

Aan het Informatieberaad zorg

OpenConsultatiesInformatieBeraadzorg@minvws.nl

Betreft: Consultatie Online toestemmingsvoorziening: Mitz als bouwsteen

Amsterdam, 5 oktober 2020

Geacht informatieberaad,

Bij deze reageer ik op de consultatie over de Online Toestemmingsvoorziening (OTV) en Mitz.

Om meteen met de deur in huis te vallen: de consultatie begeeft zich op een gebied waar het IB niet over gaat of zou moeten gaan, namelijk een Online Toestemmingsvoorziening (OTV). Indiener ZN vraagt of de voorgestelde toestemmingsvoorziening toegelaten kan worden als bouwsteen voor het duurzaam informatiestelsel in de zorg. Het antwoord kan alleen maar nee zijn, omdat het onderwerp toestemming en de beantwoording van de vragen die daaromtrent spelen niet thuishoort bij het IB, maar bij de wetgever en het parlement.

Omwille van de overzichtelijkheid van deze reactie zal ik een reactie op de belangrijkste punten geven. Omdat ik – zoals aangegeven – van mening ben dat het voorstel dat nu ter consultatie bij het IB voorligt hier niet thuishoort, zal ik niet op elk (technisch) detail van de invulling van OTV door Mitz in het tweede deel van het document ingaan, maar vooral op de hoofdlijnen die in de eerste hoofdstukken van het voorstel zijn beschreven. Dat geeft al meer dan genoeg stof tot nadenken.

Ik loop de punten hieronder door:

1. De inbreng begint met een opmerking dat de toestemmingsvoorziening 'voorzien' wordt van open standaarden. Laat een ding helder zijn: een centrale component is nooit een open standaard, ook niet als je er via open standaarden mee communiceert. Het gaat bij OTV/Mitz om een centraal systeem, dat beheerd wordt door VZVZ. Dat iedere partij hierop kan (of moet) aansluiten, maakt het systeem niet open.
2. Op pagina 3 en in de oplegger staat: *"Een toestemming 'nee' is een bezwaar tegen een bepaalde uitwisseling (voor uitwisselingen die werken op basis van een veronderstelde toestemming, de 'opt-out')"*; de opstellers van het voorstel gaan voorbij aan de juridische werkelijkheid dat in OTV niets geregistreerd mag worden zonder toestemming van de patiënt – ook geen opt-out – en van de praktische werkelijkheid dat bij een "geen bezwaar" situatie die onder Wgbo (BW art 7:457 lid 2) valt, geen centrale component betrokken is en dat een bezwaar direct door de patiënt aan de arts kan worden gemeld en kan worden geëffectueerd;
3. Op pagina 4 staat: *"Bij het opvragen van gegevens is een nieuw vraagstuk ontstaan: hoe weet je bij welke bron de relevante en noodzakelijke gegevens opgevraagd kunnen worden; en hoe maak je aan de bron duidelijk of het beroepsgeheim doorbroken mag worden?"*; het antwoord op het tweede deel van de vraag is helder: alleen de patiënt kan dat zelf duidelijk maken, aan de dossierhouder – in persoon of met een natte of digitale handtekening;
4. Halverwege pagina 4 wordt een (valse) tegenstelling gecreeerd door een index tegenover het – ondenkbare – scenario van 'broadcasting' (om informatie te vinden) te positioneren. Een model als *push autorisatie*, wat zowel broadcasting als een (centrale/externe) index in zeer veel gevallen onnodig maakt, wordt niet genoemd;
5. Op pagina 4 wordt vermeld dat een index onder gegevensverantwoordelijkheid van de (dossierhoudende) zorgaanbieder kan blijven. Onvermeld blijft dat de AP (toen CBP) heel duidelijk heeft aangegeven dat voor een index die gebruikt wordt in grootschalige "pull" systemen, zoals de verwijfsindex van het LSP/VZVZ, onder een voor patiënten kenbare verwerkingsverantwoordelijke moet vallen en dat (mede daardoor) uitdrukkelijke toestemming nodig is voor de verwerking van persoonsgegevens (BSNs) in deze verwijfsindex.
6. Een dergelijke omstandigheid, en dus ook een vergelijkbare vereiste van toestemming, geldt evenzeer voor een OTV, met inbegrip van de gevoelige gezondheidsgegevens die in onder meer de logging bijgehouden worden. Dit wordt niet benoemd.

