Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2008–2009

31 466 Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg

Nr. 50 **BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 februari 2009

Op 18 februari heeft de tweede termijn van de wetsbehandeling *Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg* (hierna: wetsvoorstel EPD) plaatsgevonden. Met deze brief beantwoord ik op uw verzoek de nog openstaande vragen schriftelijk voorafgaand aan de stemming over het wetsvoorstel.

Toegang patiënt

Mevrouw Gerkens heeft gevraagd of de burger die thuis zijn gegevens wil inzien straks moet beschikken over een PKI-certificaat en hoe ik dit denk uit te voeren. Zoals ik in mijn brief van 30 januari heb aangegeven stelt Nictiz dat voor de toegang van de patiënt tot het landelijk schakelpunt via het openbare internet, gebruik moet worden gemaakt van een versleutelde verbinding. Dit is in lijn met het advies dat PWC heeft uitgebracht in het kader van het project Toegang Patiënt. De versleutelde verbinding tussen de patiënt met de computer thuis wordt opgezet volgens een SSL-sessie met eenzijdige authenticatie-controle (namelijk de controle dat de patiënt de juiste website bezoekt, conform de campagne 3 x kloppen). Hierbij wordt een certificaat meegestuurd naar de computer van de burger. Dit gaat geheel automatisch en veelal onzichtbaar voor de gebruiker. Dit sluit dus aan bij mijn opmerking in de tweede termijn dat ik er van uit ging dat dit voor de burger geen extra last zou zijn. Dit aspect van de toegang patiënt zal overigens ook worden beproefd in de voorziene pilots.

Mevrouw Koşer Kaya constateerde terecht dat ik heb toegezegd dat de verplichting tot aansluiting op het EPD pas van kracht wordt op het moment dat de toegang van de patiënt is gerealiseerd. Zij vroeg of in de tussentijd de landelijke invoering wordt gecontinueerd. Dat is juist. De landelijke invoering zal op basis van vrijwilligheid worden voortgezet. Uiteraard gebeurt dit met grote zorgvuldigheid, waarbij het proces van

KST128191
0809tkkst31466-50
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2009

landelijke uitrol continu zal worden gemonitord. Door in de tussentijd de landelijke invoering te continueren wordt tegelijkertijd voldoende massa gecreëerd voor de grootschalige hackerstest waar mevrouw Sap om heeft gevraagd. Een ander implementatiescenario, bijvoorbeeld een «big-bang»-scenario, is in mijn ogen ondenkbaar. Natuurlijk zal de landelijke invoering in alle openheid gebeuren en niet «achter de schermen», zoals mevrouw Koşer Kaya suggereerde. In de voortgangsrapportages wordt u hiervan op de hoogte gehouden.

UZI-pas

Naar aanleiding van de vragen van mevrouw Sap en mevrouw Agema naar geruchten of de veiligheid van de UZI-pas in het geding zou zijn, wil ik ingaan op de waarborgen voor een veilig gebruik van het EPD en de UZI-pas.

Het landelijke systeem kent hoge beveiligingseisen. Deze eisen zijn gericht op de technische infrastructuur en op het gebruik van het EPD, de feitelijke gegevens-uitwisseling. Het gebruik van het EPD is omgeven met waarborgen, die zowel voorwaarde vormen voor het gebruik, werking hebben tijdens het gebruik van het EPD of achteraf controle mogelijk maken. Drie belangrijke elementen met betrek-king tot het gebruik van het EPD door de zorgaanbieder wil ik nader toelichten. Het gaat om de GBZ-eisen, de UZI-pas en de logging.

Ten aanzien van de GBZ het volgende. Een zorgverlener of instelling moet voldoen aan de eisen die zijn vastgelegd in de eisen voor een Goed Beheerd Zorgsysteem (GBZ). Het gaat dan om waarborgen omtrent een juiste en zorgvuldige registratie en de verwerking en verstrekking van gegevens. Voldoet een zorgverlener of instelling niet aan deze eisen, dan kan deze niet aansluiten op het LSP. Landelijke elektronische uitwisseling van medische gegevens is dan niet mogelijk.

