risicovolle*** *verwerking van* ***bijzonder gevoelige gegevens****."* Een systeem dat zorgvuldigheid vereist. De Eerste kamer keurde wetgeving over het EPD in dat jaar af en zette een streep door dit door de overheid opgezette systeem vanwege privacy en veiligheidsoverwegingen af. Sindsdien is het systeem in "private handen" voortgezet: met gelden van de zorgverzekeraars en subsidies van de overheid bouwde een groeiend team verder aan de doorontwikkeling van dit knooppunt-systeem.

Het idee van knooppunten was begin jaren 2000 een logische stap om daarmee de veelheid van (vaak net ontwikkelde) applicaties van zorgverleners te ontlasten op het gebied van verbindingsprotocollen en uitwisselingsstandaarden en uniformering van gegevensdefinities. Bij een knooppunt gaan gegevens als het ware via een fietswiel van alle individuele zorgverleners op de spaken, via de centrale as, naar de volgende zorgverlener op de spaken.

Sinds 2011 is de doorstart van het – nu private- EPD het aantal toepassingen en aansluitingen toegenomen. Het (besmette) EPD werd in naam herdoopt tot "het LSP" dat stapsgewijs en organisch steeds verder groeide tot een complex systeem van ICT, organisatorische en procedurele afspraken en wettelijke hervormingspogingen dat aan voortgaande vragen, wettelijke eisen en privacyregels en herstel van problemen die steeds de kop opsteken, tracht te voldoen. Omdat de opzet van het EPD/LSP geen structurele en principiële wijziging heeft ondergaan, zijn de risico's die leidden tot de afkeuring van het EPD in 2011 nog steeds actueel.

De meest recente uitbreiding betreft een register van toestemmingen van patiënten – Mitz- dat beoogt het toepassingsgebied uit te breiden naar alle zorgverleners en tegelijkertijd antwoord te geven op de noodzaak tot het geven van toestemming bij de verwerking van gegevens. Via dit nieuwe toestemmingen knooppunt wordt beoogd gegevens van 'alle' Nederlanders bij 'alle zorgverleners' toegankelijk te maken, vanuit het LSP, maar ook vanuit andere systemen, zoals ziekenhuis-samenwerkings XDS-systemen of regionale zorgICT-platforms. Dit is ontegenzeggelijk 'grootschalige en risicovolle verwerking' van medische persoonsgegevens in het kwadraat. Daarom stellen wij de vraag wie nog zicht heeft op de consequenties van het uiterst complexe bouwwerk en of het nog is te begrijpen voor betrokkenen en is het systeem nog geschikt is voor doorontwikkeling in de toekomst. Moeten we dit willen?

Tijdens de Cubacrisis waarschuwde de ingenieur Baran[1] in een klassiek geworden werk voor de risico's van het toen centrale netwerk van telecommunicatie in de VS en pleitte succesvol voor onmiddellijke decentrale of gedistribueerde hervorming hiervan. Centrale knooppunten vormen een hoog risico voor aanvallen van buiten en de impact is hoog bij uitval. Het huidige tijdsgewricht met de recente geopolitieke dreigingen – maakt een robuuste en veilige aanpak van kritische digitale infrastructuur wederom uiterst urgent en vraagt erom de risico's van de huidige centrale opzet van uitwisseling van medische persoonsgegevens tegen het licht te houden. Ook dringt zich de urgentie op om onmiddellijk een decentrale aanpak te gaan promoten. In geval van een hack bij een decentrale opzet is 1 patiënt (of wellicht 1 zorgverlener gecompromitteerd) – in geval van knooppunten alle.



Centrale uitwisseling (fietswiel)

Decentrale uitwisseling (netwerk)

De centrale aanpak – en de knooppunten aanpak- is al lang geen noodzakelijkheid meer, omdat ICT zorgsystemen volwassen zijn geworden, het veld is geconsolideerd en de capaciteit bij ICT partijen aanwezig is om zelf verbindingen en koppelvlakken ontwikkelen. Daarnaast maken recente ontwikkelingen op het gebied Informatiestandaarden, open standaarden en open koppelvlakken het steeds makkelijker om veilig peer-to-peer gegevens uit te wisselen. In zekere zin is hiermee ook in de ICT wereld sprake van een paradigma-shift, waarin door meer eenvoud, flexibiliteit en transparantie een grotere mate van veiligheid en privacybescherming mogelijk is. Open koppelvlakken maken het bijvoorbeeld mogelijk om protocollen en procedures 'in te bouwen' in de bron-ICT die voor alle systemen op gelijke wijze kunnen worden toegepast, terwijl door gegevens uit te wisselen op een decentrale manier het makkelijker is *end-to-end* encryptie toe te passen en een single point of attack en single point of failure te voorkomen.

Deze ontwikkeling zorgt ervoor dat het centrale "gemaks-argument" van knooppunten als schakelkast langzamerhand niet meer geldt. Het is dan op zijn minst bevreemdend dat de overheid en andere centrale financiers nog steeds eenzijdig te lijken willen blijven inzetten op een knooppunten-infrastructuur. De nieuwe mogelijkheden op het gebied van ICT dwingen om de noodzakelijkheids- en subsidiariteitsvraag voor een risicovol centraal gekoppeld systeem luid en duidelijk opnieuw te stellen.

Het is met de huidige stand van de ICT-techniek goed mogelijk in plaats van gegevensverkeer via een fietswiel te organiseren ook rechtstreeks verbindingen te leggen tussen de ICT-bronsystemen van de zorgverleners, waarbij steeds een lijntje wordt uitgeworpen van

1 Baran, P (1964) On distributed Communications. Rand Corporation, Santa Monica, USA

zorgverlener naar zorgverlener. Zo ontstaat: “een netwerk of web geweven rond de patiënt”.

Voorliggend visiedocument gaat in de eerste plaats over de primaire uitwisseling van gegevens tussen zorgverleners. Eerst zal het huidige systeem worden beschreven en zal worden aangegeven waar het nu steeds meer aanloopt tegen knelpunten. De knelpunten leiden tot onmogelijke keuzes en dilemma’s over *informed consent*, verantwoording en zelfs met voorstellen die neerkomen op het opheffen van het medisch beroepsgeheim (Hoofdstuk 2). Na een beschrijving van de belangrijkste knelpunten zal een route worden geschetst die het mogelijk maakt een ICT-systematiek op te zetten die voor een robuustere en toekomstbestendige opzet van gegevensuitwisseling kunnen zorgen (hoofdstuk 3). Een nieuwe opzet kan tegelijkertijd beter voorzien in de informatievraag voor de groeiende complexiteit van zorg die steeds meer in netwerken plaatsvindt en die bij voorkeur flexibeler en ontwikkelingen in de zorg volgend moet worden ingericht. Een netwerk opzet is inherent veiliger tegen aanvallen van buiten en beter instaat de vertrouwelijksheidsrelatie tussen patiënt en behandelaar op een transparante wijze te garanderen. Voordat we ingaan op de techniek is het goed de huidige organisatorische en wettelijke achtergrond van gegevensbeheer en de redenen achter deze regelgeving te beschrijven (Hoofdstuk 1).

1.1 Registratieplicht in de Zorg: WGBO, *vertrouwelijkheid* en de behandelrelatie

Als een patiënt bij een zorgverlener komt zal hij/zij zijn/haar klachten kenbaar maken en zal de zorgverlener naar zijn beste kunnen en in begrijpelijke taal uitleggen wat de diagnose is, de voorgestelde behandeling en verwachte uitkomst, de risico’s die daarbij komen kijken en eventuele alternatieve behandelingen. De zorgverlener mag pas tot behandeling overgaan na expliciete toestemming van de patiënt.

In deze interactie ontstaat een “behandelrelatie” tussen patiënt en zorgverlener waarin idealiter persoonlijke informatie **vrij en zonder schroom** besproken zal worden. Er is sprake van “een vertrouwensrelatie”.

Met dit vertrouwen wordt meteen het belang van het begrip *privacy* en **het beroepsgeheim** voor het leveren van goede zorg duidelijk. Het College Bescherming Persoonsgegevens vatte in 2011 kort samen:

“*Het beroepsgeheim is wettelijk verankerd in artikel 88 van de Wet BIG en schending van het beroepsgeheim is strafbaar gesteld in artikel 272 WvSr. Het beroepsgeheim is aan de orde indien en voor zover een hulpverlener een beroep uitoefent op het gebied van de individuele gezondheidszorg*[2]*… Kern van het medisch beroepsgeheim is het waarborgen dat persoonsgegevens verkregen door een beroepsbeoefenaar niet aan anderen worden verstrekt. De beroepsbeoefenaar moet dus het geheim bewaren door te zwijgen.*[3]”

Behalve in het individueel belang is *de zwijgplicht* ook in het algemeen belang. Het aspect van algemeen belang betreft de vrije toegang tot de gezondheidszorg, zodat de patiënt

2 Hoge Raad 15 oktober 1999, *Tijdschrift voor Gezondheidsrecht* 2000/8; Centraal Tuchtcollege voor de Gezondheidszorg 16 maart 2010, *Tijdschrift voor Gezondheidsrecht* 2010/18.

3 H.J.J. Leenen/J.K.M. Gevers & J. Legemaate, *Handboek gezondheidsrecht. Deel I: Rechten van mensen in de gezondheidszorg,* Houten: Bohn Stafleu van Loghum 2007, p. 225

zonder schroom hulp kan inroepen waarbij het blootgeven van vertrouwelijke mededelingen vaak onvermijdelijk is. Zouden bij patiënten aarzelingen bestaan over de mate waarin hun gegevens bij een hulpverlener veilig zijn, dan kan dit ertoe leiden dat zij geen hulp zoeken of op een te laat moment.[4]" De kwaliteit van de behandeling is afhankelijk van de wederzijdse open communicatie en begrip van wat er aan scheelt en wat er gedaan kan worden volgens de laatste inzichten van de geneeskunst. Anderzijds is deze garantie op vertrouwelijkheid ook van maatschappelijk belang voor een goed functionerend gezondheidssysteem. Hierdoor kan worden voorkomen dat patiënten zich, door twijfel hierover, niet - of te laat - melden. *Vertrouwelijkheid* is een fundament van de zorgrelatie en zorgvuldige omgang met deze bijzondere persoonsgegevens is dan ook expliciet opgenomen in de Wet op de Geneeskundige Behandelovereenkomst.

De wet schrijft voor dat zorgverleners de plicht hebben om een medisch dossier aan te leggen, waarin gegevens staan opgenomen die nodig zijn voor een goede zorgverlening. De zorgverlener kan diagnose, het behandelplan en uitkomsten vastleggen, om zo behandeling te monitoren en eventueel in de toekomst de patiënt-historie mee te nemen bij nieuwe vragen. Gegevens moeten gestructureerd en volgens daarvoor geldende standaarden worden opgeslagen, waardoor gegevensdeling bij bijvoorbeeld doorverwijzing eenvoudiger mogelijk wordt[5]. Al deze gegevens moeten afdoende worden beschermd zodat derden geen toegang kunnen krijgen tot de medische persoonsgegevens, en mogen alleen worden gedeeld binnen een gezamenlijke behandelrelatie (bijvoorbeeld bij doorverwijzing naar een andere zorgverlener of diagnose centrum).

1.2 Brondata, Context en Samenwerkingsverbanden

Delen van gegevens is, onder voorwaarden, cruciaal voor het leveren van goede zorg. De apotheek kan met gegevens van de huisarts over allergieën en bepaalde meetwaardes controleren of medicatie verantwoord gegevens kan worden, de specialist in het ziekenhuis wil graag weten wat de medische relevante context is over een patiënt die door een huisarts is doorverwezen en de huisarts wil van de wijkverpleegkundige of thuiszorg weten of er ontwikkelingen zijn rond de gezondheid van ouderen die een aanpassing vragen van de behandeling.

Werken met brongegevens geeft de meeste garanties dat de gegevens accuraat en actueel zijn, en laten de verantwoording over die gegevens ook liggen in de context waar ze

---

4 H.J.J. Leenen/J.K.M. Gevers & J. Legemaate, *Handboek gezondheidsrecht. Deel I: Rechten van mensen in de gezondheidszorg,* Houten: Bohn Stafleu van Loghum 2007, p. 225; zie voor een recente herbevestiging van dit met het beroepsgeheim gemoeide belang ook: College van Beroep voor het bedrijfsleven 2 augustus 2010, *Tijdschrift voor Gezondheidsrecht* 2010/38: overweging 2.4.4.3

5 Naast de directe behandelrelatie kunnen gegevens ook worden gebruikt voor kwaliteitstoetsing, wetenschappelijk onderzoek en het achteraf geven van verantwoording over het handelen van de zorgverlener. Gegevens voor het afhandelen van declaraties worden niet beschouwd als onderdeel van het eigen medisch dossier. Patiënten hebben geen recht op inzage of vernietiging van deze gegevens, maar de gegevens vallen wel onder de geheimhoudingsplicht van de zorgverlener (het blijven medische persoonsgegevens). Ook persoonlijke aantekeningen van de zorgverlener worden niet beschouwd als onderdeel van het dossier, omdat het gaat om voorlopige gedachtevorming. Wel dient de zorgverlener de aantekeningen of naar verloop van tijd te vernietigen of besluiten de aantekeningen alsnog in het dossier op te nemen, omdat het van belang is voor de behandeling van de patiënt.

gegenereerd zijn – bij de bronhoudende zorgverlener. Dit is niet alleen van belang voor de **data-integriteit** (je weet zeker dat je de juiste en actuele data ziet), maar ook voor de interpretatie en **contextgebondenheid** van data (de zorgverlener-bronbeheerder zorgt dat data op de juiste manier en in context wordt gebruikt). Datagebruik via bronbeheer geeft de mogelijkheid om controleerbaar en op te verantwoorden wijzee te werken en maakt het bij-/herstellen van gegevens mogelijk waarbij correcties bij opvraging ook voor anderen inzichtelijk zijn (i.t.t. het maken van een kopie van eerder foutieve informatie die een eeuwig leven kan leiden in andere systemen).