7. Er wordt op pagina 5 vooruitgelopen op een advies dat de minister in juni 2020 of later naar de Tweede Kamer zal sturen, aangaande GTS. Er wordt door de schrijvers vanuit gegaan dat artikel 15a lid 2 zal worden ingetrokken; echter, zelfs als de minister dit advies volgt, zal dit nog langs Tweede en Eerste Kamer moeten. Ook als dit snel verloopt, is er een kanttekening te plaatsen. Op pagina 5 onder 1a wordt niet alleen gesteld dat art.15a lid 2 wordt ingetrokken, maar ook dat de resterende *uitdrukkelijke* toestemming 'conform ATR' een brede toestemming kan zijn, waarbij de patiënt achteraf kan controleren of de raadplegers wel behandelaren zijn. De ATR wordt hier zonder meer aangehaald, maar daarbij wordt voorbijgegaan aan de lange publieke discussie die voorafging aan de vereiste van gespecificeerde toestemming in de Wabvpz en aan Europese wetgeving die generieke toestemming verbiedt. Ook in jurisprudentie tot aan de Hoge Raad in de rechtzaak VPHuisartsen – VZVZ is aangegeven dat de toestemming voor het LSP weliswaar wetmatig was, maar dat er vanuit werd gegaan dat VZVZ de toestemming voor het LSP uiteindelijk zo specifiek mogelijk zal inrichten, conform de eisen in het wetsvoorstel (de Wabvpz). Dit kan niet eenvoudig terzijde geschoven worden;
8. Op pagina 5, onder 2 (en 4) wordt een – tamelijk bizarre - omkering van het juridische model van Wgbo gecreëerd. Volgens de auteurs moet de OTV een "uitdrukkelijke" (soms ook specifieke genoemd) toestemming voor de doorbreking van het beroepsgeheim ondersteunen. De auteurs gaan er vanuit dat het in Wgbo gecodeerde beroepsgeheim via de OTV 'specifiek' doorbroken mag worden *door een ander dan de brondossierhouder die geheimhoudingsplichtig is*. Dit is onjuist.
9. Ook de Wgbo "uitdrukkelijke toestemming" is een toestemming die, zoals de auteurs later terecht aangeven, *vooraf* gegeven moet worden aan de zorgaanbieder die het dossier beheert en die geheimhoudingsplicht heeft ten aanzien van de inhoud van het dossier.
10. Op pagina 5 onder 3 wordt – net als onder 1 hierboven – gesteld dat de OTV/Mitz zo is ingericht dat uitdrukkelijk bezwaar *in de context van Wgbo* bij veronderstelde toestemming in OTV geregistreerd moet worden (opt-out). Er wordt later genuanceerd dat dit niet geldt voor eenmalige uitwisselingen onder Wgbo, maar ook met deze nuance is de suggestie dat bezwaar in een landelijk/centraal toestemmingsregister zoals OTV geregistreerd moet worden, bizar te noemen.
11. Een uitwisseling gebaseerd op Wgbo kan – in de regel – decentraal worden geïmplementeerd, middels een push (autorisatie) mechanisme. Dit is heel belangrijk *omdat juist zo*, voor mensen die bezwaar maken tegen gecentraliseerde uitwisselingssystemen, *binnen de behandeling of met uitdrukkelijke toestemming van de patiënt daarbuiten*, toch gegevens met specifieke zorgverleners kunnen worden uitgewisseld als dat medisch noodzakelijk is. Van mensen die al (decentraal, tegen hun arts) bezwaar maken tegen een dergelijke uitwisseling, is te verwachten dat zij geenzins willen dat dit bezwaar in een landelijk/centraal systeem wordt vastgelegd.
12. Het wetsvoorstel Wegiz (dat nog niet in het parlement behandeld is) stelt overigens als eis dat voor verplichte gegevensuitwisseling, toestemming nooit verplicht mag worden. Hoe verhoudt dit zich tot de centrale registratie van persoonsgegevens voor een (breed werkende) opt-out en de m.i. benodigde toestemming voor verwerking van gegevens in de OTV?
13. Met betrekking tot hetgeen onder 7 genoemd is, valt op dat het document niet of nauwelijks gewag maakt van de mogelijkheid om *decentraal* gegevens af te schermen of bezwaar te registreren. Dit betreft zowel bezwaar tegen de mogelijke opvraging van gegevens via de "Nieuwe [mogelijkheid] dat een raadplegende zorgaanbieder eveneens toestemmingskeuzes kan verwerken (ook alleen in het bijzijn van de patiënt), waardoor gegevens direct beschikbaar gemaakt kunnen worden." (p.28) als bezwaar tegen het verwerken van toestemmingsgegevens in de OTV zelf.
14. Er wordt nergens gewag gemaakt van de gevoeligheid van loggegevens. Dit is een kwetsbaar punt die reeds rond de tijd van de wet-EPD voor het LSP is benoemd, ook richting het toenmalige CBP. Als de OTV op elk punt waar een patiënt zich bevindt, automatisch of ten gevolge van een actie van de arts bevraagd wordt, bouwt zich een logboek op met informatie over alle artsen/zorgverleners die een patiënt heeft bezocht. We hebben het hier dus over een database met zeer gevoelige gezondheidsgegevens. Voor het vastleggen van deze gegevens is een opt-in noodzakelijk.
15. Heeft een patiënt/buger de garantie dat de OTV niet bevraagd wordt, en dat loggegevens niet opgebouwd worden, *tenzij* wanneer patient uitdrukkelijk toestemming heeft gegeven voor