Om een veilig gebruik van het EPD te kunnen garanderen is echter meer nodig dan alleen technische beveiligingsmaatregelen. Minstens zo belangrijk is de wijze waarop zorgverleners in de dagelijkse praktijk de fysieke beveiliging van het EPD op orde hebben. Zo is het heel belangrijk dat het EPD in een veilige werkomgeving wordt gebruikt. Om beveiligingsrisico's zoveel mogelijk te beperken dienen zorgverleners uiteraard te voldoen aan de NEN-7510 norm, onderdeel van de GBZ-eisen.

Voor informatiebeveiliging is de organisatie van de informatiebeveiliging en het gedrag van gebruikers van groot belang. Voor de toegang van de zorgaanbieder tot het EPD is de UZI-pas geïntroduceerd. De UZI-pas is een digitaal paspoort voor zorgverleners. Het is net als het reguliere paspoort een belangrijk, persoons-gebonden «waardedocument». De UZI-pas speelt een rol bij de versleuteling van gegevens en faciliteert identificatie, authenticatie en autorisatie.

Het gebruik van de UZI-pas is met de nodige waarborgen omkleed om misbruik te voorkomen. Zo wordt de UZI-pas alleen verstrekt aan bepaalde beroepsbeoefenaren als bedoeld in artikelen 3 en 34 van de Wet BIG. De beoogde pashouder moet de UZI-pas persoonlijk afhalen na legitimatie met een identiteitsbewijs, bijvoorbeeld een paspoort. Alléén een UZI-pas is niet genoeg om toegang tot het EPD te krijgen. Om de UZI-pas te kunnen gebruiken heeft men ook een pincode nodig. De houder van een UZI-pas is verplicht de pas te beschermen tegen beschadiging, verlies of diefstal. Dat betekent onder andere dat de pashouder de pas niet onbewaakt achter dient te laten en niet mag uitlenen. Uiteraard dient de PIN-code van de UZI-pas ook geheim te blijven. Bij vermoeden van

misbruik dient de pashouder zijn pincode te wijzigen of de pas in te laten trekken.

Hierbij valt uiteraard in algemene zin op te merken dat er op het gebied van (informatie-)beveiliging geen definitieve oplossingen bestaan. Beveiliging staat voortdurend bloot aan aanvallen. Dat vraagt om permanent risicomanagement en bewustzijn bij de gebruiker. Steeds zullen nieuwe maatregelen moeten worden genomen om de betrouwbaarheid van de UZI-pas te borgen.
Signalen dat de betrouwbaarheid van de UZI-pas in het geding zou kunnen zijn, worden dan ook zeer serieus genomen. Wanneer signalen concreet zijn, worden deze onderzocht op mogelijke consequenties voor het systeem.
Zo worden nu maatregelen getroffen om een onlangs in een laboratorium-omgeving geconsta-teerde kwetsbaarheid in het reken-mechanisme van de chip te ondervangen, bijvoorbeeld door gebruik te maken van de nieuwste chiptechnolo-gie. Het is om reden van een permanente bewaking van de veiligheid dat ik ook graag tegemoet kom aan de wensen van o.m. mw. Sap inzake het testen van de EPD-keten (zie onder). Met het doel relevante ontwikkelingen nauwgezet te kunnen volgen en daar zo nodig tijdig op te anti-ciperen wordt tussen de departementen die te maken hebben met de toepassing van PKI-Overheid frequent overlegd om kennis en ervaring uit te wisselen en gewenste aanpassingen te bespreken.

In het LSP wordt geregistreerd welke zorgverlener op welk moment gegevens heeft aangemeld of ingezien, de zogenaamde logging. Om misbruik te voorkomen zal intelligente logging worden ingezet, om afwijkend gebruik te detecteren. Patiënten en toezichthouders hebben recht op inzage in deze loggevens.

