

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1098

Vragen van het lid **Voortman** (GroenLinks) aan de minister van Volksgezondheid, Welzijn en Sport over *een onderzoeksjournalist die medische gegevens van een voetballer van AZ heeft verkregen* (ingezonden 23 december 2010).

Antwoord van minister **Schippers** (Volksgezondheid, Welzijn en Sport) (ontvangen 17 januari 2011).

Vraag 1

Bent u bekend met het bericht dat een onderzoeksjournalist de medische gegevens van een voetballer van AZ heeft gekregen van een medewerker van het Medisch Centrum Alkmaar?¹

Antwoord 1

Ja.

Vraag 2

Deelt u de mening dat de privacy van de betrokken voetballer ernstig is geschaad?

Antwoord 2

Ja.

Vraag 3

In welke procedures voorziet de wet- en regelgeving als onverhoopt persoonsgegevens uit het Elektronisch Patiënten Dossier (EPD) uitlekken? Wordt de betrokken patiënt in zo'n geval altijd ingelicht? Kunt u uw antwoorden toelichten?

Antwoord 3

Allereerst wil ik benadrukken dat het in dit geval niet het landelijk EPD betreft. De telefonisch opgevraagde gegevens waren opgeslagen in het lokale ziekenhuis-informatiesysteem van het Medisch Centrum Alkmaar en op cd per post aan de onderzoeksjournalist toegezonden. In het licht van de beveiligingsmaatregelen die zijn genomen met betrekking tot uitwisseling van medische informatie via de landelijke infrastructuur zou een dergelijke opvraging van medische gegevens niet mogelijk zijn geweest. De landelijke

¹ De Telegraaf, «Medisch dossier Didulica op straat», 9 december 2010.

infrastructuur is zo ontworpen dat de medische gegevens in de computersystemen van de zorgverleners staan. Medische gegevens kunnen alleen door daartoe geautoriseerde zorgverleners worden geraadpleegd aan de hand van een UZI-pas met daarbij behorende pincode onder de voorwaarde dat er een behandelrelatie is met de zorgconsument en deze toestemming voor de raadpleging heeft gegeven. Raadplegingen kunnen alleen gedaan worden vanuit de locatie (apotheek, huisartsenpost of ziekenhuis) waar de betreffende zorgverlener werkzaam is aangezien de UZI-pas in beginsel alleen in die betreffende instelling gebruikt kan worden.

Misbruik van de landelijke epd-infrastructuur kan op verschillende wijzen worden gesanctioneerd:

1. Een bestuurlijke boete voor de zorgaanbieder of individuele beroepsbeoefenaar voor overtreding van de regels in de Kaderwet zorginformatieuitwisseling (bijv. verwerking van gegevens zonder dat er een behandelrelatie met de patiënt is of opvragen van gegevens zonder toestemming van de patiënt).
2. Bestuursdwang door het College Bescherming Persoonsgegevens in verband met overtreding van de Wet bescherming persoonsgegevens (schending van regels omtrent verwerking van gegevens in de Wet bescherming persoonsgegevens).
3. Strafrechtelijke boete of gevangenisstraf in verband met schending van de bepalingen met betrekking tot het beroepsgeheim (art. 272 Wetboek van strafrecht) of computervredebreuk (art. 138a Wetboek van strafrecht).
4. Tuchtrechtelijke maatregel ten aanzien van de beroepsbeoefenaar bij overtreding van de bepalingen rondom verantwoorde zorg in de Wet op de beroepen in de individuele gezondheidszorg (bijv. boete, berisping, doorhaling register etc).
5. Bestuursrechtelijke handhaving ten aanzien van instellingen bij overtreding van de bepalingen rondom verantwoorde zorg in de Kwaliteitswet zorginstellingen (bijv. aanwijzing van de minister). Na aanvaarding van het voorstel tot wijziging van de Kaderwet elektronische zorginformatieuitwisseling die naar uw Kamer is gestuurd, komt daar nog bij:
6. De mogelijkheid voor de strafrechter om de beroepsbeoefenaar uit het beroep te onttrekken bij overtreding van artt. 138a of 272 van het Wetboek van strafrecht.