het verwerken van gegevens in de OTV? Hoe kan voorkomen worden dat de OTV bevestigd wordt voor elke patiënt/burger, zelfs als die decentraal bezwaar maakt, bijvoorbeeld als de OTV al bevestigd wordt op het moment dat een verwijfsbrief binnenkomt bij een ziekenhuis nog voordat patiënt gezien is? En zelfs als gesteld komt dat we gerust kunnen zijn en dat heus niet alle behandelrelaties gelogd worden: hoe kunnen wij, burgers, dit controleren in een enorm systeem bestaande uit vele (alle?) zorginformatiesystemen, waarvan de OTV kerncomponent ongetwijfeld closed-source wordt?

16. De toestemmingvereiste demonstreert dat een voorziening als OTV eigenlijk *alleen* voor Elektronisch Uitwisselingssystemen (EUS) conform de definitie van de Wabvpz kan functioneren. Het is ondenkbaar dat systemen die tot doel hebben om decentraal en zo privacyvriendelijk als technisch mogelijk is te opereren – zoals Whitebox - maar ook XISsen, in situaties waarbij niet expliciet toestemming is gegeven voor uitwisseling via een EUS, aansluiten op een systeem dat alleen al door het bevestigen van de toestemmingsregistratie, informatie over behandelcontacten en -relaties lekken naar een centrale component zonder dat hiervoor toestemming is gegeven.
17. Overigens kan de OTV in zekere zin zelf als een EUS gezien worden, in zoverre dat het systeem 'met een druk op de knop' de directe uitwisseling van gegevens kan orkestreert, ook zonder dat de partijen die gegevens kunnen opvragen vooraf bekend waren. Dit gebeurt dan nu wel onder de noemer "toestemming" maar kijkend naar de gebruikte technologie, verschilt het systeem niet noemenswaardig van een EUS, en het kent veel overeenkomsten met het oorspronkelijke L-EPD. Ten hoogste is de schaalgrootte zelfs nog groter dan dat systeem, aangezien het systeem de ambitie heeft om gegevens via *alle* beschikbare uitwisselingssystemen te kunnen ontsluiten/opvragen – waarbij een simpele toestemming op het "point of care" genoeg is om het proces van ontsluiting en opvraging van gegevens met directe toegang te laten 'rollen'.
18. Mij lijkt dat zelfs als het systeem alleen voor EUSen gebruikt wordt, voor de OTV nog steeds een *aparte* toestemming moet worden gevraagd van de toestemming voor systemen zoals het LSP en XDS. Dit omdat de doelomschrijving van de OTV en de reikwijdte van het systeem, doordat het meerdere uitwisselingssystemen waaronder ook XDS netwerken 'aanstuurt', veel breder is dan de doelstelling van het LSP. Bovendien vallen de onder OTV "sorterende" elektronische uitwisselingssystemen niet allemaal onder dezelfde verantwoordelijke.