Box 1 Foutieve contra-indicatie en medicatie[6]

Als een huisarts in het huidige systeem een recept voorschrijft kan het via het huidige uitwisselingssysteem (LSP) alle allergie en contra-indicaties opvragen die bekend zijn voor de betreffende patiënt. Het eigen systeem importeert dan alle bekende allergieën en contra-indicaties, die echter soms niet juist zijn of slechts uit de context van registratie te begrijpen zijn. Zo kan bijvoorbeeld een arts een klacht “buikpijn” registreren bij een medicijn, terwijl dit geen allergie is. Toch zal dit als rode vlag bij alle bevragingen van deze patiënt meekomen. Vaak is eenmaal ingevoerde allergie-of contra-indicatie niet meer te verwijderen. Dit kan ook consequenties hebben voor het functioneren van de opties in voorschriften in het systeem van de voorschrijvende arts zelf. Artsen en apothekers raadden nu alle medewerkers aan om contra-indicaties NIET automatisch meer op te slaan, maar dit met de patiënt te bespreken. Sommigen spreken van een grote landelijke bug in het systeem. Als het al mogelijk is om de fout te verwijderen komt de fout steeds weer terug in de toekomst. Eenmaal fout, blijft door de historie fout. Correctie lijkt alleen mogelijk door persoonlijk de bronhouder/zorgverlener waar de fout staat te benaderen en die te verzoeken de foutieve informatie te verwijderen. Attendering en foutherstelling in bronsystemen kan eenvoudiger mits er laagdrempelige communicatie en feedback mogelijk is tussen zorgverleners. Hoewel de bronhouder nog steeds een handeling moet verrichten kan een netwerksysteem laagdrempelig en van bronsysteem naar bronsysteem hier handen en voeten aan geven. Daarnaast hoeft in een netwerksysteem de informatie uit andere bronnen niet noodzakelijkerwijs te worden gekopieerd maar kan elke keer alleen worden “getoond”, i.p.v. opgeslagen.

1.3 Gegevensdeling, doelbinding en toestemmingen

De behoefte aan zorggegevens in het zorgproces is divers en dynamisch. Sinds eind jaren 90 is in Nederland het zorgstelsel in een constante verandering. Eind jaren 90 kwam de digitalisering op gang zowel bij zorgverleners als bij de overheid. Het uitwisselen van berichten vormt de kern van alle primaire processen in de zorg, en het wordt belangrijker met de groeiende samenwerking in ketens en netwerken van zorgverleners die gezamenlijk de zorg aan patiënten leveren. Het zonder problemen kunnen delen van dossierkennis tussen zorgverleners die zijn betrokken bij de behandeling staat daarom ook bovenaan het wensenlijstje van zorgverleners, patiëntengroepen en politiek.

6 Het hier beschreven voorbeeld staat uitgebreider beschreven in Jongejan 2022, maar zie ook bijvoorbeeld: Jongejan 2022 over informatie in context.

Als er gegevens gedeeld worden moet dit 1) waar mogelijk gebeuren met instemming van de betrokkene, 2) de behandeling dienen en 3) voor de uitvoering van de behandeling (ook in brede zin binnen het huidige gezondheidszorgsysteem) noodzakelijk zijn. Alleen noodzakelijke gegevens (data-minimalisatie) mogen zo gericht worden gedeeld met alleen die zorgverleners die bij deze (mede)behandeling (doelbinding) zijn betrokken. Regelingen en praktijken die betrekking hebben op de verwerking van bijzondere persoonsgegevens moeten altijd worden getoetst op noodzakelijkheid, proportionaliteit en subsidiariteit, willen ze legitiem zijn.

In geval het delen van (noodzakelijke) informatie tussen twee medebehandelaars is expliciete toestemming van een patiënt niet nodig. Bij het versturen van een recept of een doorverwijsbrief naar een specialist wordt de patiënt verondersteld te weten en akkoord te zijn gegaan met deling van informatie over de op te halen medicatie of de vervolgbehandeling. Dit heet "*verondersteld toestemming*". In alle andere gevallen, zoals delen van gegevens voor andere doelen zoals onderzoek, of bij het delen van gegevens met andere 'niet zorgpartijen' (die bijvoorbeeld als ICT partij gegevens als 'zelfstandige' verwerken) is expliciete toestemming vereist.

Met de voortgaande digitalisering en de invoering in 2018 van nieuwe Europese regels aangaande gegevensverwerking (de AVG) worden in het verlengde van de bestaande regels, expliciet regels gesteld aan de zorgvuldigheid en veiligheid om juist de vertrouwelijke relatie tussen zorgverlener en patiënt te kunnen behouden in het digitale tijdperk, waaronder

1. Expliciete regels rond **verwerking van gegevens namens een zorgverlener.** Als we het voorbeeld nemen van een ICT systeem van een arts dan is de zorgverlener verantwoordelijk voor de handelingen van de leverancier van dit eigen ICT systeem
2. Toestemming is nodig bij **zelfstandige verwerkers** (zoals dienstverleners[7] die gegevens onder eigen beheer transporteren of beschikbaar maken voor derden).

Voor het eerste wordt verondersteld dat de ICT leverancier als verlengde arm en onder controle van de zorgverlener werkt en is geen toestemming nodig. Wel moet de zorgverlener daadwerkelijk controle en zeggenschap hebben over de ICT-systemen, inspraak hebben op haar inrichting en expliciete garanties en afspraken maken over beheer en de veiligheid[8]. In het tweede geval moet de patiënt expliciet toestemming geven, waarbij de patiënt moet kunnen overzien *hoe, door wie* en *wanneer* gegevens worden bewerkt en kunnen worden ingezien (*informed consent*).

Naast deze regels rond verwerking van gegevens in ICT systemen gelden ook regels over *privacy by design* die onder meer vereisen dat gestreefd wordt naar dataminimalisatie en dat bij uitwisseling van medische gegevens deze *end-to-end* worden verzonden[9]

7 Denk hierbij aan het LSP of het toestemmingregister dat toestemmingen regelt in het LSP - Mitz
8 https://www.dirkzwager.nl/kennis/artikelen/cbp-uit-zorgen-over-inzet-aspsaas-in-de-zorg/
9 In order to safeguard security of networks and services, and without prejudice to the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences, the use of encryption for example, end-to-end where appropriate, should be promoted and, where necessary, encryption should be mandatory in accordance with the principles of security and privacy by default

1.4 WGBO in ICT?

Ron Rozendaal, toenmalig directeur Informatiebeleid en CIO van VWS vroeg zich hardop af of het mogelijk zou zijn een ICT systeem op te zetten die de uitwisseling onder veronderstelde toestemming volgens het WGBO kon implementeren zonder extra administratieve lasten en kopzorgen van uitbestede uitwisselingssystemen en toestemmingsvereisten. Uitwisseling onder veronderstelde toestemming zou een veel idealere opzet zijn voor gegevensuitwisseling maar dat is niet mogelijk via een uitwisselingssysteem[10]. De oplossingsrichting die in de discussie ontstond lijkt op de systematiek van "push-autorisatie" en "pull op een later moment", zoals geïmplementeerd in Whiteboxsystems.[11]

Een systematiek die volgens de WGBO werkt moet in ieder geval zorgen dat:

- Gegevens rechtstreeks gaan van bron-zorgverlenerssysteem naar opvragende zorgverlenerssysteem.
- De toestemming (autorisatie) van de bronzorgverlener aan medebehandelaar veilig en eenduidig moet aankomen bij de medebehandelaar
- De opvragende doelpartij daadwerkelijk moet bewijzen dat die is wie die zegt dat die is.
- Veilig transport (*end-to-end-encrypted*).

Zoals we later zullen zien in hoofdstuk 3 zijn ICT implementaties met een veilige gerichte autorisatie, en uitwisseling van bronsysteem naar doelsysteem, bewezen geïmplementeerd, maar de ondersteuning, investering en coöperatie binnen het zorgveld is nog beperkt. In het laatste hoofdstuk gaan we in op hoe dit verder kan worden uitgewerkt in de toekomst.

Wat hier van belang is dat geconstateerd moet worden dat uitwisseling tussen zorgverleners volgens het WGBO zeker breed gewenst wordt – niet alleen door zorgverleners, maar ook vanuit VWS, dat het mogelijk is, maar alleen heeft het, ondanks onderkende voordelen en mogelijkheden, nog steeds niet de nodige ondersteuning gehad van overheid en andere belangrijke sturende partijen in het huidige zorglandschap.

2. Regierollen, het veld en de overheid

Met de WEGIZ is VWS voornemens de regierol voor het ICT landschap in de zorg naar zich toe te trekken. Het doet dit bij wet door elektronische uitwisseling van patiëntgegevens verplicht te stellen en het kan eisen stellen aan Zorg ICT leveranciers over inrichting, normalisering, koppelmogelijkheden en veiligheid van de systemen. Aanpalend subsidieert VWS met veel geld projecten voor "gemeenschappelijke voorzieningen" en voor de aansluiting van Zorg-ICT partijen die landelijke uitwisseling mogelijk maken.

---

and by design. DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (97) and **https://www.tomshardware.com/news/european-parliament-end-to-end-encryption-communications,34809.html**

10 https://www.ronroozendaal.nl/blog/2019/12/toestemming-een-bijdrage-aan-de-hoedanwel

11 https://whiteboxsystems.nl/mblog/reactie-verwarring-toestemming

Centraal in de plannen zijn een toestemmingsregister dat handen en voeten moet geven aan de eis in de Wet Cliëntrecht in de Zorg en de Wet Aanvullende Bepalingen verwerking Persoonsgegevens in de Zorg. Dit register wordt cruciaal geacht om gegevens uit te wisselen in het LSP, maar ook tussen verschillende uitwisselingssystemen zoals LSP, XDS-systemen van de ziekenhuizen of regionale initiatieven voor gegevens uitwisseling zoals via HINQ of andere platforms.

In dit hoofdstuk schetsen wij eerst wat achtergrond om de complexiteit van dit systeem dat rond een centrale as is georganiseerd inzichtelijk te maken. Hierna volgt kort een discussie over specifieke toestemming, waarna verderwordt ingegaan op de problematische aspecten van het centralistische systeem zoals dat nu op problematische wijze verder wordt uitgebouwd.

Hieronder wordt beschreven wat de achtergrond is van waaruit het huidige voorstel is ontstaan voor een centraal "toestemmingen register", dat toegang regelt van 'alle Nederlanders' voor 'alle zorgverleners'. We zien dat een steeds meer afgezwakte vorm van het idee van toestemming leidt tot 1) een steeds minder specifieke toestemmingsverlening en 2) tot het weghalen van de toestemmingsverlening bij de bronhouder en verplaatsing daarvan naar een centraal systeem. Het resulterende systeem blijkt problematisch wat betreft de wettelijke grondslag, maar ook wat betreft de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Het systeem lijkt bovendien niet bestand tegen de groeiende vraag naar flexibele aanpassing van een systeem en vormen daarboven een ernstig veiligheidsrisico door de aard van de centrale opzet met toegang tot alle dossiers van Nederland.

