

**31 466                      Wijziging van de Wet gebruik burgerservice-  
nummer in de zorg in verband met de elektronische informatie-  
uitwisseling in de zorg**

**Nadere Memorie van antwoord**

**Algemeen**

Met belangstelling heb ik kennis genomen van het nadere verslag van de vaste commissie voor Volksgezondheid, Welzijn en Sport met betrekking tot het voorstel van wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg. Met deze nadere memorie van antwoord beantwoord ik graag de vragen en opmerkingen die ter voorbereiding van de openbare behandeling in het verslag naar voren zijn gebracht. Daarbij houd ik de volgorde van het verslag aan.

**Kwaliteit van gegevens**

1.

Genoemde leden vragen wat het precieze doel is van het landelijk EPD. Is het vooral bedoeld voor acute noodsituaties of voor ondersteuning van de reguliere zorg? Kan de regering aangeven waaraan de medische sector nu echt behoefte heeft? Als het doel duidelijk is, is de vorm, zoals in het wetsvoorstel beschreven, dan adequaat, zo vragen deze leden de regering.

1.

In de uitgangspuntennotitie invoering landelijk EPD d.d. 28 oktober 2009 zijn door de koepelorganisaties KNMG, LHV, KNMP, NHG, KNGF, VHN, V&VN, NMT en Orde en VWS gezamenlijk de volgende uitgangspunten en het doel vastgesteld.

Het doel van elektronische gegevensuitwisseling in algemene zin is: ondersteuning van het zorgproces, het verbeteren van de kwaliteit en veiligheid van zorg, het terugbrengen van fouten, het voorkómen van dubbel onderzoek en het telkens herhalen van de historie door de patiënt. Het primaire doel vanuit de zorgverleners is dat door middel van het actief en reactief bij de behandeling betrokken zorgverleners informeren, de informatievoorziening rondom behandeling van de patiënt verbetert.

De landelijke infrastructuur voor het EPD biedt daarbij een veilige en betrouwbare communicatiestructuur voor de uitwisseling van patiëntengegevens. Hierbij is zowel pull als push berichtuitwisseling mogelijk. Pull<sup>1</sup> berichtuitwisseling heeft betrekking op acute situaties, spoedsituaties en andere omstandigheden met risico's voor discontinuïteit (zoals ewd en emd). Bij push<sup>2</sup> berichtuitwisseling gaat het om actief gerichte berichtverzending naar een andere zorgverlener. De landelijke infrastructuur is geen doel maar een middel.

---

<sup>1</sup> Pull informatie: informatie is 7x 24 uur te raadplegen door geautoriseerde behandelaars.

<sup>2</sup> Push informatie: hierbij gaat het bijvoorbeeld om het waarneemretour bericht, een labaanvraag of een verwijzing naar de specialist.

Ten aanzien van de vorm waarvoor is gekozen en die in het wetsvoorstel is beschreven, het volgende. Een infrastructuur voor elektronische gegevensuitwisseling in de zorg moet aan een aantal vereisten voldoen:

- Vanuit het oogpunt van betrouwbare en efficiënte informatie-overdracht dient uit te worden gegaan van landelijk uniforme standaarden ten aanzien van techniek, communicatie, medische inhoud en bijbehorende coderingen.
- Hoge toegangs- en beveiligingseisen (zoals UZI, Goed Beheerd Zorgsysteem, autorisatie, logging, NEN 7510, etc.).
- Informatieuitwisseling dient patiëntvolgend te zijn. Waar nodig voor een goede behandeling van de patiënt dienen medische gegevens – onafhankelijk van regiogrenzen - opvraagbaar te zijn.
- Er moet sprake zijn van een toekomstvaste infrastructuur waar doorontwikkeling op mogelijk is.

Bij het ontwerpen van de landelijke infrastructuur is in eerste instantie gekeken naar de mogelijkheid om reeds bestaande lokale en regionale netwerken aan elkaar te koppelen. De technische onmogelijkheid om de diverse netwerken aan elkaar te koppelen, de grote diversiteit aan zowel inhoudelijke als technische standaarden tussen de diverse netwerken én de beperktheid van de systemen ten aanzien van de vereiste opschaling van het toegangs- en beveiligingsniveau<sup>3</sup> heeft er toe geleid dat gekozen is voor de huidige landelijke infrastructuur voor gegevensuitwisseling in de zorg. Het Landelijk Schakelpunt (LSP) voorziet hierbij - naast het bieden van een verwijzindex (telefoonboek) die de elektronische uitwisseling van gegevens tussen de systemen van zorgaanbieder ondersteunt - in identificatie, authenticatie, autorisatie en logging.

1.

Het is voor de genoemde leden evenmin duidelijk welke medische gegevens via het landelijk EPD worden uitgewisseld. Deze onduidelijkheid bemoeilijkt volgens deze leden de discussie, omdat onduidelijk is waarover het nu precies gaat. Kan de regering deze leden op dit punt duidelijkheid verschaffen en kan zij tevens verduidelijken welke gegevens 'essentieel' zijn voor een landelijke uitwisseling? Daarover moeten ook nog landelijke afspraken worden gemaakt. Graag vernemen de leden van deze fracties in hoeverre dit onderwerp wordt betrokken bij het overleg tussen koepels, Nictiz en VWS.

2.

In het wetsvoorstel is vastgelegd dat alleen die gegevens mogen worden uitgewisseld die noodzakelijk zijn met het oog op een goede behandeling of verzorging van de cliënt (artikel 13hb, eerste lid sub a). Welke gegevens dat zijn wordt bepaald door de beroepsverenigingen. In eerste instantie is gekozen om prioriteit toe te kennen aan het landelijk beschikbaar maken van de medicatiegegevens (emd) en waarneemgegevens voor huisartsen (ewd).

---

<sup>3</sup> Zie brief OZIS d.d. 13 januari 2010 en brief van de OZIS-leveranciers d.d. 26 mei 2010 (in bijlage).

Onder emd-gegevens worden verstaan: de gegevens die een apotheek of apotheekhoudende huisartsenpraktijk heeft vastgelegd over de geneesmiddelen op recept die in de laatste 15 maanden zijn verstrekt. Deze zijn raadpleegbaar in de apotheken, huisartsenposten en het ziekenhuis.

Gegevens die behoren bij het ewd ten behoeve van huisartsen op de huisartspost zijn:

- Algemene patiëntgegevens (naam, adres, woonplaats en verzekering)
- Volledige probleemlijst
- Volledige episodelijst
- Journaal (4 maanden terug of de laatste 5 consulten)
- Alle actuele medicatie (tijdelijk, chronisch intermitterend)
- Recent gestopte (4 maanden) medicatie
- Alle (geneesmiddelen) intoleranties
- Alle contra-indicaties
- Overdrachtgegevens

De ewd-gegevens zijn alleen raadpleegbaar voor huisartsen.

Op termijn kunnen andere gegevenssoorten voor uitwisseling via de landelijke infrastructuur in aanmerking komen. Het zijn de beroepsgroepen die bepalen welke gegevens 'essentieel' zijn voor een landelijke uitwisseling.

3.

De samenvatting van het huisartsendossier bevat ook 'subjectieve' gegevens. Deze leden verzoeken de regering de vraag te beantwoorden in hoeverre een te strak keurslijf leidt tot medische fouten of het gevaar dat artsen defensief gaan registreren, waardoor de betekenis van gegevens vermindert. Acht de regering het denkbaar dat een gebrek aan context om data goed te interpreteren voor artsen reden kan zijn om onderzoek te herhalen?

3.

Door de beroepsgroep van huisartsen zelf is vastgesteld welke gegevens relevant zijn voor inzage. De optimale wijze van registratie is door het NHG beschreven in de Richtlijn Adequate Dossiervorming met het Elektronisch Medisch Dossier (ADEMD); in 2009 omgedoopt tot ADEPD: Richtlijn Adequate Dossiervorming met het Elektronisch Patiëntendossier. Het doel van de richtlijn is om voor huisartsen relevante informatie overzichtelijk in het eigen zorginformatiesysteem vast te leggen en ervoor te zorgen dat deze informatie uitwisselbaar is tussen huisartsen onderling en tussen huisartsen en andere zorgverleners. De richtlijn bevordert uniforme en gestandaardiseerde registratie. Eenmaal goed geregistreerd aan de bron, zijn de gegevens precies zoals nodig in een andere situatie beschikbaar.

Uiteraard geldt dat beschikbare informatie ondersteunend is bij de zorgverlening. Artsen zullen altijd zelf navraag doen bij de patiënt of er andere relevante zaken zijn die van belang kunnen zijn bij het interpreteren van beschikbare data.

4.

Ook vragen deze leden in hoeverre – uitgaande van het inzagerecht van de patiënt – verdere EPD-vorming de dossierverantwoordelijkheden van

de arts onder druk zal zetten. Graag vernemen zij van de regering hoe groot deze het gevaar van schaduwdoSSIers acht.