Mocht iemand er dus in slagen een UZI-pas te ontvreemden en ook de beschik-king te hebben over de pincode van de pashouder, dan is er feitelijk sprake van identiteitsdiefstal. Om misbruik van de pas en de pincode te kunnen maken is bovendien toegang tot een GBZ noodzakelijk. Voorts moet de rechtmatige eige-naar verzuimen de pas onmiddellijk in te trekken. Het misbruik van de pas wordt gelogd onder de naam van de rechtmatige eigenaar van de pas. Bij inzage zal dit de patiënt opvallen. Bovenstaande waarborgen bevorderen mijn inziens een goed gebruik van het EPD. Mocht iemand er desondanks in slagen op deze wijze misbruik te maken van het EPD, dan ben ik voorstander van forse sancties, waaronder het strafrecht.

Inzage na overlijden

De heer Omtzigt heeft gevraagd of nabestaanden inzage in het dossier kunnen krijgen na overlijden. Zoals in de brief naar aanleiding van de eerste termijn is aangegeven gelden hiervoor de regels van de WGBO, die ook van toepassing zijn op het huidige medisch dossier. Inzage is ook na overlijden alleen mogelijk als de patiënt daar voor het overlijden toestemming voor heeft gegeven. Ik ben van mening dat voor het EPD geen andere regels moeten gelden dan voor het huidige papieren dossier. Daarnaast is het ook in het belang van de privacy van de patiënt dat nabestaanden geen inzage hebben zonder zijn toestemming.

Wel zal ik mogelijk maken dat de patiënt bij het EPD kan aangeven of hij toestemming geeft dat anderen na het overlijden gegevens mogen opvragen. Hiervoor zullen aanpassingen moeten worden gedaan in het LSP. Ik zal zoals toegezegd Nictiz vragen om de consequenties hiervan in

kaart te brengen. Aan de hand van die analyse zal ik bepalen wanneer deze modaliteit kan worden aangeboden.

Beveiliging

Mevrouw Sap heeft verzocht om zowel voorafgaande aan de landelijke uitrol van het EPD als gedurende de eerste jaren na invoering, periodiek de beveiliging van de gehele EPD-keten te testen. Mevrouw Sap en de heer Van der Vlies hebben mij gevraagd daarbij duidelijk aan te geven tot welke maatregelen de resultaten van deze testen eventueel kunnen leiden. In aanvulling op de beveiligingsmaatregelen zoals genoemd in mijn vorige brief, bericht ik u als volgt.
Uiterlijk voor de datum waarop de zorgaanbieders verplicht moeten aansluiten op het LSP, zal een grootschalige indringerstest plaatsvinden. Deze test zal jaarlijks worden herhaald. De basis van een dergelijke test zijn de risicoprofielen die worden opgesteld voor de schakels in het EPD-netwerk (GBZ, ASP, ZSP en LSP). In de test zal naast controle op de fysieke en systeembeveiliging, ook gekeken worden naar het «onder water» simuleren van het gebruik van de UZI-pas. Bij de opzet van de indringerstest en de uitvoering ervan worden onafhankelijke specialisten ingezet. Ik zal de Kamer nader informeren over de opzet van deze test voordat deze wordt uitgevoerd.

Na uitvoering van de grootschalige indringerstest zal ik u opnieuw informeren over de uitkomsten en over de gerichte maatregelen die mogelijk noodzakelijk zijn. Hierbij zal ik onderscheid maken in een collectief en een individueel risico. Indien uit de testen blijkt dat een collectief niet-verwijtbaar risico voor veilige en betrouwbare gegevensuitwisseling is geconstateerd, dan kan dit leiden tot een verplichte beveiligingsrelease van het LSP die alle gebruikers moeten doorvoeren binnen een gestelde termijn. In het meest ernstige geval zou ook het LSP gesloten kunnen worden om een beveiligingslek te herstellen. Bij een risico dat is ontstaan door individueel verwijtbaar gedrag worden gerichte maatregelen genomen en opgelegd aan de zorgaanbieder.