2.1 Wat achtergrond: LSP als knooppunt in de zorg

Vanaf eind jaren 90 maakte de overheid grote plannen voor stimulering van ICT bij de overheid.[12] Ook in de zorgsector werden plannen opgesteld voor een overheidsinfrastructuur met als prioriteit het kunnen inkijken van zorgverleners in elkaars dossier. Het uiteindelijke doel was *"… het komen tot een virtueel, transmuraal en multidisciplinair EPD."*[13] In 2002 wordt hiertoe Stichting NICTIZ[14] opgericht die in de daaropvolgende jaren de zogenaamde AORTA-architectuur ontwikkelde waarin NICTIZ als "zorgmakelaar" en "centraal knooppunt", of ook wel "Landelijke Schakelpunt" (LSP), fungeert voor inzage in ***alle*** Elektronische Patiënten Dossiers (EPDs) van Nederland.[15] Daarnaast werd verwacht dat uiteindelijk het declaratieverkeer via deze infrastructuur zou kunnen gaan lopen, evenals alle verwijzingen en dat de informatie ook voor beleid en onderzoek zou kunnen worden gebruikt (WRR, 2010;22, Nictiz 2002[16]). De AORTA plannen

12 De Vos 2018 De ontwikkeling van de ICT Gegevens-infrastructuur van de Overheid in relatie tot de 3 Gemeentelijke Decentralisaties in het Sociaal Domein. Essay over privacy in complexe data-infrastructuur. Voswiz, Wageningen
13 Beleidsbrief en Actieplan ICT in de Zorg aan de tweede kamer, 28 november 2000, Brief van de Minister van Volksgezondheid, Welzijn en Sport, Kamerstuk: 27 529-1.
14 Twist et al (2012) Het EDP voorbij? NSOB
https://www.eerstekamer.nl/eu/overig/20120207/rapport_het_epd_voorbij_evaluatie
15 "De scope van de referentiearchitectuur is breder dan de meeste enterprise architecturen: het betreft hier een landelijke en sectorbrede opzet voor de gehele gezondheidszorg." Alle hier genoemde termen voor de knooppuntfunctie worden in dit document aangehaald. Aorta referentiearchitectuur voor de zorg – Inzending Nederlands Kampioenschap ICT-architectuur, NICTIZ/VKA, 29 september 2005.
16 "Mogelijke toepassingen in deze gebieden zijn: inzage van de patiënt in zijn elektronisch patiëntendossier (patiëntenzorg); het indienen en controleren van declaraties (financiën en administratie); het opvragen

waren vanaf de start deel van Nederlandse Overheid Referentie Architectuur (NORA) [17], en bleven dit ook *na* het stopzetten van het project onder overheidsregie (vanwege privacy bezwaren in de Eerste Kamer[18]), en ook na de doorstart van het project als privaat initiatief in 2011.[19]

Sindsdien is het LSP met horten en stoten doorgestart, aanvankelijk alleen voor medicatie uitwisseling en huisartsenwaarneming, met wisselend resultaat en blijvende problemen (knooppunt-ontwerp[20], geen *end-to-end* encryptie[21], inhoudelijke technische problemen[22] en kosten[23]).

Een belangrijk criterium dat het College Bescherming Persoonsgegevens heeft verbonden met het huidige gebruik van het LSP is dat – in lijn met de latere AVG - voor het uitwisselen van gegevens door een landelijke infrastructuur toestemming moet worden gegeven voor de uitwisseling.

Het CBP stelt (2011)[24]: *"Ten aanzien van het in het Doorstartmodel geschetste scenario moet worden geconstateerd dat het bij het onder het beheer van VZZ vallend schakelpunt gaat om* ***grootschalige****,* ***risicovolle*** *verwerking van* ***bijzonder gevoelige gegevens****. In een dergelijke grootschalige context raakt de verwerking van patiëntgegevens feitelijk buiten de sfeer waarover de hulpverlener nog geacht kan worden feitelijk, daadwerkelijk controle te kunnen uitoefenen."(nadruk van de auteurs) "…[er] blijft voor de gegevensverwerking door VZZ, vanwege het wegvallen van uitzicht op een specifieke wettelijke regeling, uitsluitend een beroep over op* ***'uitdrukkelijke toestemming'*** *zoals bedoeld in artikel 23 eerste lid onder a Wbp."*

De rechter specificeert later dat - in lijn met de voorstellen van VZVZ zelf – bij doorontwikkeling van het LSP naar meerdere beroepsgroepen (dus voorbij de toepassing

---

van de beschikbaarheid van bedden en het afstemmen van afspraken bij verwijzingen (planning en logistiek);
het vaststellen van Diagnose Behandel Combinaties tussen instellingen (beleid en sturing) en het toegankelijk maken van relevante informatie voor de diverse registraties (kennis en wetenschap)".NICTIZ (2002;14)

17 https://www.noraonline.nl/wiki/AORTA_(Landelijke_infrastructuur_voor_berichtuitwisseling_in_de_zorg)

18 Advies Raad van State bij de Wet WEGIZ: https://zoek.officielebekendmakingen.nl/stcrt-2021-22996.pdf

19 Bij de doorstart gaat het LSP verder onder een andere beheersstructuur en formele aansturing van een Vereniging van Zorgverleners voor Zorgverleners (VZVZ), betaald door de Zorgverzekering. VZVZ medewerkers (aanvankelijk veelal NICTIZ medewerkers) zitten nog steeds in hetzelfde gebouw als NICTIZ

20 Een fundamenteel ontwerp-bezwaar tegen centrale infrastructuur is dat een inbraak, hoe goed beveiligd dan ook, kan leiden tot "besmetting" van het hele systeem, terwijl bij netwerk systemen bij inbraak alleen een lokaal aanvalspunt en eventueel direct verbonden stations gevaar lopen. Dit is een bezwaar dat voor vele gezondheidsinfrastructuur geldt zoals bijvoorbeeld het LSP en het XDS-systeem (beelduitwisseling). Een netwerk-oplossing is *by design* minder risicovol dan een "fietswiel" oplossing. De belangrijke principes van dataminimalisatie en scheiding zijn afgedekt in de netwerk oplossing terwijl het fietswiel overmatig gebruik bijna uitlokt en dus allerlei nieuwe vereisten meebrengt om dit te voorkomen.

21 https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/02/08/kamerbriefover-versleuteling-gegevens-lsp/kamerbrief-over-versleuteling-gegevens-lsp.pdf

22https://www.zorgictzorgen.nl/sterk-wisselende-betrouwbaarheid-medicatieoverzicht-lsp/

23 https://www.zorgictzorgen.nl/groot-traag-duur-en-vol-lucht-lsp-2/ en https://www.zorgictzorgen.nl/onbeschaamde-stimulering-lsp-functionaliteit-met-overheidsgeld-in-twinproject/

24https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20110816_zienswijze_nictiz_epd.pdf

van Waarneming in de huisartsenzorg en medicatieoverdracht), en andere informatie, elke keer opnieuw toestemming moet worden gevraagd aan de patiënt.[25]

2.2 Gespecificeerde toestemming, specifieke toestemming, toestemming

Via de wet Cliëntrecht voor de Zorg[26] is eerst getracht te regelen hoe bovengenoemde toestemming moet gaan plaats vinden. Hierbij geeft de patiënt aan dat hij toestemming geeft om medische gegevens door te geven voor een specifiek doel en een specifieke zorgverlener. Voor het doorgeven van gegevens aan een nieuwe (categorie) zorgverlener(s) moet wederom toestemming worden gevraagd. We zien hier dat in feite de "specifieke toestemming" die in principe in een goed doordacht systeem moet worden ingebouwd al wordt verdund tot – wat de toenmalige Minister taalkundig strategisch in nieuwe terminologie voorstelde als – "*gespecificeerde*" toestemming.

Een werkgroep van experts zocht uit hoe een dergelijk systeem vorm moet krijgen (project Gespecificeerde Toestemming – GST), maar kwam in de zomer van 2018 tot de conclusie dat minimaal 160 categorieën te onderscheiden zijn, met evenzovele vinkjes die door een patiënt zouden moeten worden gezet[27]. Een onwerkbare situatie voor zorgverleners (die de toestemming moeten vragen en vastleggen), voor patiënten (die door de bomen het bos niet meer zien) en voor ICT-leveranciers (die zeer complexe toestemmingen moeten programmeren). Na deze vernietigende studie besloot de Minister (Schippers, 2017) de eis van Gespecificeerde toestemming en de registratie hiervan uit te stellen.

Een ICT expert en CEO van Founda die al jaren in Nederland en Europa werkt aan gegevensuitwisselingen verzucht in een blog: "*Daar waar het afserveren van artikel 15a lid 2* [specifieke toestemming HV] *had moeten leiden tot het inzicht dat de aan de GTS gekoppelde landelijke on-line toestemmingsvoorziening (OTV, ikgeeftoestemming.nl, volgjezorg.nl) op zijn minst heroverwogen had moeten worden, nam het Informatieberaad Zorg het onnavolgbare besluit om het OTV project (dat ondertussen tot Mitz was hernoemt) door te zetten. Waarom en met welke autoriteit dit besluit is genomen is mij nog altijd onduidelijk*"[28].
In plaats van te zoeken naar alternatieven die wel konden zorgen voor een gewenste en afdoende wettelijke basis voor uitwisseling van gegevens en specifieke doorverwijzing van de ene behandelaar naar de andere, bijvoorbeeld door het stimuleren van decentrale inrichting van toestemmingen en berichtenverkeer, koos VWS met VZVZ er voor om via aanpassing van- en een te ruime interpretatie van wettelijke regels een al in gang gezet

25 "In een rechtszaak tegen de voortzetting van het LSP betoogde de rechter: "Het betoog van VPH c.s. dat de toestemming onvoldoende bepaald is omdat deze zich uitstrekt tot de toekomstige toepassingen van de zorginfrastructuur, brengt de rechtbank niet tot een ander oordeel. VZVZ heeft de op dit punt geuite vrees afdoende weerlegd door er op te wijzen dat het systeem weliswaar geschikt is voor bredere toepassing, ***maar dat het Toestemmingsformulier slechts ziet op de in de Brochure beschreven situaties. Volgens VZVZ zal bij uitbreiding van het systeem opnieuw om toestemming worden gevraagd voor de nieuwe toepassingen."*** https://zorgictzorgen.nl/vzvz-komt-toezegging-bij-rechtbank-over-lsp-niet-na/
26 https://zoek.officielebekendmakingen.nl/stb-2016-373.html
27 https://www.nictiz.nl/wp-content/uploads/2018/06/PBLQ_Rapport-Gespecificeerde-toestemming.pdf
28 https://smarthealth.live/2021/07/08/blog-we-zijn-op-de-verkeerde-weg-met-een-centrale-voorziening-voor-patient-toestemming/

gesubsidieerde bouw van een toestemmingsregister (een vereenvoudigd GST systeem) alsnog in de lucht te krijgen.

In 2020 is de Wet Cliëntrecht deel geworden van de Wet Aanvullende Bepalingen Verwerking Persoonsgegevens in de Zorg(Wabvpz)[29]. Hierin wordt de toestemming-eis weer gesteld; *"De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselingssysteem, voor zover de zorgaanbieder heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven"*. Het gaat hierbij om het verlenen van toestemming voor toekomstige opvraging (pull) door een nog onbekende behandelaar, en verwerking van medische gegevens door een "tussenpartij" – ***het elektronisch uitwisselingssysteem*** (EUS).

In de opzet van de ICT werd echter de eis van 'gespecifieerde of specifieke toestemming', zoals bedoeld bij de rechtelijke uitspraak over doorontwikkeling van het LSP waarbij de patiënt weet naar wie hij/zij wordt doorverwezen en welke informatie wordt gedeeld, losgelaten voor een veel generiekere toestemming voor 'een groep' van behandelaren en een voor gedefinieerde 'set van gegevens'. Door het bouwen van een oplossing en die maar gewoon te presenteren wordt gehoopt dat de oplossing vanzelf 'legitiem' wordt.

Interessant is dat bij de hele toestemmingsdiscussie die gekoppeld aan de eis van elektronische uitwisseling wordt gevoerd, de voormalig directeur Informatiebeleid van VWS signaleerde dat: " *… [er]* ***moet*** *voor uitwisseling in de behandelrelatie - die mag met veronderstelde toestemming - uiteindelijk een vorm van uitwisseling worden gevonden,* ***waar geen extra toestemming voor nodig is****. Want om een gegevensuitwisseling* ***verplicht*** *digitaal te laten verlopen mag er geen extra toestemming nodig zijn (****omdat je die niet kunt afdwingen****)."*[30]

Terecht stelt de Directeur hier dat er naast de centrale uitwisselingssystemen (met toestemmingsvereisten) een optie MOET worden gevonden en geïmplementeerd die (onder WGBO-veronderstelde toestemming) uitwisseling mogelijk maakt omdat een zorgverlener niet gedwongen kan worden het beroepsgeheim op te heffen!

Bovendien had de Eerste Kamer al in 2016 de eis gesteld aan de overheid dat naast het huidige pad van de private centrale uitwisseling van medische behandelgegevens (het LSP) ook ontsluiting van gegevens via ***decentrale koppeling*** te regelen waarbij ***bij de zorgverlener toestemming wordt vastgelegd***.[31]

Verderop zullen we beschrijven hoe partijen die decentrale gegevensuitwisseling – voortbouwend op eerdere initiatieven – en uitgaande van rechtstreekse uitwisseling van

29 https://wetten.overheid.nl/BWBR0023864/2020-07-01
30 https://www.ronroozendaal.nl/blog/2019/12/toestemming-een-bijdrage-aan-de-hoedanwel ; **nadruk** van de auteurs van dit schrijven
31 Motie Teunissen, 2016

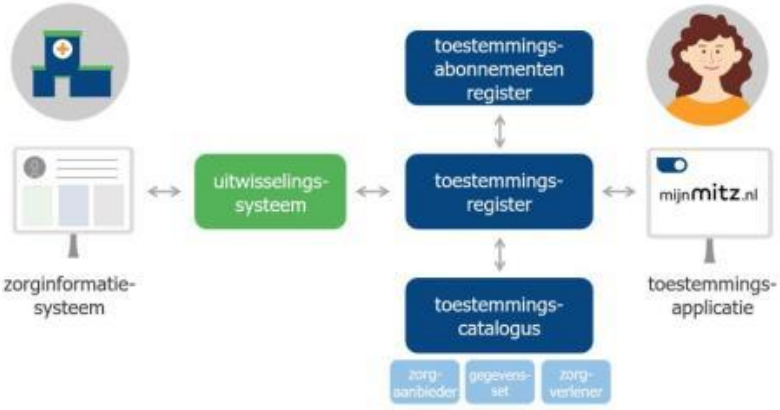
gegevens tussen de ICT-systemen van zorgverleners (decentrale koppeling) middels een open standaard en open koppelvlakken hier een invulling aan geeft.