4.

Op grond van de WGBO (artikel 7:456 BW) heeft een patiënt recht op inzage in en afschrift van zijn/haar medisch dossier. Het is niet zo dat door de patiënt elektronische inzage in zijn/haar medisch dossier te geven er een nieuwe situatie wordt gecreëerd. Het bestaande inzagerecht wordt in elektronische vorm gefaciliteerd voor een beperkte set aan gegevens die uitgewisseld kunnen worden via de landelijke infrastructuur voor gegevensuitwisseling in de zorg.

De persoonlijke werkaantekeningen van de arts worden niet uitgewisseld, deze werkaantekeningen zijn daarmee ook niet inzichtelijk voor de patiënt.

De landelijke infrastructuur voor gegevensuitwisseling in de zorg zorgt voor elektronische uitwisseling van een gelimiteerde set van relevante gegevens, maar wijzigt de huidige rechten van de patiënt niet voor wat betreft het recht op inzage van de patiënt, het recht op afschrift, het recht op correctie en vooral het recht op geheimhouding. Het gevaar van schaduwdoSSIers wordt dan ook niet aanwezig geacht.

Recent onderzoek van Pluut naar de impact van patiëntinzage op het zorgproces heeft bovendien uitgewezen dat het ontsluiten van medische gegevens aan patiënten positief kan uitpakken voor zowel artsen, patiënten als de arts-patiëntrelatie<sup>4</sup>:

- de werkvreugde van artsen kan toenemen doordat zij het portaal als extra service kunnen aanbieden;
- patiëntinzage kan leiden tot verhoogde efficiëntie, bijvoorbeeld doordat patiënten beter voorbereid naar het consult komen;
- door online inzage kan de patiënttevredenheid stijgen en worden voor patiënten de kansen voor meer zelfzorg en regie vergroot.

Er zijn geen aanwijzingen gevonden voor een hogere werkbelasting van artsen of een verlaagde kwaliteit van informatie in het dossier.

5.

De richtlijn Adequate Dossiervorming met het Elektronisch Medisch Dossier (ADEMD) is in theorie een goede richtlijn, zo menen deze leden. Maar zij vernemen graag van de regering hoeveel er in de praktijk mee wordt gewerkt. Kan de regering aangeven wat er volgens haar nodig is om de implementatie van de richtlijn te bewerkstelligen, zo vragen deze leden. Ook vragen zij naar het beeld dat de regering heeft over hoe het staat met de medewerking en motivatie van huisartsen.

5.

De ADEPD-richtlijn voor communicatie is een streefnorm die door de beroepsgroep zelf is opgesteld. Tijdens de expertbijeenkomst van 9 december 2009 heeft de heer Habets (LHV) aangegeven dat in de praktijk het gebruik van ADEPD ongeveer 40% bedraagt.

---

<sup>4</sup> De impact van patiëntinzage op het zorgproces – Resultaten van een verkennend veldonderzoek, Zenc, 11 januari 2010.

In de 'Uitgangspuntennotitie invoering landelijk EPD' (zie antwoord op vraag 1), is met de LHV, VHN en het NHG vastgelegd dat als principe geldt dat vanaf het moment van de invoering van het EWD, geregistreerd wordt volgens de richtlijn van de beroepsgroep ADEPD. Ten aanzien van de al bestaande dossiers/gegevens is afgesproken dat uitgegaan wordt van de huidige kwaliteit van de gegevens en dat er voor de beroepsgroep een inspanningsverplichting geldt om geleidelijk en werkende weg een ADEPD-aanpassingsslag te maken. Jaarlijks zal monitoring plaatsvinden naar de kwaliteit van de gegevens conform de ADEPD-richtlijn. Op basis hiervan zullen eventueel maatregelen worden genomen en zal het nog op te stellen implementatie-plan ADEPD worden bijgesteld. De ADEPD-Richtlijn zal ook deel uitmaken van de regionale werkplannen.

6.

Kan de regering bevestigen dat verantwoordelijkheden bij conflicterende gegevens, uiteenlopende interpretaties en fouten in de behandeling momenteel afdoende zijn geregeld? Indien dit niet het geval is, zijn hiervoor dan wetsaanpassingen nodig, zo vragen deze leden.

6.

In de huidige praktijk worden er op regionaal niveau op diverse wijzen en op grote schaal (circa 100 miljoen berichten per jaar) medische gegevens uitgewisseld. Gezien de diversiteit van het regionale berichtenverkeer en het gebrek aan inzicht is niet altijd aan te geven welke gegevens precies zijn uitgewisseld, door wie dit wordt gedaan omdat de logging ontbreekt en of in alle gevallen wordt voldaan aan de wettelijke eisen die voortvloeien uit de WGBO en de Wbp (zie ook de antwoorden op vraag 1 en 17).

Door de wijze waarop de landelijke infrastructuur voor gegevens-uitwisseling in de zorg is opgezet, wordt aan dit gebrek aan inzicht tegemoet gekomen. Een belangrijk voordeel van de landelijke infrastructuur ten opzichte van de huidige situatie is, dat op landelijke schaal gestandaardiseerd is en dat inzichtelijk is door welke zorgverlener welke soort gegevens over een patiënt worden bijgehouden en op welk moment een zorgverlener medische gegevens heeft aangemeld, gewijzigd of opgevraagd via het LSP. Er zijn duidelijke afspraken gemaakt over de soort gegevens die kunnen worden uitgewisseld en de wijze waarop zorgverleners hun zorginformatiesystemen moeten hebben ingericht voordat zij aan kunnen sluiten op de landelijke infrastructuur (de zogenaamde Goed Beheerd Zorgsysteem (GBZ)-eisen). Daarnaast stimuleert de landelijke infrastructuur het gebruik van richtlijnen (zoals ADEPD).

7.

Ook vragen de leden van de genoemde fracties de regering of het mogelijk is om foute gegevens uit een dossier te verwijderen als er eenmaal uitwisseling heeft plaatsgevonden.

7.

Ja, dat is mogelijk. Uitgangspunt van de landelijke infrastructuur voor gegevensuitwisseling in de zorg is dat gegevens bij de bron (huisarts, apotheek) blijven. Eventuele foutieve gegevens dienen dan ook aan de bron te worden gewijzigd. In deze context is het van belang te benadrukken dat de landelijke infrastructuur niet vergelijkbaar is met het openbare

internet. Op het internet hebben miljoenen gebruikers toegang tot gegevens en kunnen deze kopiëren en opnieuw beschikbaar stellen. Bij bepaalde informatie is verwijdering dan praktisch onmogelijk vanwege de vele kopieën. Via de landelijke infrastructuur kunnen slechts geautoriseerde zorgverleners gegevens opvragen, na toestemming van de patiënt. Het opslaan van een kopie van opgevraagde gegevens is uitsluitend in zeer specifieke gevallen toegestaan. Een ongebreidelde propagatie van kopieën zoals op internet wordt daarmee voorkomen. Een patiënt is altijd in staat door opvraging van de logging na te gaan welke gegevens door wie zijn opgevraagd en kan (bij de betreffende zorgverlener) vragen om bepaalde gegevens te vernietigen. Dit is een voordeel ten opzichte van gegevens die per post (of onveilige elektronische netwerken) wordt verzonden, omdat hiervan in het algemeen geen logging bestaat.

De heer Van Boven (Nictiz) merkte tijdens de expertbijeenkomst van 9 december 2009 op dat met de komst van de landelijke infrastructuur de noodzaak om kopieën op te slaan er in het algemeen juist niet meer is, omdat je de meest actuele gegevens altijd kunt opvragen.

### **Toegang en beveiliging**

8.

Genoemde leden achten het risicobewustzijn in de zorg laag. Zij vragen de regering hoe het zorgpersoneel kan worden getraind, zodat dit afdoende kan worden aangeleerd. Ook vragen zij de regering of het voorstelbaar is dat als het risicobewustzijn verhoogd wordt de relatie tussen zorgaanbieders en patiënten verandert. Zo ja, kan dat invloed op het zorgproces hebben.

8.

Zoals de heer Van der Staaij (Atos Origin) en de heer Jacobs (Radboud Universiteit Nijmegen) reeds aangaven tijdens het Rondetafelgesprek van 22 maart 2010 is risicobewustzijn in de zorg voor verbetering vatbaar.

Invoering van een landelijke infrastructuur voor gegevensuitwisseling in de zorg en gebruik van BSN in de zorg zorgt voor een grotere bewustwording omtrent risico's omdat bijvoorbeeld zorgverleners, om gegevens te kunnen raadplegen, gebruik maken van een Unieke Zorgverlener Identificatie (UZI)-pas met bijbehorende pincode en toestemming vragen aan de patiënt. Ook wordt bijgehouden of gegevens (on)rechtmatig zijn geraadpleegd. Zoals mevrouw Borghuis (Centrale Huisartsdienst Nijmegen) als gebruiker van de landelijke infrastructuur aangaf tijdens de expertmeeting van 9 december 2009 is in de praktijk duidelijk zichtbaar dat wat de beveiliging betreft niet alleen de techniek, maar ook het gedrag enorm is vooruitgegaan.

