Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

33 509 Wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens)

Y

VERSLAG VAN EEN NADER SCHRIFTELIJK OVERLEG

Vastgesteld 27 juni 2017

De vaste commissie voor Volksgezondheid, Welzijn en Sport[1] heeft met kennisgenomen van de reactie van de Staatssecretaris van Volksgezondheid, Welzijn en Sport van 21 april 2017 op de nadere schriftelijke vragen van de commissie van 29 maart jl.[2], naar aanleiding van het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders[3] en de daarop volgende gedachtewisseling[4].
Naar aanleiding daarvan is op 9 juni 2017 een brief gestuurd aan de Minister.

De Minister heeft op 27 juni 2017 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde nader schriftelijk overleg.

De griffier van de vaste commissie voor Volksgezondheid, Welzijn en Sport,
De Boer

[1] Samenstelling: Ten Hoeve (OSF), Koffeman (PvdD), Kuiper (CU), De Vries-Leggedoor (CDA), Flierman (CDA), Barth (PvdA), Beuving (PvdA), Ganzevoort (GL), De Grave (VVD), Martens (CDA) (*voorzitter*), Van Strien (PVV), Bruijn (VVD) (*vicevoorzitter*), P. van Dijk (PVV), Gerkens (SP), Atsma (CDA), Bredenoord (D66), D.J.H. van Dijk (SGP), Don (SP), Van Hattem (PVV), Nooren (PvdA), Oomen-Ruijten (CDA), Prast (D66), Schnabel (D66), Wezel (SP), Klip-Martin (VVD) Baay-Timmerman (50PLUS)
[2] Verslag nader schriftelijk overleg van 24 april 2017 (Kamerstukken I 2016/17, 33 509, X).
[3] Kamerstukken I 2016/17, 33 509, U en bijlage.
[4] Verslag schriftelijk overleg van 21 februari 2017 (Kamerstukken I 2016/17, 33 509, W).

kst-33509-Y
ISSN 0921 - 7371
's-Gravenhage 2017

BRIEF VAN DE VOORZITTER VAN DE VASTE COMMISSIE VOOR VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Minister van Volksgezondheid, Welzijn en Sport

Den Haag, 9 juni 2017

De commissie voor Volksgezondheid, Welzijn en Sport (VWS) heeft met belangstelling kennisgenomen van uw reactie van 21 april 2017 op de nadere schriftelijke vragen van de commissie van 29 maart jl.[5], naar aanleiding van het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders[6] en de daarop volgende gedachtewisseling[7]. De leden van de fracties van **PVV**, **SP** en **PvdD** leggen u nog graag enige nadere vragen voor.

In antwoord op de vraag van de leden van de **PVV-**fractie naar de concrete verwerking van de suggestie voor een veiliger systeem, wordt op pagina 5 van het verslag van het nader schriftelijke overleg gesteld dat de opmerkingen van de betreffende expert, de heer Verheul, «meer in zijn algemeenheid zijn meegenomen bij het opstellen van het besluit». Deze expert stelt echter heel duidelijk dat de verwijsindex in het Landelijk Schakelpunt (LSP) een risico vormt voor de privacygegevens van patiënten; de verwijsindex zou onwenselijk en niet-noodzakelijk zijn en de gegevens zouden in verkeerde handen kunnen vallen.[8] De leden van de PVV-fractie krijgen graag nader verduidelijkt welke maatregelen concreet zijn meegenomen bij het opstellen van het ontwerpbesluit, om te voorkomen dat de verwijsindex in het LSP een risico vormt voor de privacygegevens van patiënten. Kunt u bevestigen dat met het nu voorliggende besluit het door de expert aangeduide risico in voldoende mate is uitgesloten? Zo niet, hoe groot is dan het risico bij gebruik van een verwijsindex met centrale ontsleuteling?

Volgens de Autoriteit Persoonsgegevens zijn in het eerste kwartaal van 2017 vanuit de gezondheidszorg 600 meldingen gedaan van datalekken, met een verdubbeling van het aantal gevallen in ziekenhuizen ten opzichte van vorig jaar.[9] Welke maatregelen zullen er in het kader van de uitvoering van dit besluit worden genomen, om te voorkomen dat deze stijgende tendens van risico's op datalekken bij elektronische gegevensverwerking door zorgaanbieders zich voortzet?

In de uitzending van EenVandaag van 12 mei jl. werd gesteld dat patiënten die niet deelnemen in het Elektronisch Patiëntendossier niet of moeilijker medicijnen verstrekt krijgen bij de apotheek, of dat wordt voorgewend dat deelname aan het LSP een voorwaarde is om medicatie mee te krijgen.[10] Kunt u aangeven welke maatregelen bij de uitvoering van dit besluit zullen worden genomen, om te voorkomen dat verstrekking van medicatie of andere medische zorg aan patiënten die ervoor kiezen om niet deel te nemen in een elektronisch patiëntendossier, bemoeilijkt wordt? Wordt bij de uitvoering van dit besluit uitdrukkelijk en proactief naar zowel zorgverlener als zorgconsumenten gecommuniceerd dat deelname aan een elektronisch patiëntendossier geschiedt op geheel vrijwillige basis? Zo nee, waarom niet? Zo ja, op welke wijze wordt dit gecommuniceerd?