2.3 Het Online Toestemmingsregister : Mitz

Als antwoord op bovenstaande discussie heeft VZVZ in samenspraak met VWS een toestemmingenregister opgezet, voor het regelen en vastleggen van toestemmingen: het systeem “Mitz”.

Op de website van Mitz lezen we : “Voor het elektronisch delen van medische gegevens is vaak toestemming van de patiënt nodig. Het bijhouden van die toestemmingskeuzes gebeurt nu op veel verschillende manieren en plaatsen. Steeds opnieuw, vaak anders en regelmatig handmatig. Gevolg: de patiënt heeft geen regie en geen goed overzicht over de eigen toestemmingskeuzes.[32]” Feitelijk beschrijft Mitz (VZVZ) dat in de huidige situatie gegevensuitwisseling op onduidelijke – niet geïnformeerde wijze – plaatsvindt; in feite een illegale praktijk waarop tot nog toe niet is gehandhaafd.

Mitz stelt daarom: Mitz is opgericht “*… zodat iedere Nederlander zelf zijn/haar keuzes kan vastleggen en beheren. In Mitz worden* ***de toestemmingskeuzes*** *van* ***iedere*** *Nederlander voor* ***álle*** *zorgsectoren vastgelegd.*”.[33]



“De Mitz-architectuur bestaat uit verschillende onderdelen:

• De toestemmingsapplicatie is de … website waar patiënten rechtstreeks of vanuit een externe omgeving, zoals een patiëntportaal, laagdrempelig met single sign on van DigiD hun toestemmingskeuzes vastleggen.
• Het toestemmingsregister is de plek waar toestemmingskeuzes op een beveiligde manier worden opgeslagen en gecontroleerd kunnen worden.
• Het toestemmingsabonnementenregister bevat de abonnementen van zorgaanbieders op hun patiënt, zodat zij genotificeerd kunnen worden over wijzigingen in relevante

32 https://www.mitz-toestemming.nl/
33 idem

toestemmingskeuzes.
• De toestemmingscatalogus bevat de toestemmingsmogelijkheden."[34]

Voor een beter begrip van wat hier is opgezet (en al wordt gebruikt) is het goed te kijken wat de verschillende onderdelen van Mitz doen en inhouden. De patiënt geeft op een website aan- via een door VZVZ voor gedefinieerde set mogelijkheden **(*toestemmingscatalogus***) - voor welke 'groep zorgverleners' hij welke 'set data wil delen'. VZVZ bepaalt hiermee feitelijk vooraf de mogelijkheden voor "de toestemmingsinhoud". Hierdoor is het onmogelijk de inhoud flexibil in te richten naar gelang de context van zorg dit vereist. Ook is het lastiger – op maat- niet noodzakelijke informatie af te schermen, omdat vooraf bepaald is wat de inhoud is. . Een nieuwe set van gegevens definiëren of aanpassen overeenkomstig ontwikkelingen in de zorg vergt steeds weer lange procedures en overleg met professionals en beroepsorganisaties en zal altijd een compromis zijn van wat mogelijk is en wat door verschillende behandelaren wordt geëist en gewenst. Gezien de dynamische ontwikkeling van zorgprocessen en netwerkzorg is eigenlijk een flexibelere opzet van uitwisseling vereist waarin meer specifiek en flexibel bepaald kan worden welke informatie-uitwisseling wel en niet noodzakelijk en wenselijk is.

De keuze wordt opgeslagen in het **'*toestemmingsregister*'**: hierin staan dus naast "ja/nee" voor het delen, ook gegevens over de patiënt (minimaal BSN, waarschijnlijk meer) en denkend aan het zorgproces: minimaal 'gegevens over het type zorg met doelgegevensset': immers zorgverleners 'wijzen patiënten bij intake op de mogelijkheid (of wens) om gegevens te delen'[35] voor bijvoorbeeld een operatie of doorbehandeling. Dit betekent dat dit register medische persoonsgegevens bevat.

Om te weten bij welke zorgverlener gegevens staan van een patiënt moeten bronhouders lijsten van patiënten opslaan in **'het abonnementenregister'**[36]. In dit register staan dus patiënt-id's met zorgverleners. Ook dit register bevat per definitie medische persoonsgegevens.

Via het abonnementen-register krijgen zorgverleners ook notificaties van wijzigingen in toestemmingen van hun patiënt.[37] Notificaties van toestemming (of intrekking daarvan) moeten automatisch worden verwerkt in het ICT-systeem van de zorgverlener, zodat deze (het Bronsysteem) opvraging voor uitwisseling al dan niet mogelijk maakt (ongeacht het uitwisselingssysteem dat de vraag stelt).

Bij opvraging door een zorgverlener kan de zorgverlener gegevens opvragen via een Elektronisch Uitwisselsysteem (EUS), bijvoorbeeld het LSP, XDS of HINQ, waarbij het EUS een vraag naar Mitz stuurt: wie heeft gegevens over patiënt "x"?. Het US vraagt vervolgens : heeft patiënt "x" toestemming gegeven voor de opvragende partij om daar gegevens op te vragen?

---

34 idem
35 https://www.mitz-toestemming.nl/
36 In sommige gevallen weet het US zelf al waar welke gegevens staan: het LSP heeft zelf een register met patiënten*zorgverleners voor medicatie.
37 idem

Het systeem staat ook registratie van toestemmingen toe bij de behandelend arts. In geval er geen toestemming is gegeven door de patiënt en de patiënt bij de zorgverlener staat mag de zorgverlener zelf alsnog 'in naam van de patiënt' een toestemming registreren in Mitz en zal Mitz het EUS (en het bronsysteem) toestemming geven gegevens op te halen. Een zorgverlener kan dus altijd besluiten niet gegeven toestemming alsnog in te voeren en gegevens op te halen.

Het beheer van Mitz valt onder VZVZ. VZVZ is daarmee de verwerker van alle bovengenoemde informatie, plus van een belangrijk uitwisselingssysteem (EUS) het LSP.

2.4 Problematische grondslag voor Mitz[38]

Zoals we zagen is - in het geval uitbreiding van het LSP - , maar ook voor het opzetten van een register zoals geïmplementeerd in Mitz, het noodzakelijk dat de betrokken patiënt *informed consent* kan geven. Hier mikt VZVZ en VWS op bij het voorstel Mitz als oplossing voor het breder delen informatie te gaan gebruiken.

Het is belangrijk met bovenstaande kennis als achtergrond te beschouwen of de grondslag die wordt gepresenteerd ("uitdrukkelijke toestemming van de patiënt") afdoende is voor het doorbreken van het beroepsgeheim en het delen van informatie via de voorgestelde systematiek (2.4.1). Daarnaast is het echter nodig ook de vereiste noodzakelijkheid, proportionaliteit en subsidiariteit in ogenschouw te nemen (2.4.2). Pas na afweging kan worden vastgesteld of de middelen het doel heiligen (2.4.3).

2.4.1 Mitz en de verantwoordelijkheid voor verwerking

Zoals we hierboven al zagen verwerkt Mitz medische persoonsgegevens in verschillende onderdelen van het systeem. Zeer problematisch is de verwerking van deze gegevens is "het abonnementenregister". Om patiënten in het systeem vindbaar te maken, meldt de zorgaanbieder **een lijst met álle patiënten uit diens patiëntenregistratie** aan bij Mitz. Dit *vullen van een lokalisatie index* gebeurt onder een verwerkersovereenkomst – althans, dit is hoe Mitz/VZVZ dit wil organiseren/inrichten[39]. Het feitelijke belang van het aanmelden van een lijst met álle patiënten per zorgaanbieder in Mitz, is dat Mitz hiermee de juiste zorgaanbieders/EPDs kan *lokaliseren,* zodat gegevensontsluiting vanuit bronsystemen *onmiddellijk en geautomatiseerd* kan plaatsvinden.

De beheerder van Mitz, VZVZ, is feitelijk de verwerker en verwerkingsverantwoordelijke voor het systeem, maar wil deze verantwoordelijkheid "weg-organiseren" door zorgverleners 'gezamenlijk verantwoordelijk' te maken en te gaan werken onder een verwerkersovereenkomst. Hiertoe suggereert het "Trustmodel" dat zorgverleners op regionaal niveau gezamenlijk onderling overeenkomsten moeten sluiten en samen een verwerkersovereenkomst met VZVZ moeten sluiten. De zorgverleners kunnen echter nooit deze verantwoording op zich nemen gezien de complexiteit en grootschaligheid van de context, of zoals het CBP dit verwoordde in 2011 "*.. grootschalige, risicovolle verwerking van bijzonder gevoelige gegevens.* ***In een dergelijke grootschalige context raakt de verwerking van***

38 In de Bijlage zit een samenvatting van de belangrijkste bezwaren van de privacy organisaties tegen het Mitz
39 Antwoord van de Minister bij vragen tweede kamer lid Van den Berg stuk 1807 maart 2023.

patiëntgegevens feitelijk buiten de sfeer waarover de hulpverlener nog geacht kan worden feitelijk, daadwerkelijk controle te kunnen uitoefenen…".[40] Doel en middelen voor de ICT worden vastgesteld door VZVZ, niet alleen voor Mitz, maar voor de hele bredere opzet en link met het LSP (en feitelijk ook de manier waarop andere systemen kunnen koppelen met het LSP en Mitz).

De gekozen aanpak in het Mitz lijkt op die van het Landelijke EPD in de wet-EPD uit 2010. In dat systeem werden gegevens van alle patiënten (voor zover deze geen bezwaar maakten via een *opt-out)* aangemeld bij de verwijsindex van het LSP, zodat deze in beginsel opvraagbaar waren voor andere zorgaanbieders. Die andere zorgaanbieders moesten (behalve in spoedsituaties) toestemming vragen om gegevens op te mogen vragen, op het *point of care.* Hiertoe kregen zorgverleners een *pop-up scherm* te zien met de vraag of toestemming gevraagd was, welke bij bevestiging door de zorgverlener in het scherm kon worden vastgelegd waarna de gegevens direct werden opgevraagd.

Mitz biedt de middelen voor lokalisatie van dossiers en toegangscontrole bij de bevraging van dossiers op een functioneel gelijkwaardige manier als in het oude, inmiddels afgewezen, L-EPD / LSP model. In feite wordt op deze manier alsnog een Landelijk EPD ontwikkeld, met als voornaamste verschil dat het nu via het 'Online Toestemmingen Register' verloopt – echter functioneel en qua werkwijze is de aanpak zeer vergelijkbaar met het systeem uit 2010, dat door de Eerste Kamer werd verworpen. Het risico op ongeoorloofde opvraging van gegevens bij Mitz is net als bij het oude EPD/LSP model niet minder geworden, omdat de achterliggende systematiek hetzelfde is, maar het aantal aangesloten systemen op de centrale toegang groter. De omvang en het risico is dus enorm toegenomen.

Er ontbreekt dus een juridische basis voor het aanmelden van *alle* patiënten bij Mitz onder een verwerkersovereenkomst (- met zorgverleners, dan wel ICT-leveranciers -). Op zijn minst gelden voor deze constructie *alle* overwegingen die ook vermeld zijn in de zienswijze van het CBP op het LSP uit 2011.

2.4.2 De Wettelijke grondslag "geïnformeerde specifieke toestemming" voor delen van informatie (doorbreking van het beroepsgeheim)

Omdat Mitz zoals hierboven is beschreven zelf een bewerker is van een complex systeem van informatie met risicovolle medische persoonsgegevens kan met het Mitz alleen gewerkt worden met toestemming.

Het probleem van complexiteit van systematiek: informed consent

Aan de toestemmingseis is pas voldaan als de toestemming in vrijheid is gegeven en gebaseerd is op inzicht in de consequenties van de keuzes en de risico's die hieraan verbonden zijn.

Toestemming voor Mitz is noodzakelijk omdat VZVZ een verantwoordelijk zelfstandig verwerkingsverantwoordelijke is. Deze toestemming is feitelijk onmogelijk (als *informed consent*) te geven gelet op het gebrek aan duidelijkheid en transparantie vanwege de

40 CBP, 2011

groeiende complexiteit en uitgebreidheid van de systemen, verschillende uitwisselingssystemen en registers.

Problematisch daarbij is dat ook feitelijk in Mitz medische persoonsgegevens staan opgeslagen in de Registers voor toestemmingen en in het Abonnementen Register. Hiervoor is geen wettelijke basis, behalve als patiënt – naast voor de uitwisseling zelf - ook hiervoor uitdrukkelijk toestemming geeft. Een patiënt moet dan kunnen overzien wat de aard, omvang en inhoud van deze toestemmingen is en wat dat allemaal betekent voor de zorg, maar ook hoe risicovol het is en of het veilig is. Deze gestapelde technologische brei van oplossingen van gekoppelde centrale systemen – en hun interactie met bronsystemen- is problematisch en moeilijk uit te leggen.