Ook de heer Van Boven (Nictiz) gaf tijdens de expertmeeting van 9 december 2009 aan dat het grote voordeel van een landelijke EPD-infrastructuur is dat gegevensuitwisseling veel transparanter wordt dan nu het geval is: inzichtelijk wordt door wie welke gegevens worden bijgehouden en tussen welke zorgverleners gegevens worden uitgewisseld. Eén en ander zal het gedrag van mensen beïnvloeden.

Maatregelen voor het verhogen van het risicobewustzijn voor informatiebeveiliging van zorgverleners zijn beschreven in de NEN 7510 norm voor informatiebeveiliging in de zorg. Deze norm is reeds wettelijk verplicht op

grond van de Regeling gebruik BSN in de Zorg. Het betreft hier maatregelen als het opstellen van gedragscodes voor de omgang met gegevens, bewustzijnsverhogende campagnes en trainingen, continue voorlichting en toezicht op naleving. Hierbij kan tevens gedacht worden aan e-learning-programma's zoals de heer Van der Staaij (Atos Origin) tijdens het Rondetafelgesprek van 22 maart 2010 aangaf.

Een goed voorbeeld van voorlichtingsmateriaal voor risicobewustzijn dat ter beschikking is gesteld door belangenverenigingen van zorgverleners is het handboek voor NEN 7510<sup>5</sup> implementatie met daarin richtlijnen en templates voor bewustwording.

Ten aanzien van de landelijke infrastructuur voor gegevensuitwisseling in de zorg vindt voorlichting richting zorgverleners over het goed gebruik van het landelijk EPD plaats. Verhoging van het risicobewustzijn in de zorg kan alleen maar leiden tot een (nog) groter vertrouwen van patiënten in het zorgproces aangezien patiënten er dan in alle redelijkheid op kunnen vertrouwen dat er op zorgvuldige wijze met hun persoonlijke medische gegevens wordt omgegaan.

9.

De leden van de fracties van het CDA, mede namens de leden van de PvdA, SP, GroenLinks, SGP en CU, vragen de regering of het denkbaar is dat door te streven naar een L-EPD de beveiligingseisen zo hoog zullen moeten zijn, dat het zorgproces er niet meer door wordt ondersteund, maar juist door wordt bemoeilijkt. Ook vragen deze leden of het L-EPD niet leidt tot meer bureaucratie en minder tijd voor echte zorg.

9.

De landelijke infrastructuur is zo ingericht dat voldaan wordt aan de eisen die de Wet bescherming persoonsgegevens (Wbp) en de Wet geneeskundige behandelingsovereenkomst (WGBO) stellen aan veilige gegevensuitwisseling in de zorg. Bij het ontwerp en de implementatie van de landelijke infrastructuur voor gegevensuitwisseling in de zorg is steeds een balans gezocht tussen de benodigde functionaliteit voor een werkbare praktijksituatie enerzijds (zowel uit het oogpunt van gebruiksvriendelijkheid als de kosten en complexiteit van beheer) en informatiebeveiliging anderzijds.

Zoals de heer Jacobs (Radboud Universiteit Nijmegen) reeds aangaf tijdens het Rondetafelgesprek van 22 maart 2010 vergen de meer technische informatiebeveiligingsmaatregelen geen extra inspanningen van zorgverleners bij het digitaal raadplegen van medische gegevens ten opzichte van het gebruik van de huidige lokale informatiesystemen.

Wel is het zo (zoals ook bij het antwoord op vraag 8 is aangegeven) dat het gebruik van de UZI-pas met pincode die benodigd is voor het kunnen uitvragen van medische gegevens via de landelijke infrastructuur, een verandering in de manier van werken van zorgverleners vergt. Hiermee is echter de kans op onbevoegde toegang tot medische gegevens teruggedrongen waardoor de privacy van de patiënt beter is beschermd. Door een systeem waarbij gebruik wordt gemaakt van een UZI-pas en bijbehorende pincode is de kans op ongeautoriseerde toegang kleiner dan bij

---

<sup>5</sup> Zie [www.nen7510.org](http://www.nen7510.org)

het gebruik van alleen een gebruikersnaam in combinatie met een wachtwoord. Wanneer veilig gebruik van en omgang met authenticatiemiddelen als de UZI-pas onderdeel uitmaken van de dagelijkse praktijk, heeft dit geen tot weinig additionele inspanningen tot gevolg. Bevindingen ten aanzien van de werkbaarheid in de praktijk zijn gedurende een pilot geanalyseerd en geadresseerd.

10.

Ook vragen de leden van genoemde fracties of het systeem zoals het er nu ligt afdoende is beveiligd. Kan de regering duidelijk maken hoe kwetsbaar een systeem is dat via UZI-passen, waarvan er uiteindelijk 200.000 à 300.000 – of een veelvoud hiervan - in omloop zullen zijn, toegankelijk is?

10.

In de eerste plaats merk ik op dat een UZI-pas op zichzelf nog geen toegang geeft tot de landelijke infrastructuur voor gegevensuitwisseling in de zorg. Er is altijd een gekwalificeerd Goed Beheer Zorgsysteem (GBZ) van een zorgaanbieder noodzakelijk dat is aangesloten op het LSP.

Voorts bevat iedere UZI-pas een certificaat van de betreffende zorgaanbieder. Hiermee kan een zorgverlener bij het LSP bewijzen wie hij is en tot welke categorie zorgverleners hij behoort (bijvoorbeeld huisarts). Op basis hiervan stelt het LSP vast tot welke informatie/dossier(s) de betreffende zorgverlener toegang heeft. Kortom, er wordt gecheckt welke bevoegdheden de zorgaanbieder op grond van zijn zorginhoudelijke rol en functie heeft. Dit heet autorisatie. In het zogenaamde autorisatieprotocol is voor ieder type zorgverlener (beroepsbeoefenaar) aan de hand van de zogenaamde BIG-rolcodes vastgelegd welke gebruikshandelingen hij mag verrichten.

In beginsel kan de UZI-pas alleen gebruikt worden in de instelling waar de betreffende zorgverlener werkzaam is.

Een zorgverlener mag alleen medische gegevens opvragen van patiënten waarmee deze een behandelrelatie heeft. Het GBZ is zodanig ingericht dat wordt gecontroleerd of de opvragende zorgverlener eerder medische gegevens van de betreffende patiënt heeft aangemeld bij het LSP. Indien dat niet het geval is wordt gecontroleerd of de betreffende patiënt al voorkomt in de eigen patiëntenregistratie. Vervolgens wordt de zorgverlener via een pop-up scherm gevraagd of er sprake is van een behandelrelatie en of de patiënt toestemming heeft gegeven voor de raadpleging. Antwoordt de zorgverlener ja dan wordt inderdaad toegang verleend. Van dergelijke opvragingen wordt een apart logbestand bijgehouden.

De UZI-pas wordt overigens niet alleen gebruikt voor veilige uitwisseling van ewd- en emd-gegevens via de landelijke infrastructuur voor gegevensuitwisseling in de zorg, maar ook voor algemeen gebruik in de zorg, bijvoorbeeld voor veilige toegang tot het netwerk van een zorginstelling. Het aantal UZI-passen dat in omloop is, is dan ook groter dan het aantal dat daadwerkelijk gebruikt wordt voor de uitwisseling van medische gegevens via de landelijke infrastructuur.

Aan het eind van het derde kwartaal van 2010 waren 47.264 UZI-passen in gebruik. Met ongeveer de helft van de in gebruik zijnde passen kan



toegang worden verkregen tot de medische gegevens die via de landelijke infrastructuur voor gegevensuitwisseling in de zorg worden uitgewisseld.

11.

Zijn verdere technische maatregelen (bijvoorbeeld 'risk-based authentication', 'adaptive authentication', technische toegangsbeperkingen op de UZI-pas) nodig om de beveiliging te verhogen, zo vragen deze leden voorts. Indien het antwoord bevestigend luidt, welke maatregelen staan de regering dan voor ogen? Kan de regering aangeven wat zij een acceptabel niveau van beveiliging acht en tegen welke kosten.

11.

De termen 'risk-based authentication'<sup>6</sup> en 'adaptive authentication'<sup>7</sup> zijn niet exact gedefinieerd binnen het vakgebied van informatiebeveiliging, maar komen er in zijn algemeenheid op neer dat het bewijsniveau (de gebruiker dient te bewijzen dat diegene echt is wie deze beweert te zijn) af wordt gestemd op het risiconiveau van een bepaalde transactie. Factoren van invloed op dit risiconiveau kunnen het gebruikerstype of het gegevenstype voor de betreffende transactie zijn.