Via de landelijke infrastructuur is altijd inzichtelijk welke zorgverlener, wanneer welke gegevens heeft geraadpleegd en gecontroleerd kan worden of dit rechtmatig is geweest. Meerdere aspecten van het opvraaggedrag worden 24 uur per dag bewaakt binnen het LSP.

Afwijkingen en eventueel misbruik worden gedetecteerd, geanalyseerd en opgevolgd. Indien (een poging tot) misbruik wordt geconstateerd wordt dit aan de toezichthouders CBP en IGZ gemeld. Hiertoe zijn afspraken gemaakt tussen Nictiz en de toezichthouders.

Om de positie van de burger verder te versterken en het vertrouwen in de landelijke infrastructuur te vergroten, heb ik (onder meer naar aanleiding van discussies die in de Eerste Kamer hebben plaatsgevonden) Nictiz de opdracht gegeven om een voorziening in te richten waarmee burgers die dat wensen automatisch een notificatie per e-mail of sms kunnen krijgen zodra hun gegevens zijn geraadpleegd. Hiermee kan worden voorzien in nog meer transparantie en controlemogelijkheden op de uitwisseling van medische gegevens.

Vraag 4

Hoe denkt u om te gaan met de belangrijkste zwakke plek in de beveiliging van het EPD: de menselijke factor?

Antwoord 4

Zoals in de beantwoording van vraag 3 is beschreven, is er binnen de landelijke infrastructuur juist een aantal technische maatregelen getroffen om de informatie-beveiliging minder afhankelijk te laten zijn van de menselijke factor. Zorgverleners kunnen via de landelijke infrastructuur alleen gegevens uitwisselen met daartoe bevoegde collega's die gebruik maken van daarvoor gekwalificeerde informatiesystemen en beveiligde netwerkverbindingen. De identiteit van de zorgverleners wordt vastgesteld met behulp van UZI-passen.

Door dit soort technische maatregelen wordt menselijk falen (in dit geval van het type «te goed van vertrouwen») door middel van de landelijke infrastructuur beperkt. Daarnaast bestaat nog een aantal juridische en procedurele maatregelen ten aanzien van het beveiligingsbewustzijn binnen de zorgsector. Specifiek voor de landelijke infrastructuur zijn factsheets opgesteld voor zorgverleners over informatiebeveiliging. Zo worden zorgverleners gewezen op de veilige installatie van en de omgang met werkstations en UZI-passen.

Vraag 5

Heeft u al hackers betrokken bij de ontwikkeling van het EPD, zoals uw voorganger de Kamer heeft toegezegd? Zo ja, wat waren de resultaten? Zo nee, wanneer kunnen de resultaten van de hacktest worden verwacht? Gaat u de hacktest regelmatig, bijvoorbeeld jaarlijks, herhalen? Kunt u dat toelichten?

Antwoord 5

Ja. Bij het ontwerp en beheer van de landelijke infrastructuur vindt nadrukkelijk periodiek afstemming plaats met verschillende experts op het gebied van beveiliging van elektronisch gegevensverkeer waaronder ook «goede hackers» (ethical hackers). Zo worden bepaalde onderdelen van de landelijke infrastructuur jaarlijks door onafhankelijke beveiligingsexperts aan een hackerstest onderworpen.

De wijze waarop dat gebeurt, is beschreven in bijlage 2 van de voortgangsrapportage elektronisch patiëntendossier die 20 juli 2009 aan uw Kamer is verstuurd. Voorafgaand aan het verplicht aansluiten op het LSP, worden de verschillende componenten van de landelijke infrastructuur aan een grootschalige ketenbrede indringerstest (GKI) onderworpen. Over de voortgang en de resultaten van de testen die onderdeel uitmaken van de GKI wordt uw Kamer door middel van de voortgangsrapportages per kwartaal geïnformeerd.