Illustratief in dit verband is de Corona Opt-out discussie. Wie in Nederland weet dat er via de Corona opt-out wetgeving alle persoonlijke medische dossiers waarvoor geen toestemming was genoteerd plots is "aangezet"? Is deze niet geïnformeerde toestemming inmiddels al weer teruggedraaid? Wie in Nederland weet dat als in een ziekenhuis wordt gevraagd "wilt u uw gegevens delen met uw huisarts" via welk systeem dat gaat en of dat veilig is? De kluwen van legitimatie, systemen, administraties van toestemmingen en registers die elkaar nodig hebben en met elkaar verbonden zijn, de beveiligingsmaateregelen die zijn getroffen – de mogelijke alternatieven - dit alles is nu al met alleen het LSP voor een patiënt niet meer goed uit te leggen.[41]

Met *nog meer complexiteit* met de drie registers in het Mitz wordt het niet eenvoudiger een patiënt voor te lichten om *informed consent* te geven. Feitelijk kan de patiënt echter niet overzien waar hij toestemming voor verleent en hoe de verwerker van zijn gegevens (Mitz) werkt; van '*informed consent*' is hier geen sprake.

Daarnaast speelt echter nog dat ook over de inhoud van wat wordt gedeeld geen overleg in context plaatsvindt tussen de bronhouder-zorgverlener en de patiënt zodat samen besloten kan worden wat nodig is in een volgende stap van zorg en ook voor de inhoud van "*informed consent*" kan worden gesproken. De plaats van toestemming zit op de verkeerde plek en veroorzaakt problemen voor de intentie en principes van het beroepsgeheim.

Onterechte aanname over Beroepsgeheim

ZorgICT-watcher Wim Jongejan schreef aangaande Mitz: "*Door zowel de toestemming als de beslissing over het al dan niet buiten de zorginstelling versturen van persoons-/behandelgegevens buiten de zorgverlener-/patiëntrelatie te halen is er in feite sprake van een aantasting van het medisch beroepsgeheim.*"

VZVZ gaat er expliciet vanuit dat doorbreking van beroepsgeheim mag bij een registratie van toestemming door de patiënt in Mitz, of door de zorgverlener die in een praktijk navraag doet bij de patiënt en de toestemming dan namens de patiënt invult.[42] Of de toestemming

41 Jongejan (2020) en Jongejan (2020) en Jongejan (2020)
42 Online toestemmingvoorziening: Mitz als Bouwsteen, 1 september 2020.

van patiënt voor het delen van informatie altijd tot een "*informed*" besluit kan leiden door de patiënt is de vraag. Kan een patiënt overzien of zijn toestemming voldoende informatie oplevert of juist teveel? Is een patiënt vrij in de keuze – zoals de wet dit duidelijk vereist - als een zorgverlener van hem vraagt gegevens van andere zorgverleners te delen, in de angst geen behandeling te krijgen - als hij 'nee' zegt.

VZVZ/Mitz legt hiermee onterecht 'het recht op doorbreking van beroepsgeheim' bij de patiënt zelf. Maar: "*De informatie die tussen arts en patiënt gewisseld is en de resultaten van onderzoek plus overwegingen van de arts vallen onder het medisch beroepsgeheim. De arts legt die vast in een zorg-informatiesysteem.* ***Dat beroepsgeheim is bij wet belegd bij de arts****. Die is er ook door zijn artseneed aan gehouden. De klassieke betekenis van het beroepsgeheim is dat bij het delen van informatie met een andere zorgverlener er altijd sprake moet zijn van toestemming van de patiënt. Toestemming voor welke informatie, voor welk doel, met een gekende derde wordt uitgewisseld. Een generieke (algemene) toestemming om toekomstige, dus nog onbekende, informatie uit te wisselen is daar al strijdig mee. … Wat betreft de toestemming van de patiënt om zorgdata te delen met niet-behandelaars dient men zich terdege te beseffen dat die toestemming het medisch beroepsgeheim niet noodzakelijkerwijs opheft. Een arts heeft de* ***plicht*** *zich af te vragen of het beschikbaar stellen van zorgdata aan derden wel in het belang is van de patiënt.* ***De arts is en blijft de geheimhouder die eigenstandig beslist over het verschaffen van zorgdata aan instanties.*** *Het kan zeer wel voorkomen dat hoewel de patiënt toestemming gaf, de arts het niet in het belang van de patiënt acht dat die informatie uitgewisseld wordt. Niet verlangd kan worden dat de arts, ook al zegt de patiënt toestemming te geven,* ***automatisch*** *medische informatie, in welke vorm dan ook doorstuurt. Of die gegevens klakkeloos openstelt voor toekomstige raadpleging*."[43]

Dit argument was bekend bij VZVZ en VWS, en werd in de juridische analyse van het programma GST (2020)[44] al gepresenteerd: "*Rechtsgeldige toestemming [van de patiënt] ontheft de hulpverlener van zijn* ***zwijgplicht*** *en geeft de hulpverlener een spreek****recht****.* ***De hulpverlener heeft geen spreekplicht of kan niet gedwongen worden het geheim te doorbreken.*** *Hij is zelf verantwoordelijk voor het maken van een professionele afweging waar hij dat nodig acht. "*

De intentie van de WGBO en AVG wordt pas ingevuld met een systeem waarbij de hier bedoelde toestemming wordt vastgelegd **bij de bron**, **door de bronhouder, in interactie met de patiënt**. Mitz kan hier niet aan voldoen. Het Mitz geeft niet de "mogelijkheid" of vraagt de bronhouder niet of hij met de toestemming van de patiënt (delen) van zijn dossier wil openstellen. Mitz is zo opgezet dat er sprake is van **"openstellingsdwang"**.

Volgens bovenstaande discussie is "toestemming" van de patiënt op zich noodzakelijk, maar **niet voldoende** voor doorbreking van het beroepsgeheim. Door registratie van toestemming

43 Jongejan (2020) Online toestemmingsregister gaat uit van onjuiste premisse t.a.v. medisch beroepsgeheim
44 Toestemming is niet vrijelijk verleend, en dus ongeldig, als de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen. Programma GST (2020)

ook door een opvragende zorgverlener mogelijk te maken implementeert het Mitz de mogelijkheid voor alle zorgverleners die (op zijn minst zeggen) een patiënt voor zich te hebben openstelling van alle zorgdossiers in Nederland. Dat is een heel ver opgerekte interpretatie van toestemming en is niet de doordachte “specifieke of gespecificeerde toestemming’ die de rechter had vereist en VZVZ had beloofd waar te maken.

Een route waarbij VWS, NICTIZ, ZN en zorgverleners naar een eenvoudiger opzet zou streven in plaats van voort te bouwen op een oud en centraal opgezet systeem zou verlichting kunnen brengen in de warboel van ICT, wetgeving en administratieve cirkels, nieuwe organisatie en lokale overeenkomstvereisten en voortgaande creativiteit om steeds aangepaste nieuwe wetten te maken om wat krom is en in strijd is met de wet te legitimeren.

De eenvoud in opzet en transparantie *moet* en *kán* beter. Via een decentrale aanpak valt eenvoudig uit te leggen en in te zien hoe toestemmingen verlopen (rechtstreeks van zorgverlener 1 naar zorgverlener 2) en wie inzage heeft gehad (is de toestemming daadwerkelijk omgezet in een inzage). Hiermee kunnen op specifiek zorgverlener niveau inzage rechten worden gegeven en hoeft een patiënt niet als een waakhond signalen in te zien of niet illegaal is ingelogd (want dat kan nu eenmaal in de huidige opzet). De zorg verdient betere, eenvoudigere en transparantere oplossingen.

2.4.3 Noodzakelijkheid, Proportionaliteit en Subsidiariteit

Naast een wettelijke grondslag voor verwerking moet de verwerking ook op zijn minst voldoen aan de criteria van noodzakelijkheid, proportionaliteit en subsidiariteit. Mitz beoogt het mogelijk te maken dat zorgverleners informatie met elkaar kunnen delen. Op zich is dit een veelgehoorde wens en staat het met het groeiende belang van netwerkzorg hoog op de agenda van zorgverleners en beleidsmakers.

Het delen van informatie kunnen we opsplitsen in twee situaties: spoed en NIET spoed. NIET spoed betreft 99% van alle berichtenuitwisselingen in het land. Spoed is daarmee een uitzonderingssituatie die specifieke aparte eisen stelt aan berichtenverkeer. Het is niet logisch de eisen van spoed aan het gehele systeem te stellen als spoed ook op andere manieren kan worden bediend.

Niet Spoed

Zorgverleners wensen en “vinden het handig” als ze op eenvoudigere wijze dan nu het geval is informatie kunnen delen. De noodzaak is aanwezig om hier oplossingen voor te vinden, maar de urgentie is lager dan bij levensbedreigende spoed. De toepassing die nu is gebouwd is zo opgezet dat er een (centraal) vast gedefinieerde set van gegevens kan worden doorgegeven, zonder enige flexibiliteit of afstemmingsmogelijkheid met de context. Informatie is echter pas optimaal bruikbaar in de één-op één mede behandelrelatie, waarbij de bronhouder kan meedenken en bepalen wat nuttige informatie is in de context van de klacht en de patiënt en met kennis van wat te verwachten valt van de doorverwijzing of medebehandeling. Dat zal vaak een standaard set gegevens zijn maar kan ook per geval verschillen. Flexibiliteit is nodig en met het toenemende belang van netwerkzorg is dit zelfs een essentieel vereiste.

De noodzakelijkheid van het nu voorgestelde systeem heeft niet alleen een problematische rechtsgrond, maar lijkt ook niet echt noodzakelijk zeker gezien het feit dat nu al allerlei informatie op minder inbreuk makende manier wordt en kan worden gecommuniceerd en alternatieven mogelijk zijn die minder inbreuk makend zijn (via rechtstreeks verbindingen, verwijsbrieven, decentrale opties of andere communicatiekanalen).Dit allesomvattende systeem waarbij je als behandelaar - zelfs eigenhandig toestemming kan verlenen namens een patiënt - en daarmee gegevens kan opvragen is niet alleen *niet* 'urgent' nodig, het vormt door zijn centrale opzet en omvang een ernstig veiligheidsrisico, zeker in het huidige tijdsgewricht - in het licht van de nieuwe geopolitieke spanning - waarin de kwetsbaarheid van centrale systemen steeds duidelijker wordt.

De centrale opzet maakt het systeem gevoelig voor misbruik (medische gegevens zijn veel waard in het illegale circuit) en maakt het 'aantrekkelijk' voor aanvallen van buiten. De impact van een mogelijke hack is rampzalig. Ook betekent uitval dat heel Nederland hier last van zal hebben, omdat het een 'single point of failure' vormt. Verder maakt de centrale opzet het mogelijk dat door een politiek of administratief besluit alle gegevens "open" gesteld zullen worden voor de toepassing die dan voorligt. De invoering van de Corona -opt out laat zien dat een "druk op de knop" toegang tot (delen van) het dossier technisch mogelijk wordt. We zeggen en hopen niet dat hier misbruik van wordt gemaakt, maar geven wel aan dat het risico bestaat dat het – al dan niet met criminele, dan wel politieke, intenties – ooit kan gebeuren.

Voorts lijkt de optie "zorgverleners kunnen ook toestemming zelf invullen voor een patiënt" zeer risicovol: bij het LSP konden al grote aantallen zorgverleners met eigen of geleende UZI-pas in alle regionale dossier van patiënten kijken, met het nieuwe systeem zal dit aantal exponentieel groeien als ook "alle zorgverleners" via het toestemmingsregister (weliswaar alleen voor hun - op landelijk niveau bepaalde – 'relevante' gegevens) kunnen opvragen. Dit verhoogd het risico op een incident waarbij door onrechtmatige inzage dossiers worden gestolen of verspreid[45]. De toenmalige al uitgebreide toegangsmogelijkheden van het LSP zelf (alleen dienstwaarneming en medicatie) waren in 2011 al een belangrijke reden om het wetsvoorstel in de Eerste Kamer af te keuren[46]. 99% van de medische data tussen zorgverleners betrokken bij een behandeling behoeft niet te worden ingericht overeenkomstig overwegingen en vereisten verbonden met zorgverlening in een spoedsituatie.

Spoed

In het geval van spoed is het voorstelbaar dat het nodig en functioneel handig is als je altijd bij de gegevens kunt van anderen als de patiënt met spoed bij jou is binnengebracht (ambulance, Spoedeisende Hulp, andere situaties van spoed). De opzet waarbij je in dat geval als behandelaar als een soort "*breaking glass*" – waar mogelijk met toestemming van

45 Het gemak om medische gegevens te stelen van kritische personen zoals de premier of de generaals van het Nederlandse leger en de mogelijke beloning bij verkoop weegt al snel op tegen het risico op ontdekking – de vogel is dan al lang gevlogen. De opzet van het systeem zelf is niet robuust.

46 De minister noemde dat er naar verwachting 200.000 tot 300000 uzi passen in omloop zouden zijn waarmee opvragingen konden worden gedaan. Met het Mitz stijgt dit aantal exponentieel naar alle zorgverleners in Nederland.

de patiënt gegevens ophaalt die van levensbelang zijn kan vallen onder het criterium van noodzakelijkheid.