19. Op pagina 6 onder 5 wordt expliciet gemaakt dat een OTV in staat zou moeten zijn om "bij de opvrager een toestemming te regelen". Effectief kan hiermee *het systeem van de zorgaanbieder die het dossier beheert het berhoepsgeheim doorbreken*. Op pagina 18 wordt dit expliciet gemaakt: " *is de zorgverlener die het dossier beheert [...] niet in de zorginstelling aanwezig, bijvoorbeeld in de avond / nacht weekend (ANW) of tijdens vakantie, dan worden de systemen zodanig ingericht dat de toestemmingskeuzes automatisch worden vewerrkt.*"
20. Op pagina 6 punt 5 onder a wordt uiteengezet hoe dit moet werken, namelijk dat aan de opvragende kant de toestemming gezet en gecheckt wordt, en dat dit 'cryptografisch' wordt geborgd aan de hand van *zorgaanbiederstoken, mandaattoken* en een *bsn-token*. Dit klinkt indrukwekkend, maar het komt erop neer dat de opvragende partij – de arts die de gegevens wil inzien, of diens medewerker - de genoemde informatie digitaal ondertekent, en dat op basis hiervan gegevens aan de bronkant worden ontsloten. Dit gebeurt bovendien *zonder dat de brondossierhouder eraan te pas komt*. En *zonder dat cryptografisch verifieerbaar is dat de patiënt toestemming heeft gegeven* – de omschrijving verbloemt dat de patiënt zelf geen aantoonbare toestemming heeft gegeven. Op basis van de niet-verifieerbare toestemming van patiënt maakt het systeem van de brondossierhouder de gegevens *direct beschikbaar* (p. 28).
21. Merk op dat in de huidige situatie, een toestemming alleen als rechtsgeldig wordt beschouwd als de patiënt een natte of een digitale handtekening onder een toestemmingsformulier heeft gezet, en dat de geheimhoudings-plichtige arts deze handtekening zelf evalueert/controleert alvorens de noodzakelijke gegevens te verstrekken.
22. Uit de omschrijving onder 5a blijkt overigens dat de patiënt "via Mitz [kan] controleren wie de toestemming namens hem/haar heeft gezet en gezet en wie t.b.v. een specifiek uitwisseling de toestemming heeft gecheckt". Uit dit punt en het hierboven genoemde blijkt dat dit gewoon een pull systematiek is. Het doet zeer denken aan het systeem van het Landelijk Elektronisch patiëntendossier (L-EPD), de voorganger van het LSP, waarbij de opvragende arts een vinkje moest zetten om te verklaren dat deze een behandelrelatie heeft – waarna de opvraging gaat

rollen. Het wordt nu langs de band van toestemming gespeeld, maar ook hier is de toestemming indirect, en is het effect hetzelfde – gegevens zijn met een druk op de knop opvraagbaar.