Voor de toegang voor zorgverleners tot de landelijke infrastructuur voor gegevensuitwisseling in de zorg is er met de UZI-pas voor zorgtoepassingen het hoogst beschikbare niveau van authenticatie gecreëerd (zie ook de beantwoording van vraag 9 en 10). De UZI-pas voldoet aan alle eisen gesteld vanuit de wet op de Elektronische Handtekening en het daaraan gerelateerde normenkader van de PKI voor de overheid. Jaarlijks vindt hierop onafhankelijke audit plaats en toezicht vanuit de OPTA<sup>8</sup>.

Er zijn momenteel geen verdere 'technische toegangsbeperkingen op de UZI-pas' noodzakelijk. Zoals eerder aangegeven, vereist het gebruik van de UZI-pas een PIN en na 3 foutieve invoerpogingen blokkeert de pas.

Zoals de heer Jacobs (Radboud Universiteit Nijmegen) reeds aangaf in het Rondetafelgesprek van 22 maart 2010 is informatiebeveiliging geen statisch gegeven. Risico's veranderen in hetzelfde tempo als de continue technologische voortgang van de techniek binnen de informatiemaatschappij (denk aan ontwikkelingen op het Internet). De bij de landelijke infrastructuur voor gegevensuitwisseling in de zorg betrokken beheerorganisaties borgen daarom een adequaat informatiebeveiligingsniveau door middel van een continu proces voor identificeren van risico's. Op deze wijze worden bedreigingen ten aanzien van de informatiebeveiliging voor de landelijke infrastructuur geïnventariseerd, geanalyseerd en geadresseerd. Indien hieruit nieuwe inzichten naar voren komen, worden aangepaste of aanvullende technische, procedurele en organisatorische maatregelen getroffen.<sup>9</sup>

---

<sup>6</sup> Zie <http://www.rsa.com/glossary/default.asp?id=1094>

<sup>7</sup> Zie <http://www.rsa.com/node.aspx?id=3018> en [http://www.rsa.com/press\\_release.aspx?id=7396](http://www.rsa.com/press_release.aspx?id=7396)

<sup>8</sup> Zie <https://www.opta.nl/nl/tsl/toezicht-door-opta/>

<sup>9</sup> Deze maatregelen worden gebaseerd op best practices en standaarden zoals VIR, NEN 7510, ISO 27001/27002 en ITIL

12.

Genoemde leden achten het systeem inbraakgevoelig. Zij stellen dat in de digitale wereld inbraak geen sporen nalaat, zodat het onopgemerkt blijft. Graag vernemen zij van de regering in hoeverre het belang van het EPD in verhouding staat tot de risico's.

12.

Binnen de landelijke infrastructuur voor gegevensuitwisseling in de zorg worden wel degelijk sporen nagelaten van misbruik van autorisaties door zorgverleners. Zoals door de heer Van Boven (Nictiz) reeds aangegeven tijdens het Rondetafelgesprek van 22 maart 2010, wordt het gebruik van het landelijk EPD 24 uur per dag bewaakt. Wanneer ongebruikelijke patronen worden gesignaleerd, kan het betreffende Goed Beheerd Zorgsysteem worden afgesloten van het LSP waarna contact wordt opgenomen met de betreffende zorgverlener om uit te zoeken wat de achterliggende oor-zaken zijn.

Om het toezicht op het gebruik van het landelijk EPD door de IGZ en het CBP zo effectief en efficiënt mogelijk te laten verlopen, worden log-gegevens op basis van gedefinieerde *use-cases* automatisch geanalyseerd en kunnen onregelmatigheden worden gedetecteerd. De loggegevens worden alleen bewaard om na het signaleren van onregelmatigheden te kunnen reconstrueren welke gegevens zijn aangemeld of opgevraagd. Op deze wijze wordt vermeend misbruik gedetecteerd. Het gaat dan bijvoorbeeld om gevallen van excessief opvragen van medische gegevens, abnormaal gebruik van mandateringen en pogingen tot opvragen van gegevens waartoe de betreffende zorgverlener niet geautoriseerd is.

13.

Genoemde leden vragen de regering de vraag te beantwoorden of en – zo ja – waarom een 'smartcard' voor de patiënt met een gekwalificeerd PKI-overheid certificaat uit veiligheidsoogpunt de voorkeur boven de huidige DigiD met face-to-facecontrole.

13.

In opdracht van VWS is een onafhankelijk onderzoek uitgevoerd door PricewaterhouseCoopers in samenwerking met de Radboud Universiteit Nijmegen en de Universiteit van Tilburg naar beschikbare identificatie- en authenticatiemiddelen waarmee - in het licht van de vereiste beveiligings-eisen - zorgconsumenten op een veilige manier toegang kunnen krijgen tot hun eigen medische gegevens. Over de uitkomsten van dit onderzoek is de Tweede Kamer op 12 december 2008 geïnformeerd.<sup>10</sup> In het advies-rapport<sup>11</sup> wordt beschreven dat het te gebruiken authenticatiemiddel het authenticatieniveau 'sterk' moet hebben zoals gedefinieerd in de NEN 7512 norm. Het middel dient te voldoen aan face-to-face controle en two factor authentication.

Zowel DigiD met face-to-face controle als een 'smartcard' voor de patiënt met een gekwalificeerd PKI-overheid certificaat voldoen aan dit niveau.

---

<sup>10</sup> MEVA/ICT-2899251

<sup>11</sup> Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD), PricewaterhouseCoopers Advisory, het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen en het Tilburg Institute for Law, Technology and Society van de Universiteit van Tilburg, 2 december 2008.

Volgens bovengenoemd onderzoek lijkt op de langere termijn de eNIK (de door Binnenlandse Zaken en Koninkrijksrelaties te ontwikkelen e-functionaliteit van de nationale identiteitskaart) het meest geschikte authenticatiemiddel te zijn. Echter, omdat de eNIK niet binnen de realisatietermijnen voor het landelijk EPD beschikbaar zou komen, is er gekozen voor de in het rapport van PwC c.s. geschetste variant voor DigiD, met sms en face-to-face controle, ontwikkeld onder de naam EPD-DigiD. Dit authenticatiemiddel komt overeen met het door de heer Van der Staaij (Atos Origin) beschreven DigiD+ mechanisme. Het voordeel van DigiD is dat het een publiek middel is dat voor meerdere doeleinden geschikt is. Het verdient dan ook de voorkeur ten opzichte van een PKIO-pas.

Zoals in de Voortgangsrapportage aan de Tweede Kamer met betrekking tot de landelijke infrastructuur voor gegevensuitwisseling in de zorg over het tweede kwartaal 2010 is aangegeven heeft GOVCERT.NL (het Computer Emergency Response Team van de Nederlandse overheid) echter een GSM en SMS-kwetsbaarheid - waar bij DigiD gebruik van wordt gemaakt – geconstateerd. Momenteel wordt onderzocht welke activiteiten moeten worden ondernomen om binnen een reële termijn en op een veilige en betrouwbare wijze elektronische toegang voor patiënten tot hun medische gegevens te realiseren. Hiertoe zijn onder andere gesprekken met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gevoerd over de e-NIK. Tevens zijn er gesprekken gaande met Logius over de implementatie van mitigerende maatregelen voor de SMS/GSM-kwetsbaarheid. Ook het uitgeven van een PKIO-pas door een marktpartij zal worden gezien. Alternatieven en mogelijke scenario's worden nu op een rij gezet om een beslissing te kunnen nemen.

14.

Is de regering van oordeel dat de wettelijke beveiligings- en toegangsnormen strenger dienen te worden (NEN 7510; mogelijke toegang door keuringsartsen, verzekeringsartsen, zorgverzekeraars of indicatieorganen), zo vragen deze leden.

14.

Zorginstellingen dienen op basis van de Regeling gebruik burgerservice-nummer in de zorg te voldoen aan de NEN 7510 norm voor informatiebeveiliging in de zorg. Toezicht op de juiste implementatie van de NEN 7510 norm door zorgverleners vindt plaats door de toezichthouders, de Inspectie voor de Gezondheidszorg (IGZ) en het College Bescherming Persoonsgegevens (CBP).

Wat de mogelijke toegang door keuringsartsen, verzekeringsartsen, zorgverzekeraars of indicatieorganen betreft: op grond van het wetsvoorstel EPD - zoals deze door de Tweede Kamer is aangenomen – is het keuringsartsen, verzekeringsartsen en zorgverzekeraars verboden toegang te krijgen tot de landelijke infrastructuur voor gegevensuitwisseling in de zorg, *behalve voor zover dit noodzakelijk is voor de uitvoering van zorgverzekeringen of zijn wettelijke taak*. Naar aanleiding van de adviezen van het CBP en de Raad van State op het concept-Besluit heb ik besloten (zoals ik u in mijn brief van 14 juni 2010 heb laten weten) de uitzonderingsbepaling te schrappen. Bij de Tweede Kamer heb ik dan ook een voorstel tot wijziging van de Kaderwet elektronische zorginformatieuitwisseling ingediend waarbij bovengenoemde uitzondering is geschrapt. Hierdoor komt er een algeheel verbod te bestaan voor zorgverzekeraars,

verzekeringsartsen, bedrijfsartsen en keuringsartsen op toegang tot het LSP en het verwerken van gegevens in het EPD.