In het geval van Mitz gaat het om een systeem waarbij de mogelijkheid bestaat “alle relevante informatie” van “alle behandelaren” te laten ontsluiten – de opzet is echter overkill: bij spoed wil je alleen het allernoodzakelijkste hebben, zoals gegevens over allergie en contra-indicatie en kritische medicatie. Hoewel dus de methodiek van doorbreking van beroepsgeheim op de locatie van de spoedinterventie een systeem met de logica van Mitz zouden kunnen legitimeren onder het criterium “noodzakelijkheid”, is nu de hele opzet te uitgebreid, voor teveel zorgverleners toegankelijk en te verstrekkend wat betreft informatie-inhoud. Ook hier is dus de techniek niet toegespitst op de spoed-situatie. De dubbele intentie van het huidige systeem maakt de boel onnodig ingewikkeld.

Het is logisch dat de gedachte van een *breaking glass*-methode via een centraal register voor een apart systeem voor Spoed een logische keuze is, maar dat kan een veel bescheidener systematiek zonder een elektronisch uitwisselingssysteem (namelijk decentraal rechtsreeks van vrager naar bron) en kan ontworpen worden volgens de criteria van *privacy by design*, kan patiënten keuze geven hier aan mee te doen en kan transparant worden opgezet.

Onlangs[47] is in de Tweede Kamer een voorbeeld van een alternatieve systematiek, gebaseerd op een vrij beschikbare Open Standaard Autorisatie (DECOZO), gepresenteerd.

Proportionaliteit en subsidiariteit

De zeer risicovolle verwerking van persoonsgegevens roept meteen de vraag op: Is de verwerking nog wel proportioneel? Waarom is het nodig een heel ingewikkeld en duur systeem op te zetten? Kan het niet beperkter en is er geen alternatieve methode dan wel alternatief systeem?

De doorontwikkeling van de huidige opzet vergt niet alleen veel geld[48] (meer dan 3 miljard naast het jaarlijkse bedrag voor de jaarlijkse kosten voor de LSP aansluiting die wordt betaald door ZN), het is ook een enorme inspanningsverplichting voor de ICT-leveranciers die allen – weliswaar vaak betaald- maar wel verplicht verschillende koppelingen moeten aanmaken en de deuren van hun systeem moeten open zetten.

In een document[48] gericht aan de Eerste Kamer presenteert VWS de volgende gegevens: tot 2026: 0,5 miljard voor ‘generieke functies’ (*a: pagina 2*), waarmee wordt beoogd centrale EU-Systemen te faciliteren. De overheid schat daarbij in dat voor elke zorgaanbieder per functionele aansluiting 20.000 euro beschikbaar wordt gesteld. Voor 1000 zorgaanbieders wordt zo 20 miljoen Euro per functie begroot (*pagina 8*). Daarnaast wordt 1,4 miljard geïnvesteerd in “geprioriteerde gegevensuitwisselingen” (pagina 3) en nog eens ruim 1 miljard in medicatie-overdracht (*b: pagina 3*). Deze uitwisselingen zijn beoogd te lopen via de centrale uitwisselings-infrastructuur. Daarnaast wordt ingeschat dat 287 miljoen Euro nodig is voor “kosten landelijke infrastructuur” (*c: pagina 3*) die de landelijke gegevensuitwisselingen ondersteunen. Ook voor de periode na 2026 zijn substantiële bedragen gebudgetteerd.

47 9 februari 2023. Zie ook de website DECOZO.org – nieuwsberichten.
48 VWS 26 november 2021 Digitale Gegevensuitwisseling en ICT-Infrastructuur in het Zorgdomein

Een veelgehoorde klacht in de gebruikerscommissies van huisartsen is dat voor het implementeren van verbetering van hun systeem er welgeteld een handvol ontwikkeldagen beschikbaar zijn tegenover de berg aan wettelijk verplichte aanpassingen van de systemen aan de gemeenschappelijke voorzieningen.

Het doel van de huidige opzet van LSP met Mitz en aanpalende programma's als TWINN (die toegang tot ziekenhuisgegevens regelen) is dat via het Centrale Uitwisselingssysteem (van LSP) alle gegevens van alle zorgverleners met gemak centraal worden ontsloten. Je kunt met recht in twijfel trekken of voor een normale behandeling het nodig is dat alle gegevens overal en van iedereen wordt ontsloten.

De proportionaliteitseis is nog belangrijker omdat alternatieven ook mogelijk zijn, zoals rechtstreekse koppeling via een decentrale koppelingsopzet die zich al op verschillende manieren bewezen heeft, zoals bij NUTS en ouderenzorg, en het voorbeeld van dienstwaarneming in Amsterdam en Maastricht (Whitebox). (zie verder hieronder).

Nu uit de regelgeving blijkt dat een optie zonder toestemming niet alleen minder ingrijpend is maar ook **móet** (zie 2.2 Ron Roozendaal en voetnoot 24) èn de kamer de overheid de opdracht heeft gegeven om *decentrale uitwisseling* uit te werken[49] èn de betaler van het de lopende kosten van huidige LSP-Mitz-systeem de decentrale route toch als zeer veelbelovend heeft aangemerkt[50], is het van belang dat de *subsidiariteiteis* luid en duidelijk te stellen. Alle seinen staan op groen voor een beter alternatief.

49 Motie Teunissen, 2016
50 WeDoTrust , 28 oktober 2019 Onderzoek Whitebox. Zorgverzekeraars Nederland.

3. Open standaarden en netwerkstructuur versus centrale voorzieningen

Uitwisseling tussen ICT systemen kan via twee wegen: 1) via een centraal "knooppunt" of "*man in the middle*" (ofwel het zogenaamde 'fietswielmodel') waarbij alle informatie via een centrale as verloopt die de uitwisseling medieert, dan wel via 2) een "netwerk model" ofwel decentrale koppeling van ICT-systeem van zorgverlener "a" rechtstreeks naar ICT systeem van zorgverlener "b".

ICT professionals, wetenschappers en *privacy by design* onderzoekers wijzen de laatste jaren steeds vaker op de grote voordelen van een netwerksysteem voor de veiligheid, meer gerichte uitwisselingsmogelijkheid en flexibelere opzet.

Ook VWS streeft naar een beter stelsel van decentrale uitwisseling en heeft zich voorgenomen dit waar mogelijk als voorkeurs-opzet te stimuleren: *"In een open decentrale architectuur worden kwetsbare zwakke schakels en de afhankelijkheid van één of weinig systemen zo veel mogelijk vermeden. Dit betekent bijvoorbeeld dat niet alle zorginformatie via één enkel knooppunt wordt uitgewisseld. Of dat alle gegevens op één plek bewaard worden. Dit zou namelijk leiden tot grote afhankelijkheid van één dienstverlener en tot risico's voor de continuïteit van zorg en de informatiebeveiliging."*[51] De regering streeft naar "een decentrale oplossingen tenzij" strategie. 'Tenzij' doelt op het geval dat er dringende uitzonderingsredenen zijn om dit anders te doen (idem).

Conceptueel valt op dat VWS spreekt van 'meerdere knooppunten' en dat dit zou kunnen worden opgevat als een vorm van 'decentraal'. Hoewel het juist is dat bij meer knooppunten vermeden wordt dat er 1 '*point of failure*' is (functionele uitval), blijft het zo dat ook meerdere knooppunten een groot risico inhouden voor inbraak of misbruik. Elk knooppunt geeft immers toegang tot vele zorgverleners-gegevens, helemaal als de architectuur zo is opgezet dat alle knooppunten aan elkaar verbonden worden (via bijvoorbeeld een project als TWIN). Dan zijn dus alsnog alle gegevens via elk knooppunt afzonderlijk benaderbaar. Het gebruik van knooppunten bij decentrale, dus rechtstreekse, uitwisseling van gegevensverkeer is helemaal niet nodig (zoals hieronder wordt beschreven). Hierdoor is het risico van rechtstreekse uitwisseling beperkt tot gegevens van 1 patiëntendossier.

Voor een decentrale- (of netwerk) aanpak is nodig dat ICT-bronsystemen elkaar kunnen vinden en begrijpen. Tot nog toe is bij gebrek aan regie gekozen voor 'ad hoc' oplossingen voor verbindingen tussen systemen, waarbij pragmatisch wordt gekozen voor een koppelmethode, en een methode om elkaar te kunnen herkennen en erkennen als legitieme partij in de interactie. Hierdoor is het lastiger de oplossing 1-op-1 door te zetten naar een nieuwe aansluiting omdat de oplossingen vaak afhangen van de eigenaardigheden van de bron en het ICT-doelsystemen zelf.

Al in 2017 was de opzet van een Open Standaard voor Push Autorisaties door NICTIZ erkend als veelbelovend concept voor uitwisseling van gegevens in de zorg[52] en in 2020 schreef

---

51 Brief van de Minister voor Medische Zorg 233. Informatie – en communicatietechnologie in de zorg. Tweede Kamer der Staten Generaal: 27529. 15 december 2020.

52 NICTIZ (2017) Onderzoek zorginfrastructuur, 28 februari 2017, J.L van Duivenbode, Nictiz, The Netherlands en API strategie Nictiz 2022

WeDoTrust voor Zorgverzekeraars Nederland dat het 'het concept van de Open Standaard Push Autorisatie' een veelbelovende oplossing is voor uitwisseling in de toekomst, die zeker moet worden onderzocht en uitgewerkt [53]. Ook eerder aangehaalde directeur Informatiebeleid van VWS herhaalde in 2020: "*…maak het mogelijk om in de behandelrelatie voor een specifieke vraag digitaal informatie op te vragen met digitaal bewijs van zowel identiteit van de arts als van (veronderstelde) toestemming van de patiënt.* ***Dat volgt de WGBO*** *…*".[54]

Open standaarden en open koppelvlakken zijn een betere en toekomstbestendige optie om een systeem voor gegevensuitwisseling op te zetten, waarbij alle ICT-partijen op zelfde wijze gebruik kan maken van goed doordachte en getoetste methoden van koppelen en elkaar her(er)kennen[55]. Recentelijk heeft VWS deze strategie omarmd als "de Api strategie", en tracht deze interoperabiliteit te bevorderen.[56] Het idee is schaalbaar en zal zich ook veel beter en flexibeler kunnen aanpassen aan steeds nieuwe vragen die ontstaan in de netwerkzorg.

Op dit moment zijn er twee belangrijke initiatieven die toepassing van open standaarden in decentrale oplossingen in praktijk brengen: NUTS[57], en de Stichting DECOZO[58]. NUTS is een netwerk van ICT-leveranciers die samen via afspraken decentrale-rechtstreekse koppelingen tussen ICT systemen opzetten en software-koppel-modules openbaar beschikbaar stellen. DECOZO is een initiatief dat door het structureel beheer van open standaarden, koppelvlakken en software voor decentrale communicatie tot doel heeft betere, veiligere en eenvoudigere berichtenuitwisseling mogelijk te maken.

3.2 Open Standaard Push Autorisatie

De techniek die is neergelegd in de Open Standaard Push Autorisatie (hierboven genoemd door NICTIZ en ZN) is bewezen technologie en is al eerder toegepast voor dienstwaarneming in Amsterdam en Maastricht. Andere bewezen toepassingen zijn: visite rijden, patiënten-inzage, dienst-waarneming en in PoC voor ketenzorg, via een lokale applicatie van huisartsen – de Whitebox . Onlangs is tijdens een HL7-NUTS-hacketon een *use case* voor medicatie overdracht van de ene zorgverlener naar de volgende samen met verschillende ICT leveranciers en NUTS gedemonstreerd[59]. De toepassingen laten in praktijk telkens zien dat – naast de standaarden van informatiesets voor bepaalde doelen – het ook telkens mogelijk is maatwerk toe te passen. Hieronder zal iets verder worden uitgelegd wat de voordelen van deze Open Standaard zijn.

De logica van de Open Standaard Push Autorisatie is dat een bronsysteem rechtstreeks een inzage-toestemmingslink kan sturen naar een doelsysteem of mee kan geven aan de patiënt.

---

53 WeDoTrust , 28 oktober 2019 Onderzoek Whitebox. Zorgverzekeraars Nederland.
54 Ron Roozendaal, Chief Information Officer VWS, 1 december 2019, https://www.ronroozendaal.nl/blog/2019/12/toestemming-een-bijdrage-aan-de-hoedanwel
55 Zie voor een discussie over her(er)kenning van elkaars systemen op de website voor Openstandaarden: https://www.gidsopenstandaarden.org/identiteit-authenticatie
56 Op weg naar een API strategie in de Zorg. Advies rapport aan Ministerie van VWS. 17 december 2021.
57 https://nuts.nl/position-paper/
58 https://decozo.org/#over-ons
59 https://youtu.be/qeadC5w9oR4 vanaf minuut 59.30

Met de toestemmingslink kan de behandelaar in het doelsysteem rechtstreeks het dossier van de patiënt inzien. Dit heet “push autorisatie van pull-rechten”.

De toestemmingslink kan meer of minder informatie bevatten, met vooraf gedefinieerde of zelf in te richten “rechten en plichten”, bijvoorbeeld ‘wie mag inzien’, ‘wanneer’, ‘hoelang’ en ‘welke informatie’, maar ook: ‘tweede zorgverlener mag onder x,y,z-voorwaarden inzagelink doorgeven aan volgende zorgverlener’ en ‘zorgverlener mag via de opgezette verbinding terugrapporteren’.