23. Volgens de auteurs is deze procedure afdoende voor de dossier om erop te vertrouwen dat de toestemming 'gecheckt is'. In het document wordt veel gezegd over vertrouwensmodellen, echter vertrouwen komt te voet en gaat te paard. En het beroepsgeheim is er juist om het vertrouwen te waarborgen. Daarmee is genoeg gezegd over de waarde van een vertrouwensmodel: dit is geen vervanging voor zichtbare, snapbare menselijke procedures en de afspraak tussen arts en patiënt dat wat in de spreekkamer besproken is, vertrouwelijk blijft.
24. Het verbaast dat de koepels, met inbegrip van de patiëntenfederatie, zo blijkt op pagina 27, al in 2019 in een convenant hebben vastgelegd dat zij het kennelijk met deze werkwijze eens zijn. Want als dit de manier is waarop het beroepsgeheim (technisch) kan worden *overruled* kunnen we het beroepsgeheim wel afschaffen.
25. Zoals vaker in het debat over elektronische zorgcommunicatie, wordt in het document stevig gebruik gemaakt van het argument dat bij spoed en in avond, nacht of weekendsituaties of in vakanties, de eigen arts niet beschikbaar is om toestemming te geven. Echter, het zijn de artsen zelf die vaak – onder meer in de debatten over het L-EPD – hebben beargumenteerd dat gegevens in spoed zelden noodzakelijk zijn. En dan nog, artsen hebben toch alle ruimte om met patiënt een risico-afweging te maken en toestemming vooraf te organiseren? patiënten kunnen dit ook steeds makkelijker zelf doen, via diverse websites – OTV kan een prima platform zijn voor patiënten om pro-actief en dus op voorhand (met betrokkenheid van de eigen arts) toestemming voor een *EUS, dus ten behoeve van beschikbaarstelling vooraf, voor spoed* te organiseren. Dit moet net als nu gaan via een bericht aan de arts, waarbij de arts persoonlijk de gegevens aanmeldt – en dus niet waarbij de toestemming geautomatiseerd in het systeem van de zorgverlener verwerkt wordt, zoals nu wordt voorgesteld. Daarnaast kan gekeken worden naar moderne middelen om wel ter plekke toestemming te geven – en dan wel digitaal verifieerbaar met een digitale handtekening zoals met IRMA, of via een autorisatiecode uitgegeven via een App of op een pasje zoals dat in Whitebox kan.
26. Merk op dat het steeds eenvoudiger wordt om systemen van artsen te laten helpen bij beslissondersteuning, bijvoorbeeld door kwetsbare patiënten te "flaggen" zodat de arts eraan herinnerd wordt om toestemming te vragen voor het geval dat. Dan kan de brondossierhouder op dat moment vragen om de gegevens ontsluiten voor dit doel, als hij of zij dit noodzakelijk acht. Dit is heel anders dan met een druk op de knop op afstand, zonder technisch aanwijsbare / onweerlegbare betrokkenheid van de patiënt, het zorgvuldig overwogen gesloten houden van een dossier te overrulen.
27. Een centraal geregistreerde algemene opt-out is iets heel anders dan een selectief bezwaar voor een individuele transactie om gegevens uit te wisselen binnen Wgbo. Ook is een generieke opt-in of opt-out niet hetzelfde als het geven of onthouden van toestemming voor het beschikbaar stellen van gegevens bij individuele zorgaanbieders. Het beroepsgeheim is deel van de relatie tussen een patiënt en een specifieke arts, in een specifieke context die geheimhouding kan vereisen. De uitgangspunten van het 'klassieke' beroepsgeheim zoals gecodeerd in Wgbo, van waaruit de vigerende toestemmingseisen zijn ontworpen, passen hier goed bij. Centraal geregistreerde 'brede' opt-ins of opt-outs die meerdere zorgverleners overstijgen, passen hier inherent slecht bij. Context verdwijnt, en de noodzaak om na te denken over het ontsluiten van gegevens en toestemming ook.
28. Los van de juridische overwegingen is er een technische overweging om geen opt-out centraal te willen registreren. Met de mogelijkheid om een opt-out te registreren, bouw je technisch ook de mogelijkheid in om de opt-out centraal te *deregistreren*. In combinatie met een opt-in/toestemmings-mogelijkheid die tot *onmiddellijke, geautomatiseerde ontsluiting van gegevens* leidt, zelfs van gegevens die onder het beroepsgeheim liggen en normaliter alleen na een expliciete beslissing en actie van een arts ontsloten mogen worden, wordt een systeem neergezet waarmee in feite, met direct effect, voor *alle* systemen die op OTV aangesloten worden, het beroepsgeheim doorbroken kan worden. Er is in het voorgestelde model geen (decentraal vastgelegde) barrière tegen een dergelijke omstandigheid. Ik noem dit met recht een goudmijn voor hackers.
29. De conclusie is simpel: verwerking van persoonsgegevens in de OTV vereist in zichzelf uitdrukkelijke toestemming, OTV betreft alleen Wabvpz Elektronische Uitwisselingsystemen /

pull systemen, en er moet zeer terughoudend worden omgegaan met onmiddelijk effectueren van toestemming – geautomatiseerd *overrulen* van het beroepsgeheim zonder dat een mens aan de bronzijde betrokken is, mag nooit.