15.

Ook vernemen deze leden graag van de regering of het toezicht op het functioneren en gebruik van het L-EPD afdoende (acceptabel en betaalbaar) is geregeld. Mocht het antwoord ontkennend luiden, dan vernemen deze leden graag van de regering hoe dit (wettelijk) kan worden geregeld.

15.

Op verzoek van het CBP heeft het Ministerie van VWS het toezichtkader in kaart gebracht. Het rapport 'Toezichtkader EPD' is u tezamen met deze Nadere Memorie van Antwoord aangeboden (zie bijlage). De maatregelen van controle en toezicht zoals opgenomen in dit Toezichtkader EPD vormen de basis voor de inzet van horizontaal toezicht door de formele toezichthouders CBP en IGZ. Hiermee is naar mijn mening een efficiënt en effectief toezichtkader ingericht.

16.

De dossierplicht van artsen verplicht tot het vaststellen en bewaren van gegevens en bevindingen van patiëntencontacten. Om deze reden en ook om bij eventuele klachten eigen handelen te kunnen staven, worden kopieën van dossiers in waarneemsituaties bewaard. Via het LSP uitgewisselde gegevens worden daarom na uitwisseling niet alleen bij de oorspronkelijke dossierbeheerder opgeslagen, maar ook bij eventuele 'ophalers'. De leden van de genoemde fracties vragen de regering of deze beschrijving feitelijk juist is en wat dit betekent voor de privacy van de patiënt.

16.

Voorop staat dat zorgverleners alleen medische gegevens kunnen opvragen onder de voorwaarde dat er een behandelrelatie is met de patiënt, de gegevens noodzakelijk zijn voor de behandeling en de patiënt toestemming voor inzage heeft gegeven. Opgevraagde gegevens moeten worden gewist, maar er zijn enkele uitzonderingen: gedurende het zorgcontact mogen gegevens 48 uur worden bewaard om te voorkomen dat ze steeds opnieuw moeten worden opgevraagd. Een zorgverlener mag de informatie als kopie overnemen in zijn dossier indien hij zijn conclusies baseert op externe informatie die hij als bewijs van zijn besluitvorming wil bewaren. In het verlengde hiervan kan de zorgverlener zijn eigen aantekeningen er aan toegevoegd hebben, of de inhoud gewijzigd hebben. In dat geval is de zorgverlener mede-auteur geworden. Medische gegevens die via de landelijke infrastructuur voor gegevensuitwisseling in de zorg zijn opgevraagd en vervolgens tijdelijk of permanent in het eigen medische dossier worden opgeslagen, moeten worden gewaarmerkt als kopie. Dit is opgenomen in het Plan van Eisen Goed Beheerd Zorgsysteem (PvE GBZ) waarin de eisen zijn vastgelegd waaraan het informatiesysteem van de zorgverlener moet voldoen. Bestaande wettelijke voorschriften (waaronder WGBO en Wbp) blijven onverkort van kracht.

17.

In de huidige situatie waarin regionale uitwisseling plaatsvindt bieden sommige Huisartsenposten waarnemende huisartsen de mogelijkheid om dossiers van patiënten bij de eigen huisarts in te zien. Graag vernemen genoemde leden of de patiënt er in die gevallen van op de hoogte is dat

zijn dossier wordt ingeladen en wordt ingezien. Ook worden zij graag geïnformeerd of het altijd alleen maar gaat om de professionele samenvatting (voorgeschiedenis, medicatie overzicht) en de laatste vijf consulten. Aanvullend vragen zij de regering of hierbij wordt geregistreerd met ADEMD, of er wordt ingelogd met UZI-passen en of de inzage achteraf is aan te tonen. Hoe vindt deze uitwisseling plaats, via het LSP of anders, zo vragen deze leden voorts. Zij verzoeken de regering voorts te verduidelijken wat de feitelijke situatie is bij de HAPpen en wat de wenselijke situatie is.

17.

Uit een inventarisatie van Nictiz blijkt dat op regionaal niveau heel veel elektronische communicatie van patiëntgegevens plaatsvindt. Ongeveer 35% van de huisartsenposten is aangesloten op een OZIS-cluster voor dienstwaarneming huisartsen.<sup>12</sup>

Gezien de diversiteit van het regionale berichtenverkeer en het gebrek aan een gestructureerd inzicht is niet aan te geven welke gegevens in de hierboven geschetste situatie precies worden uitgewisseld (of het inderdaad alleen maar gaat om de professionele samenvatting en de laatste vijf consulten) en of in alle gevallen wordt voldaan aan de wettelijke eisen omtrent privacy die voortvloeien uit de WGBO en de Wbp.

De Stichting OZIS heeft in januari 2010 aangegeven dat indien de IGZ en CBP gaan toetsen of de huidige regionale (OZIS-)communicatie voldoet aan de eisen voor landelijke communicatie, zij genoodzaakt zal zijn de bij haar aangesloten partijen te adviseren de op OZIS gebaseerde communicatie niet meer te gebruiken. Daarom onderneemt zij, tezamen met NICTIZ, diverse stappen voor de migratie naar de standaarden van de landelijke infrastructuur.

Voor de beantwoording van de vraag omtrent de registratie via ADEMD verwijs ik u naar het antwoord op vraag 5.

In de beantwoording van vraag 24 tot en met 30 ('Landelijk versus regionaal') wordt nader ingegaan op de huidige situatie omtrent informatiebeveiliging binnen de regionale uitwisseling.

18.

De leden van de fracties van het CDA, mede namens de leden van de PvdA, SP, GroenLinks, SGP en CU, vragen de regering of het mogelijk is een klantenportaal afdoende te beveiligen? Via het klantenportaal heeft de patiënt inzage in zijn dossier, de loggegevens en de verwijzingsgegevens.

18.

Ja, dat is mogelijk. Wel is het te gebruiken toegangsmiddel een aandachtspunt. Zoals in het antwoord op vraag 13 is aangegeven, is door GOVCERT.NL een GSM en SMS-kwetsbaarheid geconstateerd (waar bij EPD-DigiD gebruik van wordt gemaakt). Totdat er meer duidelijkheid bestaat over mogelijke mitigerende maatregelen voor de door GOVCERT.nl geconstateerde GSM en SMS kwetsbaarheid – is er vooralsnog een pas op de plaats gemaakt met de ontwikkeling van die

---

<sup>12</sup> E-Health monitor 2010 Volumes, Nictiz, 1-6-2010.

onderdelen van het Klantenloket die van de beveiligingskwetsbaarheid in SMS afhankelijk zijn, waaronder een patiëntenportaal.

De uitgevoerde risicoanalyse met de door PWC en de Radboud Universiteit Nijmegen geschetste oplossingen zijn nader bestudeerd. Momenteel wordt onderzocht welke activiteiten moeten worden ondernomen om binnen een reële termijn en op een veilige en betrouwbare wijze elektronische toegang voor patiënten tot hun medische gegevens te realiseren. Hiertoe zijn onder andere gesprekken met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gevoerd over de e-NIK. Tevens zijn er gesprekken gaande met Logius over de implementatie van mitigerende maatregelen voor de SMS/GSM-kwetsbaarheid. Ook het uitgeven van een PKIO-pas door een marktpartij zal worden bezien. Alternatieven en mogelijke scenario's worden nu op een rij gezet om een beslissing te kunnen nemen.

### **Positie en rechten patiënt**

19.

De leden van de fracties van het CDA, mede namens de leden van de PvdA, SP, GroenLinks, SGP en CU, vragen de regering of zij van oordeel is dat de informatievoorziening aan de burgers kan worden verbeterd en - zo ja - op welke punten. Deze leden menen namelijk te kunnen vaststellen dat het draagvlak slinkt en dat het als storend wordt ervaren dat de invoering van het EPD doorgaat terwijl het wetsvoorstel nog niet is afgehandeld.

19.

Duidelijke informatievoorziening aan zorgconsumenten én zorgverleners is een voortdurend punt van aandacht.

In reactie op de moties die op 6 juli jl. door uw Kamer zijn aangenomen, heb ik u in mijn brief van 5 oktober 2010 laten weten dat er in ieder geval volwaardige en goede communicatie komt als de wet in uw Kamer aan de orde is geweest. Met de huidige implementatie van de landelijke infrastructuur wordt niet vooruitgelopen op nog aan te nemen wetgeving aangezien er geen aparte wettelijke basis nodig is voor de inrichting van het LSP en de aansluiting van zorgaanbieders op het LSP momenteel op vrijwillige basis plaatsvindt. Ook hierover dient vanzelfsprekend duidelijk te worden gecommuniceerd, opdat er geen misverstanden kunnen ontstaan.