Naast zorgverleners kunnen ook patiënten een inzagelink krijgen, waarmee inzicht in eigen dossier, maar ook bijvoorbeeld in wat er met gegevens gebeurt tijdens het zorgproces (logging). De standaard heeft een zeer sterk uitgewerkt vertrouwensmodel in vergelijking met andere uitwisselingsopzetten, is het zeer flexibel en modulair op te zetten en leidt in het zorgproces als bijproduct tot inzicht in het netwerk van zorg rond een patiënt.[60]

De open standaarden en koppelvlakken die door DECOZO worden beheerd passen goed in de strategie van de overheid om te komen tot open APIs voor uitwisseling van gegevens in de zorg. DECOZO heeft recentelijk een open koppelvlak gepubliceerd (OKAPI) waarmee - naast de koppeling van gegevens zelf - het beleid van gegevensuitwisseling strak is ingeregeld. Zo kan bijvoorbeeld de verplichting gelden dat het bronsysteem aan het vragend ICT systeem vraagt of uitwisseling via “veronderstelde toestemming” of “expliciete toestemming” is geregeld. In dat laatste geval zal de bronhouder-zorgverlener voordat gegevens benaderbaar worden gemaakt eerst een toestemming moeten registeren, of omgekeerd kan in het andere geval de API direct aan de vraag voldoen. OKAPI is een illustratie hoe decentrale standaard oplossingen regelgeving kunnen “inbouwen” en implementeren in de praktijk.

Potentieel is de systematiek van de Open Standaard Autorisatie veel uitgebreider dan alleen het regelen van inzage – maar ondersteunt het ook indirect het opzetten en bijhouden van een netwerk van zorg rond de patiënt (met alleen die zorgverleners die betrokken zijn bij de zorg), waarbij het ook mogelijk wordt voor een huisarts om doorverwijzingen ‘door een ziekenhuis’ te volgen of om historische gegevens te delen als dat nodig is voor de behandeling. Tot slot is de systematiek goed denkbaar in te zetten voor geografie onafhankelijke Spoed-zorg.[61]

De toepassing (zie box[62]) van de Open Standaard Push Autorisatie DECOZO, samen met de toepassing van identificatie en koppeling van zorgverlener-organisaties van NUTS, bewijst dat makkelijke toegang en goede privacybescherming niet strijdig zijn. De toepassing maakt ook duidelijk dat strikte toepassing van de WGBO en communicatie onder veronderstelde toepassing goed te implementeren zijn in techniek. De WGBO bakent heel precies af welke

60 Zie voor een discussie over vertrouwensmodellen in verschillende uitwisselingssystemen: https://www.gidsopenstandaarden.org/identiteit-authenticatie

61 *Emergencycode.eu*; Travelling Safely with Secure Access to your Medical Data (TESAME) Hozizon202 proposal. Van ‘t Noordende & de Vos 2017.

62 https://youtu.be/qeadC5w9oR4 vanaf minuut 59.30

uitwisseling van gegevens wel en niet binnen het zorgproces toegestaan is, met afdoende ruimte voor invulling door de professional binnen het zorgproces.

> *Tijdens een HL7-NUTS Hacketon in december 2022 is de case "actueel medicatie-overzicht" uitgewerkt door NUTS, DECOZO en Meditools, voor toepassing van standaard receptenverkeer, maar ook bijvoorbeeld inzien door patiënten of door wijkverpleegkundigen. De methodiek kan ook als "open" toestemming worden opgezet via de patiënt die onbekende toekomstige wijkverpleegkundigen toestemming kan geven. Via NUTS methodiek kun je de eenmalige toestemming "bestendigen" tot een tijdelijke of permanente link tussen twee zorgverleners(organisaties). Zo wordt in het proces van zorg het netwerk van zorgverleners opgebouwd en wordt bij elke volgende stap van zorg in potentie het hele zorgnetwerk gekoppeld.*
>
> *Een dergelijke flexibele aansluiting van nieuwe netwerkzorgers laat ook te kracht zien van het decentrale model dat flexibel de zorg kan volgen.*

Concreet: als gegevensuitwisseling nodig is binnen de kaders van een behandeling met bijvoorbeeld een specialist is uitdrukkelijke toestemming voor deze uitwisseling van gegevens niet nodig als de gegevens rechtstreeks van bijvoorbeeld de huisarts naar specialist gaan (veronderstelde toestemming – geen gegevens-verwerkend uitwisselingssysteem). De systematiek van Push Autorisatie maakt dit mogelijk. De huisarts stuurt een toegangs-toestemming, de specialist kan rechtstreeks opvragen. Ook kan inzagerecht worden gegeven bij (of toegevoegd aan) bestaande processen zoals verwijzen, of het sturen van een medicijnrecept. De systematiek werkt zo dat *alleen* de ontvanger van een recept of een verwijzing vervolgens gegevens kan ophalen. Hierdoor zijn *privacy* en *security by design* optimaal gewaarborgd.

3.3 Implementatie van Open Standaarden

De voordelen van open standaarden zijn groot, omdat het gemeenschappelijke afspraken transparant maakt voor alle betrokken partijen. Iedereen kan de werking (efficiëntie, veiligheid, eenvoud) toetsen en in een beheersstructuur, zoals DECOZO, kunnen in overleg met het veld aanpassingen en bijstelling worden doorgevoerd.

Open standaarden en koppelvlakken voor *gezamenlijke functies* maken het mogelijk toekomstbestendige en schaalbare ICT te ontwikkelen Door het delen van standaard samenwerkings-software blijft de complexiteit die bij samenwerking in het Nederlandse zorgstelsel komt kijken beheersbaar[63]. Dit is nadrukkelijk ook de ontwikkelfilosofie van partijen als Stichting en Netwerk NUTS en Stichting DECOZO.

63 Zie ook bijvoorbeeld: https://www.gidsopenstandaarden.org/algemene-informatie en NUTS.nl

Het concept van open standaarden en open koppelvlakken maakt het mogelijk voor ICT-bedrijven van zorgverleners (eventueel met ondersteuning) deze standaarden te kunnen inbouwen, of als blokje software (*docker*) aan hun systeem te koppelen. De Open Standaard Push Autorisatie is zo'n standaard die ingebouwd of als docker kan functioneren om uitnodigingen te versturen met een vooraf geteste "poort" in een kasteelmuur die voldoet aan herkenbare afspraken (toegang alleen met een paspoort samen met uitnodiging door de kasteelheer)[64]. Dit maakt adoptie laagdrempelig, sneller te implementeren en veel eenvoudiger dan de ingewikkelde constructies (en voortdurende uitbreidingen) die tot nog toe zijn opgezet om de via zelfstandig opererend centraal uitwisselingssysteem de toegang tot gegevens te bedienen.

Wat nog mist is een sterkere ondersteuning vanuit het zorgveld (VWS, ZN, ICT-bedrijven) om met financiële, organisatorische middelen en tijd ruimte te bieden voor veiligere oplossingen.[65] Nu heeft het huidige systeem de schijn tegen - waar dat met de zeer ruime middelen beschikbaar voor de ontwikkeling van systemen voor informatie-uitwisseling in de zorg - slechts voor 1 optie wordt gekozen, namelijk voor de doorontwikkeling van LSP en aanverwante centrale systemen en voorzieningen, met al de daarmee verbonden beperkingen, problemen en risico's zoals hierboven besproken. Meer ondersteuning voor decentrale opties is tenslotte ook een wettelijk vereiste gezien de Motie Teunissen die ondersteuning van decentrale koppeling eist, en het voornemen in de WEGIZ om decentraal waar mogelijk te stimuleren.

64 "Het Mitz-verstand van toestemming in de zorg." Franssen 3 juli 2020.
65 Jacobs (2009) Architecture is politics: http://www.cs.ru.nl/~bart/PAPERS/cpdp09-jacobs.pdf

4 Conclusie : het moet en kan anders

Bij ICT en privacy vraagstukken dient altijd de vraag te worden gesteld of – naast de wettelijke grondslag- de voorgestelde ICT oplossing functioneel werkt, of het doel de middelen heiligt (proportionaliteit) en of er geen minder zwaar middel is om hetzelfde doel te bereiken (subsidiariteit).

Feitelijk zien we dat de oplossing die nu wordt gezocht er één is die voortkomt uit het ICT-systeem dat er nu eenmaal is: als je vanuit de techniek vraagt hoe je via een centraal punt gegevens kan doorgeven zul je direct het antwoord krijgen dat dan alle gegevens van alle patiënten en zorgverleners bekend moeten zijn op het centrale punt zodat de ICT zijn werk kan doen. De zorgverleners, de organisatie en de rechten van de patiënten en zelfs wetten moeten zich dan maar aanpassen om de ingeslagen weg te kunnen vervolgen. Dit is duidelijk een techniek-gedreven oplossing die gebruikers vraagt zich maar te schikken naar de ICT. De ICT-oplossing wordt hierbij gepresenteerd als een noodzakelijkheid omdat “het immers niet anders kan”.

Een decentrale oplossing (het kan wel anders) gaat uit van goede afspraken en protocollen waar de berichtenuitwisseling aan moet voldoen en implementeert die in de context van de plek waar de uitwisseling start en de wens voor gegevensdeling zich voordoet; in de zorgverlenerspraktijk. De decentrale optie is een zorgvolgend proces, waarbij ICT zich aanpast aan de processen van het dagelijkse zorgproces van zorgverleners en patiënt.

Hierom willen we als conclusie ingaan op een vergelijking van het huidige voorstel voor uitwisseling met een alternatieve – decentrale – opzet van gegevensdeling binnen de Nederlandse zorgsector.

In onderstaande tabel wordt geïllustreerd hoe twee verschillende methodes (1. Toestemmingen-register/EUS en 2. Decentrale koppelingen) zijn ingericht en aangeven wat er minimaal nodig is voor het functioneren bij de twee ideaaltypes voor gegevensuitwisseling.

Uit de tabel blijkt vooral dat een aanpak volgens de decentrale weg veiliger, goedkoper en transparanter is. Bovenal is het een veel eenvoudiger oplossing voor gegevensdeling, die het mogelijk maakt aan de privacy-eisen en de WGBO te voldoen en minder invasief is. Er hoeven geen ingewikkelde beheersorganisaties en samenwerkingsverbanden te worden opgezet en de WGBO kan volledig overeind blijven. De WGBO is een centraal onderdeel van ons zorgstelsel waarin de patiënt in vertrouwen alle informatie kan delen onder het beroepsgeheim met de wetenschap dat de informatie veilig is en alleen wordt gedeeld met in het kader van de behandeling.

De privacy wetgevingseisen geven aanleiding om de decentrale opzet nu door te zetten en het verder investeren in grote complexe onduidelijke dure systemen te staken. Omdat op dit moment nog geen alternatief van decentrale netwerken voor heel Nederland is geïmplementeerd is het te begrijpen als de huidige aanpak voorlopig – onder voorwaarden van zorgvuldigheid en beperktheid – zonder de uitbreiding wordt gecontinueerd.

Ideaaltypes gegevensuitwisseling	**Toestemmingssysteem/EUS**	**Decentrale netwerken**
Wordt het doel bereikt (gerichte uitwisseling)?	Uitwisseling categorieën zorgverleners	Gerichte uitwisseling
	Uitwisseling alleen voor standaard set	Uitwisseling voor standaard set
		Uitwisseling voor maatwerk
Benodigde ICT	Complex van Centrale Toestemmingssystemen	Open Standaard in te bouwen door ICT leveranciers
	Eenheid van Taal	Eenheid van taal is handig / niet noodzakelijk
	Koppelvlak (nu vaak betaald door VZVZ/VWS projecten)	Open koppelvlak (gezamenlijk onderhouden)
	Centraal register zorgverleners	
	CentraalRegister patiënt*zorgverlener	
	Centrale Registers types	Is handig als er standaarden zijn voor types zorgverleners
	Adresboek zorgverleners	Adresboek is niet noodzakelijk, maar kan handig zijn
Benodigde veiligheidsmaateregelen	Authenticatie systeem	Authenticatie systeem
	Besloten Netwerk, maar heel veel gebruikers (alle zorgverleners)	Kan op internet door beschermende maatregelen
	Logging (hele complex moet gelogd)	Logging eenvoudiger
	End to end encryptie niet mogelijk/lastig	End to end encryptie ingebouwd
Kosten	LSP kostte: 30-50 miljoen per jaar - in toekomst met MITZ en andere registers veel meer	Fractie hiervan
Beheersorganisatie	Groot	Lean en samen met directe gebruikers
Verwerkingsgrond	(Problematische) Toestemming	Veronderstelde toestemming (WGBO)
	Probleem dat bronhouder gedwongen openstelling krijgt	
Administratieve last voor zorgverleners en patiënt	Bijhouden toestemmingen	Zeer laag
	Uitnodigen om toe te stemmen	In zorgproces logische handeling
	Aanvinken eigen toestemmingen namens patiënt	
Aanvullende wetgeving	Veel tijd om te proberen bestaand systeem te legitimeren	Geen aanvullende wetgeving nodig
Organisatievereisten	Vertrouwensmodel vereist dat op regioniveau een beheersorganisatie het systeem inregelt (zie website MITZ: MITZ-vertrouwensmodel)	Geen organisatie nodig
Flexibiliteit	Laag - over elke standaardwijziging moet landelijk overeenstemming bereikt	Hoog - beheersorganisatie werkt rechtstreeks met ICT leveranciers van zorgverleners. flexibiliteit is standaard ingebouwd.
Voorlichting aan patiënt	Ingewikkeld uit te leggen en landelijk ingezet	Kan in zorgproces zelf - eenvoudig uit te leggen
Foutieve informatie makkelijk te herstellen	Ingewikkeld door steeds ophalen foutieve data	Via rechtstreeks verbinding in netwerk te signaleren

De wens van de overheid te komen tot een veilig en open stelsel van decentrale Zorg-ICT waar keuzevrijheid van zorgaanbieders en patiënten is gewaarborgd[66] vereist wel dat de overheid actief stimuleert dat bewezen en veilige open standaarden en koppelvlakken worden toegepast. In plaats van de huidige financiering van doorontwikkeling van dure centrale kwetsbare infrastructuur met semipublieke middelen moet de overheid dringend starten met het actief bevorderen van decentrale opties. Dit kan door financiële steun voor verschillende toepassingen en innovaties, maar moet daarnaast ook door slimme regelgeving voor implementatie van open standaarden, beheer hiervan en APIs, die voor een veiliger, robuuster en goedkoper systeem van uitwisseling kunnen leiden.