30. Technisch detail: de inleiding op pagina 7 lijkt te suggereren dat de indieners van het voorstel, de *infrastructuur* via welke een uitwisseling plaatsvindt, willen wegabstraheren uit de toestemmingsvraag. Dit is ten onrechte: het is belangrijk voor patiënten om te weten wie (welke verantwoordelijke) welke gegevens op welke manier verwerkt. Zeggenschap betekent dat burgers kunnen aangeven met de ene infrastructuur wel, en met een andere niet gegevens uit te willen (laten) wisselen. De gebruikte infrastructuur of infrastructuren moeten dus expliciet zichtbaar blijven in de in OTV gebruikte omschrijvingen.

Nog enkele nuanceringen:

Uit het onder 2 genoemde blijkt een grote misvatting van hoe veronderstelde toestemming onder Wgbo en het beroepsgeheim werkt. Veronderstelde toestemming werkt in situaties waarin een arts – de dossierhouder en geheimhoudingsplichtige – besluit om, onder voorwaarden (noodzakelijkheid, informatievoorziening richting patiënt) gegevens uit te wisselen met een andere bij de behandeling betrokken arts, of een waarnemer. *Op dat moment* wordt patiënt geïnformeerd, en kan deze bezwaar maken. Zowel het versturen van de informatie als het registreren van bezwaar vinden dus plaats in dezelfde context, en hebben betrekking op dezelfde handeling van de dossierhouder. Bezwaar kan ter plekke gegeven worden. Voor deze vorm van bezwaar hoeft dus geen centrale bezwaarmogelijkheid georganiseerd te worden. In zoverre dat bezwaar nodig zou zijn voor een herhaalde beschikbaarstelling binnen een behandelrelatie, vindt dit plaats onder dezelfde voorwaarden en kan bezwaar ook decentraal geregistreerd worden.

Alleen als overwogen wordt om het beroepsgeheim via een externe component te doorbreken, heeft een centrale opt-out voor Wgbo communicatie een functie. Het blijkt uit alles dat dit de situatie is die OTV wil realiseren. Wat auteurs en het IB echter niet moeten vergeten, is dat zowel de wet als heel veel burgers er vanuit gaan en erop rekenen dat als geen toestemming is gegeven, gegevens *niet* opvraagbaar zijn. Zolang er geen toestemming gegeven is voor “beschikbaarstelling vooraf”, mogen gegevens niet vindbaar en niet opvraagbaar zijn – dit vereist het beroepsgeheim, vastgelegd in het wettelijke ‘contract’ tussen zorgverlener en patiënt – de Wgbo. Zo simpel is het.

Daarmee raken we ook het eerste punt dat ik noemde in deze reactie: de invoering van een OTV zoals hier voorzien, is niet een beslissing voor bestuurders in het IB om te maken, maar voor de regering en het parlement, onze volksvertegenwoordigers.. Want dat zorgverleners iets willen is niet voldoende: dit gaat de hele bevolking aan. Wie willen de gegevensuitwisseling in de Nederlandse zorg organiseren, en waarom? En wat zijn de alternatieven? Wat is handelingsperspectief voor mensen die niet dezelfde keuze willen maken dan anderen?

Pas na een zuiver publiek debat, kan een beslissing genomen over een (wettelijke) ondersteuning van een systeem zoals OTV en alternatieven.

Hopelijk heb ik u met deze kritische noten van nuttige informatie voorzien.

Bij vragen ben ik beschikbaar.

Met vriendelijke groeten,

Guido van 't Noordende

Whitebox Systems, Amsterdam
06-14792788
guido@whiteboxsystems.nl