In mijn brief van 5 oktober 2010 heb ik tevens aangegeven dat ik samen met Nictiz in gesprek ben met de regionale samenwerkingsverbanden over de mogelijke afstemming tussen regionale en landelijke systemen op het terrein van voorlichting en communicatie richting de burger, toegang patiënt en registratie bezwaar.

Mede in het licht van de motie van het lid Dupuis c.s. acht ik het van groot belang dat burgers volwaardige en duidelijke informatie krijgen over de ontwikkelingen ten aanzien van de regionale en landelijke elektronische informatie-uitwisseling in de zorg opdat zij een weloverwogen keuze kunnen maken: uitwisseling van medische gegevens via de landelijke infrastructuur, eventueel met regionale begrenzing door de patiënt, ofwel uitwisseling via bestaande regionale systemen.

20.

Afscherming van gegevens door de patiënt staat op gespannen voet met de verantwoordelijkheid van artsen voor volledige dossiervorming, zo stellen deze leden. Is het (juridisch) zo te regelen dat patiënten dit recht krijgen, zonder dat artsen hierdoor problemen krijgen, zo vragen zij de regering. Ook vragen genoemde leden of het mogelijk én nodig is om in het EPD aan te geven dat bepaalde gegevens zijn afgeschermd.

20.

Het feit dat patiënten het recht krijgen om bepaalde gegevens af te schermen, ontslaat artsen niet van hun reeds bestaande dossierplicht en onderzoekspllicht (zie het antwoord op de vragen 4 en 6 hierboven). Het recht op afscherming van gegevens geeft patiënten de mogelijkheid om ervoor te zorgen dat bepaalde gegevens niet worden uitgewisseld. Dit laat onverlet dat zorgaanbieders bij wie zij in behandeling zijn de verplichting hebben om een dossier *in te richten* ten behoeve van een goede hulpverlening aan de patiënt. Wel kunnen op verzoek van de patiënt bepaalde gegevens uit het medisch dossier worden weggelaten. De patiënt zelf heeft overigens een inlichtingen- en medewerkingsplicht (artikel 7:452 BW): hij/zij moet de zorgverlener naar beste weten de inlichtingen en medewerking geven die redelijkerwijs nodig is voor de behandeling van de patiënt.

Wat de "melding onvolledig EPD" betreft: conform de wens van de Tweede Kamer was in het voorstel tot wijziging van de Kaderwet elektronische zorginformatieuitwisseling een bepaling opgenomen waarin de zorgverlener werd verplicht om – indien hij op verzoek van de patiënt gegevens uit het dossier had verwijderd – hiervan melding te maken in het EPD en aan te geven dat het dossier van die patiënt onvolledig is. Naar aanleiding van het advies van het CBP en de Raad van State is er echter voor gekozen om deze bepaling uit het wetsvoorstel (zoals dit op 25 oktober bij de Tweede Kamer is ingediend) te schrappen. Gekozen is om het belang van de patiënt die bepaalde gegevens uit zijn EPD heeft laten verwijderen te laten prevaleren boven het belang van de opvragende zorgaanbieder om te weten of er al dan niet gegevens uit het dossier zijn verwijderd. Ook hier gaat het overigens om een recht dat de patiënt al heeft op grond van de WGBO.

21.

De leden van genoemde fracties vragen de regering hen te informeren over hoever het ministerie van VWS is gevorderd met de realisering van het inzagerecht en de mogelijkheid om daar een bepaalde mate van regie op te voeren, inclusief het herstel van fouten, zonder dat dit traceerbaar is. Ook vernemen zij graag van de regering hoe zij de gevolgen inschat voor het draagvlak bij eventuele vertraging. Tevens verzoeken zij de regering te verduidelijken hoe snel het inzagerecht te realiseren zal zijn. Voorts vernemen zij graag van de regering of het inzagerecht überhaupt te realiseren is op de manier zoals de Tweede Kamer verlangde.

21.

Het is voor patiënten nu reeds mogelijk om via het door VWS ingerichte Klantenloket inzage te krijgen in wie hun gegevens hebben aangemeld en wie hun gegevens via de landelijke infrastructuur voor gegevensuitwisseling in de zorg hebben opgevraagd. Tot op heden (peildatum 1 oktober 2010) hebben 1772 burgers een verzoek tot inzage ingediend.

Via de vernieuwde website voor zorgconsumenten (InfoEPD.nl) kunnen burgers, naast een verzoek voor bezwaar en inzage op papier, ook elektronisch een verzoek voor bezwaar en inzage indienen middels elektronische formulieren die te benaderen zijn met Digid basis (gebruikersnaam en wachtwoord). Inzage in de medische dossiers zelf kan via de zorgverlener worden verkregen.

Onder regie van VWS hebben Nictiz, CIBG, Logius en TNT Post gewerkt aan het op een veilige en gebruiksvriendelijke manier mogelijk maken van elektronische toegang voor de patiënt tot zijn/haar medische gegevens. Te dien einde is het patiëntenportaal ontwikkeld. Echter, zoals reeds bij de beantwoording van vraag 13 en 18 is aangegeven, is er met het oog op de geconstateerde GSM-kwetsbaarheid van het toegangsmiddel EPD-DigiD vooralsnog een pas op de plaats gemaakt.

22.

Is de regering van mening dat het eigen beheer van medische gegevens door de patiënt de voorkeur verdient, zo vragen deze leden. Deze leden denken hierbij aan een elektronische informatiedrager ('Gesundheitskarte', 'stick') die patiënten bij zich hebben of opslag van (versleutelde) gegevens op internet (digitaal kluisje), waarbij de patiënt beslist wie toegang krijgt tot de gegevens. Bij deze vormen heeft de patiënt een meer centrale rol en het is minder fraudegevoelig en privacy-beschadigend, zo menen deze leden. Kan de regering deze leden verduidelijken in hoeverre de genoemde mogelijkheden verenigbaar zijn met de huidige plannen voor het landelijk EPD, of dat ze daarvoor een alternatief vormen?

22.

De heer Nouwt (KNMG) merkte tijdens het Rondetafelgesprek van 22 maart 2010 op dat, in het licht van de wettelijke dossierplicht van artsen in het belang van een goede zorgverlening, het eigen beheer van medische gegevens door patiënten niet de voorkeur verdient. Maar dat persoonlijke gezondheidsdossiers wél een nuttige aanvulling kunnen zijn op de dossiers van de arts.

Ook de heer Van Boven (Nictiz) gaf tijdens het Rondetafelgesprek van 22 maart 2010 aan dat persoonlijke gezondheidsdossiers (personal health records) het dossier van de arts niet kunnen vervangen. Informatie zal nooit uitsluitend op een draagbaar medium staan. Personal health records kunnen wel bijdragen aan een betere informatiepositie van de patiënt en kunnen met name chronische patiënten met slimme ondersteunende computerprogramma's meer verantwoordelijkheid nemen voor hun eigen gezondheid. Ook vanwege het toenemend beslag dat chronische patiënten op de zorg leggen, is die ontwikkeling van groot belang.

Het beheer van medische gegevens door de patiënt is volgens de heer Van Bommel (Erasmus MC) ook niet in lijn met de centrale rol die de huisarts in de Nederlandse gezondheidszorg vervult. Daarnaast zijn er volgens hem omstandigheden waarbij eigen beheer van medische gegevens door patiënten niet goed mogelijk is. Bijvoorbeeld in geval van hele jonge patiënten of patiënten die ouder worden en die, los van vele kwalen en ziekten, mentale problemen krijgen.

Eigen beheer van medische gegevens door de patiënt moet dus niet als alternatief worden gezien van het landelijk EPD, maar als aanvulling.



In Duitsland heeft men overigens gekozen voor een systeem waarbij patiënten eigenaar zijn van hun EPD en waarbij toegang tot de betreffende infrastructuur enkel kan worden verkregen met behulp van een zogenaamde Gesundheitskarte die de patiënt onder zich heeft. Duitse artsen hebben echter kritiek geleverd op het Duitse systeem. Bij proeven is namelijk gebleken dat maar liefst 70% van de patiënten hun bijbehorende pincode kwijt was of was vergeten. Ook werd de vrees geuit dat de kaart zoek zou raken.

23.

Waar kunnen patiënten hun recht halen als er ergens wat fout gaat, zo vragen de leden van genoemde fracties. Zij vragen de regering voorts of een meldingsplicht nodig is bij identiteitsfraude, diefstal, inbraak of verlies van gegevens.

23.

VWS heeft een klantenloket ingericht waar patiënten terecht kunnen met een klacht jegens een zorgverlener of instelling inzake misbruik van gegevens van henzelf of van iemand anders. Indien het een melding van vermeend misbruik betreft, wordt de melding onderzocht door CIBG (SBV-Z)/Nictiz en - indien een redelijk vermoeden van misbruik bestaat - vervolgens doorgestuurd naar het CBP/IGZ.