Beheerder LSP

Mevrouw Koşer Kaya heeft gevraagd wie de beheerder wordt van het LSP. Zoals aangegeven zal Nictiz het LSP beheren. Dat zal in de AMvB worden vastgelegd.

Toestemming patiënt

Mevrouw Koşer Kaya vroeg ook wanneer de patiënt toestemming moet gegeven voor raadpleging van het EPD. Is dit eenmalig of aan het begin van iedere behandeling. Toestemming dient per zorgverlener en per behandelrelatie eenmalig te worden gegeven, dus niet iedere keer als de patiënt bijvoorbeeld bij de huisarts komt.

Bijwerken gegevens

De heer Zijlstra vroeg hoe snel gegevens moeten worden bijgewerkt in het dossier. Dat gebeurt binnen 24 uur of zoveel sneller als nodig is voor het verlenen van goede zorg.

Afschermen gegevens

De heer Zijlstra en de heer Van der Vlies hebben vragen gesteld over het zichtbaar maken dat gegevens zijn afgeschermd. Net als de heer Zijlstra zie ik het belang dat voor de opvragende zorgverlener duidelijk is of gege-

vens in het medisch dossier van de patiënt al dan niet zijn afgeschermd. Wel is van belang dat daarbij geenszins valt te herleiden om welke gegevens het dan gaat. Dit zou immers een schending van de privacy van de patiënt opleveren. Ik hecht er aan het oordeel van het CBP en de Raad van State hierover te vragen, zodat de aspecten die door de leden Zijlstra en Van der Vlies naar voren zijn gebracht zorgvuldig kunnen worden gewogen.
Een voorstel hiertoe zal worden meegenomen in het wetsvoorstel waarin ook de strafrechtelijke bepaling voor misbruik van het EPD zal worden geregeld.

Ook is gevraagd of het mogelijk zou zijn het afschermen alleen zichtbaar te maken in geval van spoedsituaties. Ik zal onderzoeken of dat mogelijk is. Mijn eerste inschatting is dat dit technisch veel implicaties heeft.

Amendementen

Tijdens de tweede termijn ben ik ingegaan op de regionale component van amendement 27, 28, 29, 30. Hierbij heb ik aangegeven dat ik daar welwillend tegenover sta, maar dat gekeken dient te worden naar een formulering die juridisch zuiver is. Gelet op het overleg dat hierover gevoerd is, ben ik van mening dat de aangepaste formulering juridisch correct is. Het oordeel over de amendementen heb ik reeds uitgesproken.

Met betrekking tot het oorspronkelijke amendement 16 dat een nahangprocedure regelt, is een nieuwe versie ingediend door de leden Vermeij en Omtzigt. Ik begrijp de wens van de Kamer om voldoende invloed te kunnen uitoefenen op de inhoud van de Amvb. Ik wil wel opmerken dat de gekozen vorm afwijkt van de gebruikelijk vormen van voor- en nahang. Ik laat het oordeel over dit amendement over aan de Kamer.

Verder heb ik toegezegd aan mevrouw Gerkens dat ik in zou gaan op het nieuwe amendement 44 ter vervanging van amendement 20. Hierover wil ik opmerken dat amendement 28 ter vervanging van amendement 19 van de heer Omtzigt het amendement van mevrouw Gerkens overbodig maakt. Het amendement van de heer Omtzigt regelt namelijk in ruimere mate hetgeen mevrouw Gerkens ook voor ogen heeft.

Tot slot

Ik ga er vanuit dat ik uw vragen hiermee afdoende heb beantwoord en dat heden over het wetsvoorstel gestemd kan worden. Tot slot wil ik nog opmerken dat ik bij de uitrol van het EPD met inachtneming van de motie van mevrouw Vermeij uiteraard nauw zal samenwerken met het veld, waarbij ik de regie op mij zal blijven nemen.

De minister van Volksgezondheid, Welzijn en Sport,
A. Klink