Bedreigingen worden continu geïnventariseerd, geanalyseerd en geadresseerd. Indien nodig worden maatregelen aangepast of aanvullende technische, procedurele en organisatorische maatregelen getroffen. Uit de tot op heden uitgevoerde indringerstesten zijn geen kritieke bevindingen gedaan.

Vraag 6

Hebben patiënten al toegang tot hun gegevens in het EPD? Hebben zij de mogelijkheid om bepaalde (deels) informatie te vergrendelen? Bent u voornemens de toegang van de patiënt tot het dossier verder te verbeteren? Kunt u uw antwoorden toelichten?

Antwoord 6

Ik hecht er veel waarde aan dat patiënten kunnen beschikken over inzage in hun eigen medische gegevens. Echter, zoals ik u al in de voortgangsrapportages heb bericht, zijn er kwetsbaarheden geconstateerd in het GSM- en SMS-verkeer waar het authenticatiemiddel EPD-DigiD primair van afhankelijk is. Er is thans dus geen afdoende beveiligd authenticatiemiddel voorhanden om zorgconsumenten online toegang tot hun eigen medische gegevens te verschaffen. Zoals aangekondigd in de genoemde voortgangsrapportages beraad ik mij op dit moment op alternatieven.

De burger kan (door middel van een papieren formulier of met behulp van zijn DigiD) totaal bezwaar maken bij het Klantenloket waarmee zijn/haar verwijzindex geheel wordt vernietigd en de gegevens in de index worden verwijderd.

Het is voor zorgaanbieders vervolgens niet meer mogelijk om aanmeldingen of opvragingen te doen.

Vanaf het tweede kwartaal 2011 wordt het mogelijk om via het papieren proces en e-formulieren ook beperkt toegang te geven tot een door de patiënt aangegeven selectie van (een categorie van) individuele zorgverleners of zorginstellingen. Op deze wijze kunnen burgers specifiek aangeven dat alleen de eigen huisarts, de eigen specialist en apotheek toegang krijgt tot de gegevens en de rest niet.

Vraag 7

Krijgt de patiënt inzage in wie wanneer toegang heeft gehad tot zijn dossier? Zo nee, waarom niet? Zo ja, hoe wordt dit geïmplementeerd?

Antwoord 7

Via het Klantenloket kunnen burgers inzage krijgen in wie hun gegevens hebben aangemeld en wie hun gegevens via de landelijke infrastructuur voor gegevens-uitwisseling in de zorg hebben opgevraagd. Dit inzageoverzicht kan via een papieren formulier of met behulp van DigiD worden aangevraagd. Dit inzage-overzicht wordt vervolgens naar het GBA-adres verstuurd.

Op dit moment hebben ruim 2 200 burgers een dergelijk inzageverzoek verstrekt gekregen.

Zoals aangegeven in het antwoord op vraag 3 zal ik als extra controlemaatregel het mogelijk maken dat burgers ervoor kunnen kiezen om automatisch per email of per sms een bericht van het Klantenloket te ontvangen indien hun gegevens zijn geraadpleegd.

Vraag 8

Hoeveel mensen hebben op dit moment bezwaar aangetekend tegen opname in het EPD? Welk percentage van artsen en ander medisch personeel heeft bezwaar gemaakt tegen opname in het EPD? Hoe beoordeelt u deze cijfers?

Antwoord 8

Het totaal aantal verwerkte bezwaarverzoeken per 31 december 2010 bedraagt 435 222 (= 2,6% van de gehele Nederlandse bevolking inclusief in reactie op de landelijke campagne van 2008).

Tot en met 31 december 2010 zijn 2161 verzoeken tot intrekking bezwaar verwerkt.

Ik beschik niet over de gegevens waaruit valt op te maken welk percentage van mensen die bezwaar hebben gemaakt daarvan artsen en of ander medisch personeel is. Registratie van bezwaar vindt plaats op basis van het betreffende Burger Service Nummer (BSN). Er worden geen andere persoonsgegevens vastgelegd in de verwijzindex. Dat is ook nadrukkelijk niet de bedoeling.