Daarnaast kunnen patiënten terecht bij reeds bestaande instanties, te weten de klachtencommissies, de tuchtcolleges, de civiele rechter, de strafrechter, en (rechtstreeks) de Inspectie voor de Gezondheidszorg en het CBP. Richting patiënten zal het klantenloket – waar nodig – een assisterende rol vervullen ten aanzien van klachten die gericht zijn aan genoemde instanties.

Naast klachten van patiënten zelf wordt er binnen CIBG en Nictiz op technisch/operationeel niveau toezicht uitgeoefend om onrechtmatigheden ten aanzien van elektronische informatieuitwisseling in de zorg op te kunnen sporen. Zo heeft Nictiz – als beheerder van het Landelijk Schakelpunt (LSP) – een functie bij het reguleren en controleren van de toegang tot patiëntgegevens. Door middel van logging wordt binnen het LSP geregistreerd welke gegevens zijn geraadpleegd en of dit op rechtmatige wijze heeft plaatsgevonden. Zo kunnen gevallen van vermeend misbruik worden gesignaleerd.

Zoals eerder aangegeven, is toegang tot het LSP alleen te verkrijgen met een geldige UZI-pas en bijbehorende pin-code. Bij het UZI-register – dat ressorteert onder het CIBG – dient een zorgverlener zo spoedig mogelijk melding te doen van verlies of diefstal van de UZI-pas, of bij het bekend worden van de PIN-code of PUK-code opdat de pas kan worden ingetrokken. Intrekken van de pas kan 24 uur per dag en zeven dagen per week.

### **Landelijk versus regionaal**

24.

De leden van de fracties van het CDA, mede namens de leden van de PvdA, SP, GroenLinks, SGP en CU, vragen de regering of zij van oordeel is dat het voor de vorm en standaardisering uitmaakt of er verplicht een landelijk EPD wordt gebouwd, dan wel of het vrijwillig vanuit regionale netwerken wordt vormgegeven. Voorts vragen zij de regering of het

verplichtende karakter van het wetsvoorstel de regionale ontwikkeling ook in de weg staat.

24.

De implementatie van de landelijke infrastructuur is in beperkte zin centraal vormgegeven met bouw van het landelijk schakelpunt inclusief de mechanismen voor identificatie, authenticatie, autorisatie en logging. De implementatie, oftewel de aansluiting van de zorgverleners op de infrastructuur volgens uniform gestelde standaarden, vindt vanuit regionaal perspectief plaats. Verschillende regionale samenwerkingsverbanden werken met Nictiz samen en dragen bij aan de implementatie van de zorgverleners vanuit hun regio. Op dit moment vindt de aansluiting vrijwillig plaats. Op peildatum aansluiting 12 november zijn er inmiddels 1.531 zorgverleners aangesloten (23%). Op basis van de aanmeldingen voor het aansluitsubsidie LSP is de verwachting dat komende voorjaar circa 5000 (75%) zorgverleners zich vrijwillig zullen aansluiten op het LSP.

De verplichting jegens zorgaanbieders zoals opgenomen in het wetsvoorstel strekt er uiteindelijk toe om er voor te zorgen dat niet de zorgaanbieders, maar de burger zelf kan kiezen voor het wel of niet hebben van een epd. De verplichting borgt dat een burger – indien zijn/haar zorgverlener niet vrijwillig aansluit – over een epd kan beschikken. Zoals eerder aangegeven is met de beroepsgroepen afgesproken dat een verplichting pas aan de orde is als een substantieel deel (75%) van de betreffende zorgverleners is aangesloten. De inwerkingtreding van een wettelijke verplichting is daarmee een sluitstuk van een implementatie.

Het verplichtende karakter staat regionale ontwikkeling niet in de weg. Regionale uitwisseling en de landelijke uitwisseling van gegevens dienen als aanvullend op elkaar te worden beschouwd en niet als tegenstrijdig. In de regio's wordt aangegeven dat een verplichtend karakter zelfs ondersteunend kan zijn in de regionale ontwikkeling. Zo zal het de bereidheid van ICT-leveranciers voor noodzakelijke investeringen in de geleverde ICT-producten verhogen en daarmee een versnelde noodzakelijke innovatie hiervan bevorderen.

25.

Kan de regering voorts precies aangeven wat nog het verschil is als regionale EPD's de basis gaan vormen voor het L-EPD, maar deze via het landelijk schakelpunt (LSP) aan elkaar worden gekoppeld, zo vragen deze leden. Ook vernemen deze leden graag of dit, gezien de veelheid van systemen, mogelijk is. Kan de regering toelichten in hoeverre het L-EPD en de regionale EPD's aanvullend kunnen zijn?

25.

Zoals reeds bij het antwoord op vraag 1 is aangegeven, is het technisch onmogelijk om de diverse regionale netwerken aan elkaar te koppelen. Er is sprake van een grote diversiteit aan zowel inhoudelijke als technische standaarden tussen de diverse netwerken én van beperktheid van systemen ten aanzien van de vereiste opschaling van het toegangs- en beveiligingsniveau.<sup>13</sup>

---

<sup>13</sup> Zie brief OZIS d.d. 13 januari 2010 en brief van de OZIS-leveranciers d.d. 26 mei 2010 (in bijlage).

Zoals de heer Habets (LHV) aan heeft gegeven tijdens het Rondetafelgesprek van 22 maart 2010 is er nog een weg te gaan om de bestaande regionale structuren te laten voldoen aan de normen waaraan de landelijke infrastructuur voldoet. De verschillende regio's bevinden zich in zeer uiteenlopende fasen van ontwikkeling. Regionale netwerken en de landelijke infrastructuur (LSP) kunnen samenwerken om de beoogde doelen van veilige elektronische informatieuitwisseling te behalen. In de, bij de beantwoording van vraag 1 reeds aangehaalde, 'Uitgangspuntennotitie' is dit door diverse koepelorganisaties eveneens gemeld. Ook is hierin aangegeven dat regionale gegevensuitwisseling gebruik kan maken van de landelijke infrastructuur. Regionale gegevensuitwisseling en uitwisseling via de landelijke infrastructuur kunnen in die zin aanvullend op elkaar zijn doordat de gegevensuitwisseling parallel en geïntegreerd kan verlopen. De gebruiker (arts/apotheker) ziet in zijn zorginformatiesysteem binnen dezelfde applicatie uit welke infrastructuur de gegevens afkomstig zijn.

26.

Regionale systemen vervullen binnen de huidige zorgpraktijk een belangrijke rol bij de uitwisseling van medische gegevens. Er is echter kritiek op het niveau van beveiliging. Kan een landelijk systeem de beveiliging van regionale systemen verhogen, zo vragen de leden van genoemde fracties de regering.

26.

De bedoeling is dat ook regionale systemen worden opgeschaald conform de landelijke beveiligings- en toelatingseisen opdat ook alle regionale systemen kunnen voldoen aan de wettelijke eisen (WGBO en Wbp). Zoals door de Stichting OZIS is aangegeven, worden stappen gezet voor de migratie naar de standaarden van de landelijke infrastructuur.

Bij opschaling conform de landelijke standaarden gaat het overigens niet alleen om technische vereisten, maar ook om te nemen maatregelen op organisatorisch niveau ten behoeve van het beheer van het maken/registeren van bezwaar, logging, informatievoorziening aan burgers, etc. op regionaal niveau. Regionale samenwerkingsverbanden kunnen hier een waardevolle rol bij vervullen.

27.

Ook verzoeken deze leden de regering te specificeren waaraan regionale systemen moeten voldoen. Komt er een keurmerk voor regionale systemen en wie ziet toe op de uitvoering?

27.

Zoals tijdens het Rondetafelgesprek van 22 maart 2010 door de heer Nouwt (KNMG) en mevrouw Beuving (CBP) is aangegeven, komen de eisen voort uit bestaande wet- en regelgeving. Zo heeft het CBP in haar persbericht van 28 april 2008 aangegeven dat 'De lijn van het CBP is gebaseerd op bestaande wetgeving, namelijk de Wet op de geneeskundige behandelingsovereenkomst (WGBO) en de Wet bescherming persoonsgegevens (Wbp). Op regionaal niveau bestaan reeds initiatieven met elektronische patiëntendossiers. Het CBP wijst er op dat ook dergelijke initiatieven aan de WGBO en de Wbp moeten voldoen'. Daarnaast heeft de Tweede Kamer bij amendement van de leden Omtzigt en Vermeij (Kamerstukken II, 2008/09, 31 466, nr. 48) in het wets-

voorstel een bepaling opgenomen op grond waarvan bij algemene maatregel van bestuur regels worden gesteld over de verwerking van gegevens in regionale netwerken.