Of zoals de eerder aangehaald ICT expert stelde: "*Geachte tweede-kamer leden, zorgbestuurders, artsen, apothekers, federaties van medisch specialisten, behartigers van patiëntenbelangen, stop alstublieft de onnodige en zinloze opmars van centralisatie in de digitale zorginformatie-infrastructuur en roep een halt toe aan onnodige en geldverslindende projecten die de zorg in zijn geheel niet verder helpen."* [67]

De Nederlandse - nu kwetsbare - kritische centrale infrastructuur van medische gegevensuitwisseling moet dringend worden aangepast aan de eisen van deze tijd. De zorg verdient ICT die het zorgproces volgt en de vertrouwensrelatie kan garanderen, in plaats van zich in bochten te moeten wringen om een centralistisch georganiseerde ICT te kunnen gebruiken.

66 Brief van de Minister voor Medische Zorg 233. Informatie – en communicatietechnologie in de zorg. Tweede Kamer der Staten Generaal: 27529. 15 december 2020.
67 https://smarthealth.live/2021/07/08/blog-we-zijn-op-de-verkeerde-weg-met-een-centrale-voorziening-voor-patient-toestemming/

Bijlage 1 Samenvatting bezwaren tegen MITZ

Opgesteld door de aanwezige Privacy Organisaties bij het beraad bij de AP op 1 december 2022 (Privacy First, Platform Burgerrechten, Stichting KDVP)

Mitz is een door VZVZ met financiële steun van Zorgverzekeraars Nederland ontwikkelde **Online Toestemmings Voorziening (OTV),** waarin centraal toestemmingen kunnen worden geregistreerd die kunnen (moeten) dienen voor het ontsluiten van gegevens uit verschillende bronsystemen, op basis van de Wabvpz[i].

De opzet, inrichting en reikwijdte van het Mitz is onnodig en disproportioneel. Het doel en de reikwijdte van Mitz overstijgt wat de wetgever en parlement (o.a. met de Wabvpz, vermijding privacyschending en uitholling beroepsgeheim) hebben beoogd.

Hoofdpunten:

1. Het standpunt van de ontwikkelaars van Mitz[ii] lijkt te zijn dat Mitz **geen eigenstandige verwerkingsverantwoordelijkheid kent** en dat de voor de werking van Mitz benodigde (medische) persoonsgegevens van *alle* patiënten[iii] onder een *verwerkersovereenkomst* in het systeem Mitz kunnen worden geregistreerd, zónder dat hiervoor uitdrukkelijke toestemming is vereist**. Ons inzien is dit onjuist** omdat:

   - VZVZ als centrale (regisserende) partij bepaalt overduidelijk **doel en middelen** (functionaliteit, werking) van Mitz;

   - Bij de registratie van de toestemming in Mitz *onder een verwerkers-overeenkomst* **hebben burgers géén mogelijkheid tot *verzet* tegen de verwerking van gegevens.** Dit terwijl de wetgever met de Wgbo en de Wabvpz nu juist heeft beoogd dat de burger altijd zeggenschap heeft, via uitdrukkelijke toestemming (o.a. via de Wabvpz).

   - Mitz heeft de techniek en de middelen zo georganiseerd dat een toestemming die op het 'point of care' (d.w.z., aan de opvragende kant) wordt geregistreerd, tot gevolg heeft dat gegevens ***direct*** worden opgevraagd;

   - **Burgers kunnen zich niet verweren tegen en hebben geen zeggenschap over** de mogelijkheid dat hun medische gegevens direct worden opgevraagd doordat een *andere* zorgverlener dan bronhouder *namens de patiënt* toestemming heeft vastgelegd, of een spoedsituatie heeft geclaimd.

   - De functionele opzet van Mitz kent veel overeenkomsten met de werking van het Landelijke EPD onder een opt-out, zoals beoogd in de wet-EPD uit 2010. Door de opzet en architectuur van Mitz (toestemming op het point of care) en de schaalgrootte zijn alle argumenten van de **zienswijze van het CBP** op het doorstartmodel voor het LSP uit 2011, **onverkort van toepassing.**

   -

2. **De 'vaststelling' van de uitdrukkelijke toestemming (Art 15a lid 1 Wabvzp) vindt in de opzet van Mitz *geautomatiseerd* plaats** (aan de bron of in het EUS), waarna ontsluiting/uitwisseling van gegevens direct kan plaatsvinden, zónder dat de bronhouder zich er bewust van is. Mitz voldoet hierdoor niet aan de eisen die de wet stelt aan de doorbreking van het beroepsgeheim.

- Zorgaanbieders die gegevens ontsluiten op basis van een in Mitz geregistreerde toestemming hebben zelf geen directe controle over de ontsluiting van gegevens. Dit in tegenstelling tot een 'traditionele' opzet van OTVs, waarbij voor het aanmelden van de gegevens een actie van de bronhouder noodzakelijk is [iv].

- Het wordt **zorgaanbieders (bronhouders) *onmogelijk* gemaakt om te voldoen aan de eisen die in wet- en regelgeving aan hen stelt,** met name de Wgbo Art. 7:457 lid 3 BW die aangeeft dat zorgverleners bij het doorbreken van het beroepsgeheim moeten nagaan dat dit de privacy van de cliënt/patiënt *en van anderen dan de patiënt* niet onnodig schaadt.

3. **De inrichting en technische architectuur van Mitz geeft een vergroting van beveiligings- en privacyrisico's** van (gevoelige) patiëntgegevens[v], vergeleken met een systeem dat uitgaat van handmatig lokaal vragen en vastleggen van toestemming zoals vereist voor de inwerking treden van de Wabvpz. Of met het handmatig overnemen van toestemmingen uit een OTV zoals beoogd onder de Wabvpz.

   - De aanpak van Mitz waarbij een bronhouder *direct en zonder interventie van een zorgverlener (de bronhouder)* gegevens ontsluit via een EUS op basis van een toestemming die door een *andere* zorgaanbieder in/via Mitz is geregistreerd, geeft een aanzienlijke vergroting van risico's op ongeoorloofd gebruik of misbruik door aangesloten zorgverleners of zorgaanbieders. Deze risico's worden vergroot doordat in Mitz gegevens *direct* ontsloten / uitgewisseld (kunnen) worden, nadat een toestemming in Mitz is geregistreerd.

   - Het risico van misbruik door hackers die zich toegang verschaffen tot systemen van zorgaanbieders die aangesloten zijn op Mitz neemt toe met het aantal aangesloten systemen.

De beoogde verwerking van bijzondere persoonsgegevens van patiënten/cliënten die (nog) geen toestemming hebben gegeven voor de uitwisseling van gegevens conform de Wabvpz, alsmede de werkwijze, de beoogde doelen, en de technische inrichting van Mitz, is **onnodig en disproportioneel.**

Het is onjuist om inrichting van systemen te baseren op werkwijzen en functionaliteiten voor andere specifieke doelstellingen zoals spoed. Het is beter om dan een separaat systeem voor dit doel in te richten, ontkoppeld van een OTV die tot doel heeft de registratie van toestemmingen door de patiënt conform de Wabpvz in te vullen. Er zijn **eenvoudiger en minder risicovolle** OTV's denkbaar. De aan het Mitz als OTV gekoppelde werkwijze rond spoed (break-the-glass) is onnodig omdat er voor burgers andere, beter begrijpelijke en **veel eenvoudiger alternatieven** bestaan.

Tevens is er een wetsvoorstel in voorbereiding dat een wettelijke grondslag (opt-out) moet gaan bieden voor gegevensuitwisseling voor de acute zorg Daarom is de beoogde verwerking van bijzondere persoonsgegevens in Mitz onnodig, **en mag dit zeker niet zonder een eigenstandige grondslag (uitdrukkelijke toestemming).**

Toestemmingsverlening is binnen het systeem van Mitz op zichzelf problematisch, omdat het gegeven de complexiteit van organisatie en werkwijze van Mitz voor betrokken patiënten niet te overzien is welke gegevens bij het verlenen van "toestemming" bij verschillende zorgverleners worden opgezet voor uitwisseling. Bij een niet uit te leggen systeem is geen sprake van *informed consent*.

Toelichting bij artikel 15a lid 1 Wabvpz, de grondslag waarop Mitz draait.

Op basis van Artikel 15a lid 1 van de Wabvpz kan een zorgaanbieder (bronhouder) patiëntgegevens aanmelden bij een Elektronisch Uitwisselingssysteem (EUS) nadat een bronhouder heeft *vastgesteld* dat deze toestemming is gegeven. De vastlegging van een toestemming kan plaatsvinden in een Online Toestemmings Voorziening (OTV)[vi].

Mitz is zo'n OTV maar doet (veel) meer dan het vastleggen van toestemmingen. Het staat behalve het vastleggen van toestemmingen *door de patiënt zelf,* ook toe dat zorgaanbieders *namens een patiënt* toestemming registreert. Mitz kent een abonnementsfunctie die niet alleen het *notificeren* van bronsystemen regelt nadat er iets in de toestemmingsregistratie van een patiënt verandert[vii], maar die ook een lokalisatieprocedure voor spoed inricht (break-the-glass).

Op basis van de in het systeem vastgelegde toestemmingen kunnen *direct* en *geautomatiseerd* gegevens worden uitgewisseld via een op Mitz aangesloten EUS. De integratie van Mitz met EUS'en leidt tot aanzienlijke en aantoonbare risico's voor de privacy/ gegevensbescherming van patiënten, terwijl patiënten in het voorgestelde model geen weet hebben van de verwerking van hun gegevens in Mitz. En dus geen recht of mogelijkheid hebben op verzet (of toestemming) met betrekking tot de beoogde verwerking.

i https://wetten.overheid.nl/BWBR0023864/2019-04-01
ii Voor de eenvoud gebruiken we het woord 'Mitz' ook als ware Mitz de organisatie die Mitz heeft ontwikkeld. Waar Mitz op deze manier wordt gebruikt, wordt bedoeld "de ontwikkelaars van Mitz", in casu VZVZ en ZN.
iii Dit betreft niet alleen de gegevens van patienten die toestemming hebben gegeven, maar de gegevens (BSNs) van áll;e patienten die geregistreerd zijn bij een zorgaanbieder; dit ten behoeve van de lokalisatiefunctie van Mitz, die onder meer voor abonnementen en bij (spoed) bevragingen gebruikt wordt.
iv Bij een handmatige verwerking van toestemmingen nadat via een OTV (handmatig) is vastgesteld dat deze gegeven zijn, kan de bronhouder deze controle desgewenst wel uitvoeren.
v Niet genegeerd kan worden dat de verwerking van gegevens voor de verschillende doeleinden van Mitzv ***bijzondere (medische) persoonsgegevens*** betreft. Bijvoorbeeld, bij het aanmelden van lokalisatiegegevens wordt het BSN van *alle* patiënten van een zorgaanbieder gekoppeld aan informatie over de zorgaanbieder. Dit kan informatie geven over het type behandeling welke een patiënt/cliënt ondergaat. Hetzelfde geldt voor een gegevens-opvragende partij. Elke opvraging vanaf een *point of care* die binnenkomt in Mitz geeft informatie over waar een patiënt zich bevindt.
vi De wijze waarop de bronhouder vaststelt dat toestemming is gegeven en de criteria waaraan de toestemming moet voldoen is in de Wabvpz niet duidelijk omschreven Mitz probeert via een *afsprakenstelsel* te komen tot (regie over) een uniforme werkwijze rond het vastleggen van toestemmingen zodanig dat uitwisseling van gegevens tussen op Mitz aangesloten zorgaanbieders eenvoudig en snel (direct zelfs) mogelijk wordt.
vii In een 'klassieke' OTV waar de primaire toestemmingregistratie lokaal is en waarbij een *break-the-glass* procedure niet in (samenwerking tussen EUS en) het OTV is geïmplementeerd, is notificatie niet nodig;