Deze regels moeten gelet op het amendement in ieder geval betrekking hebben op de personen die bevoegd zijn tot het verwerken van gegevens in deze netwerken, de rechten van de cliënt en de beveiliging van deze netwerken. Dit amendement maakt het mogelijk om in de wijziging van het Besluit gebruik burgerservicenummer in de zorg specifieke regels op te nemen waaraan de regionale netwerken moeten voldoen. Deze regels zullen worden gebaseerd op de eisen waar deze netwerken ook nu reeds aan moeten voldoen ingevolge de WGBO en de Wbp (eisen met betrekking tot kwaliteit, veiligheid en privacy).

Meer specifiek zullen aan regionale netwerken de volgende eisen worden gesteld:

- Net als bij de landelijke infrastructuur voor gegevensuitwisseling in de zorg moeten cliënten geïnformeerd worden over de verwerking van hun gegevens, zodat zij hun rechten kunnen uitoefenen in de vorm van maken van bezwaar daartegen of het verzoeken om inzage in die gegevens.
- Daarnaast dient, net als bij gegevensuitwisseling via de landelijke infrastructuur, voor de verstrekking van gegevens uit een regionaal dossier door de ene zorgaanbieder aan een andere zorgaanbieder de toestemming van de cliënt te worden gevraagd. In situaties waarin het vragen van toestemming niet mogelijk is, bijvoorbeeld omdat de patiënt buiten bewustzijn is, maar het voor de cliënt wel noodzakelijk is dat informatie wordt geraadpleegd, zal deze toestemming verondersteld kunnen worden.
- Net als bij de landelijke infrastructuur wordt een gebruiksregistratie verplicht gesteld. Hiermee moet elke uitwisseling van gegevens via een regionaal netwerk geregistreerd (logging) worden in een gebruiksregistratie. Hierin wordt vastgelegd wie, wanneer toegang heeft gezocht tot de gegevens van welke cliënt.
- De beveiliging van persoonsgegevens dient, overeenkomstig artikel 13 van de Wet bescherming persoonsgegevens, te bestaan uit passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen moeten garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, dat er sprake is van een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
- Alleen hulpverleners die betrokken zijn bij de behandeling van een cliënt zullen gegevens mogen inzien over de cliënt. Er dient, net als bij de landelijke infrastructuur, sprake te zijn van een behandelrelatie tussen de cliënt en de beroepsbeoefenaar die de gegevens verwerkt.

Bij aansluiting op het LSP stelt Nictiz eisen, waarop zij ook toeziet (zie ook antwoord op vraag 26).

Als er geen sprake is van aansluiting op het LSP, is de betreffende zorgaanbieder zelf verantwoordelijk voor het voldoen aan bovengestelde eisen. Naleving wordt gecontroleerd door onder andere het CBP.

28.

De leden van genoemde fracties stellen vast dat regionaal al veel meer wordt uitgewisseld dan het wetsvoorstel op dit moment beoogt. Betekent dit dat de regionale uitwisseling bij de landelijke invoering moet worden beperkt, zo vragen deze leden, en wat zijn hiervan de gevolgen.

28.

Regionale uitwisseling hoeft niet ingeperkt te worden door de invoering van de landelijke infrastructuur. Zoals eerder is aangegeven, is landelijke en regionale gegevensuitwisseling aanvullend op elkaar.

29.

Genoemde leden vragen de regering voorts te verduidelijken hoe snel het landelijk EPD moet (of kan) worden ingevoerd en met welke vormen van evaluatie en (onafhankelijk) onderzoek dat gepaard dient te gaan. Kan de regering tevens aangeven welke technische en logistieke problemen overwonnen moeten worden.

29.

Op dit moment vindt aansluiting van huisartsen, apotheken, huisartsenposten en ziekenhuizen op de landelijke infrastructuur plaats op basis van vrijwilligheid. Op peildatum 5 november 2010 zijn 1519 zorgaanbieders aangesloten op het LSP. In totaal hebben ruim 5.000 zorgverleners subsidie voor aansluiting aangevraagd. De verwachting is dan ook dat op basis van deze aanvragen komend voorjaar circa 75% van de zorgverleners binnen de EPD-doelgroep zal zijn aangesloten op de landelijke infrastructuur voor gegevensuitwisseling in de zorg.

Diverse evaluaties en onderzoeken zijn en worden in de toekomst uitgevoerd. Zo zal op de veiligheid en betrouwbaarheid van de landelijke infrastructuur voor gegevensuitwisseling in de zorg periodieke toetsing plaatsvinden door middel van audits en testen. Daarbij wordt niet alleen gekeken naar het centrale deel zoals het LSP, maar ook naar alle afzonderlijke schakels in de keten. De daadwerkelijke implementatie wordt gemonitord door Nictiz en CIBG.

Voor de invoering van de eerste onderdelen van de landelijk EPD (huisartswaarneemgegevens en medicatiegegevens) zijn op dit moment geen technische belemmeringen aan de orde die de invoering van het emd en ewd belemmeren. Op dit moment is nog een klein deel van de ICT-leveranciers zich aan het kwalificeren. Logistieke zaken hieromtrent zijn vastgelegd in een werkplan tussen Nictiz en de ICT-leveranciers.

30.

Kan de regering aan deze leden aangeven wat de noodzaak en toegevoegde waarde is van het L-EPD, uitgaande van het regionale EPD volgens landelijke richtlijnen. Is de regering van oordeel dat de regionale optie goedkoper en minder risicovol is? Welke bezwaren en risico's zijn verbonden aan landelijke koppeling, zo vragen deze leden ten slotte.

30.

Er zijn er geen vast omliggende landelijk dekkende bestuurlijke zorgregio's waarbinnen een patiënt zich als in een ijzeren regio beweegt. Binnen enkele regio's dekt de huidige regioafbakening deels de patiëntbewegingen. In veel regio's is dit echter niet het geval. Zo is in de regio

Amsterdam 50% van de patiëntenbeweging van buiten de regio, waarbij communicatie veelal via telefoon en fax plaatsvindt.

Op zichzelf staande, niet-gekoppelde regionale EPD's zullen de gewenste communicatiebehoeften daarmee niet kunnen ondersteunen.

De onmogelijkheid van het koppelen van de bestaande regionale EPD's is reeds toegelicht in het antwoord op vraag 1 en 25.

De landelijke infrastructuur biedt door de schaal kostenvoordelen ten opzichte van regionale infrastructuren. Het werken via regionale infrastructuren betekent dat per regio een initiële investering moet worden gedaan voor de ontwikkeling van een infrastructuur die voldoet aan de wettelijke richtlijnen en deze moet worden geïmplementeerd. De kosten hiervoor zullen in zekere mate overeenkomen met de kosten die zijn gemaakt voor de ontwikkeling van de landelijke infrastructuur. Vervolgens moet per regionale infrastructuur een organisatie worden ingericht die verantwoordelijk is voor professioneel beheer en onderhoud en aanspreekpunt is voor de patiënten in de regio voor het verstrekken van informatie en het invullen van de patiëntrechten als bezwaar en inzage. Uitgaande van ruim 30 regio's die nodig zullen zijn om landelijke dekking te realiseren, betekent dit dat kosten in 30-voud zullen worden gemaakt.

Los van de kosten voor de regio's zit hier verder een nadeel aan vast voor de patiënt. Deze heeft namelijk geen mogelijkheid om op één plaats bezwaar te maken en zijn rechten uit te oefenen op het vlak van inzage.

Om toch aan een eventuele voorkeur van patiënten voor regionale uitwisseling van hun medische gegevens tegemoet te komen, is door Nictiz de mogelijkheid onderzocht om op verzoek van de patiënt regionale begrenzing van de informatie-uitwisseling binnen de landelijke infrastructuur aan te brengen. In de 'Impactanalyse regionale begrenzing' – die u tezamen met deze Nadere Memorie van Antwoord is aangeboden (zie bijlage) – is aangegeven op welke wijze tegemoet kan worden gekomen aan mensen die de toegang tot de uitwisselbare gegevens op voorhand willen beperken tot een kleine kring van zorgverleners. Uit de impactanalyse komt naar voren dat inperking tot een regionale context in principe mogelijk is. Het probleem is echter dat er geen sprake is van bestaande vastomlijnde bestuurlijke zorgregio's. Wel is er sprake van een groot scala aan samenwerkingsverbanden die in een regionale context werken, maar deze diverse verbanden overlappen elkaar vaak. Voorts geldt dat burgers - indien men inperking wenst - naar alle waarschijnlijkheid deze beperking 'op maat' willen kunnen aangeven. Daarom stelt Nictiz voor om de begrenzing zo in te richten opdat een burger zelf een selectie van zorgverleners kan aangeven waartoe de uitwisseling van de gegevens via de landelijke infrastructuur beperkt kan worden. Op die wijze kan men er bijvoorbeeld voor kiezen om alleen de eigen huisarts, de eigen apotheek en medisch specialist toegang te geven tot de gegevens en toegang van alle overige zorgverleners op voorhand te blokkeren.

Deze optie is op korte termijn te realiseren. Ik heb Nictiz dan ook gevraagd de begrenzing van de toegang van zorgverleners op deze wijze te implementeren.