---

[5] Verslag nader schriftelijk overleg van 24 april 2017 (Kamerstukken I 2016/17, 33 509, X).
[6] Kamerstukken I 2016/17, 33 509, U en bijlage.
[7] Verslag schriftelijk overleg van 21 februari 2017 (Kamerstukken I 2016/17, 33 509, W).
[8] Tijdens de deskundigenbijeenkomst van 15 april 2016 (Kamerstukken I 2015/16, 33 509, L).
[9] Zie ook Tweede Kamervragen van 15 mei 2017 (2017Z06286) en https://www.security.nl/posting/515076/PVV+vraagt+om+maatregelen+tegen+datalekken+in+ziekenhuizen
[10] http://binnenland.eenvandaag.nl/tv-items/74023/_zonder_pati_ntendossier_moeizaam_of_geen_medicatie_

De leden van de fractie van de **SP** hebben kennisgenomen van de toelichting op het verschil tussen dataprotectie, informatiestromen en beveiliging met betrekking tot de NEN-normen. Er wordt echter niet ingegaan op wat dit vervolgens betekent voor de technische beveiliging. De leden van de SP-fractie krijgen graag nader geduid hoe de NEN-normen de technische beveiliging borgen.

Ook krijgen de leden van de SP-fractie graag nader toegelicht waarom *end-to-end* encryptie niet als hoogst mogelijke beveiliging zou moeten worden opgenomen. U wijst erop dat er in de toekomst mogelijk betere technieken zullen komen. Is het niet zo dat *end-to-end* encryptie niet gaat over technieken, maar over welke onderdelen je beveiligd? Mogen de leden van de SP-fractie het zo uitleggen: als de deur openstaat, kunnen er heel makkelijk mensen binnenkomen; als de deur niet op slot zit, is het al iets lastiger; de deur op slot doen, is het beste wat je kunt doen om de deur te beveiligen, maar met welk slot dat het beste kan, hangt af van de stand van de techniek. Het gaat dus om *wat* we beveiligen en niet *hoe*, want ook de leden van de SP-fractie zijn van mening dat *hoe* onderhavig is aan de laatste stand der techniek. Maar wat er beveiligd wordt, is iets wat de tand des tijds kan doorstaan. De leden van de SP-fractie vragen nogmaals dringend een *end-to end* encryptie te verplichten.

Zij zijn wat verward door het antwoord op de vraag hoe wordt geoordeeld over de mogelijkheid kwetsbaarheden in software toe te staan of actief te laten bestaan. In het antwoord wordt herhaald hoe het straks met de Wet op de inlichtingen- en veiligheidsdiensten (WIV) geregeld is. Ook wordt herhaald dat de kwetsbaarheden in software kunnen blijven bestaan als er andere belangen zijn dan de belangen van betrokkenen. Daarmee is het dus mogelijk dat zwakheden in software, bekend bij de diensten, blijven bestaan, waardoor partijen met kwaadaardige bedoelingen die zwakheid ook kunnen gebruiken om aan medische gegevens te komen. Erkent u dat dit een mogelijkheid is? Zo nee, waarom denkt u dat de medische sector hiervan gevrijwaard kan blijven? Met dit verhaal in het achterhoofd, zou de regering er dan op zijn minst niet voor moeten pleiten om *end-to-end* encryptie als een minimumeis te stellen, zodat áls een partij (hackers óf diensten) een kwetsbaarheid vindt en toepast om een component die zich tussen verzender (end 1) en ontvanger (end 2) bevindt te compromitteren, dit geen effect heeft op de integriteit of confidentialiteit van de het verstuurde bericht?

Is de regering niet van mening dat de confidentialiteit en integriteit van gegevens die de gezondheid van mensen betreffen en die onder het medisch beroepsgeheim vallen, boven het potentiële belang van diensten gaan die mogelijk in een component tussen verzender en ontvanger een bericht met medische inhoud zouden kunnen afluisteren, na een inbraak? Zou een verzoek om inzage in medische gegevens niet altijd via de verantwoordelijke arts moeten gaan, en zou het afluisteren van gegevens buiten deze arts om dan niet technisch onmogelijk moeten worden gemaakt? U stelt bovendien zelf dat *end-to-end* versleuteling op dit moment tot het hoogste niveau van technische ontwikkeling behoort. Er zijn op dit moment echter talloze systemen in de zorg die hier niet aan voldoen. Zouden niet *alle* systemen die zorginformatie communiceren en waarbij *end-to-end* beveiliging technisch toepasbaar is, moeten voldoen aan dit [het] hoogste niveau van beveiliging?

Naar aanleiding van de antwoorden van 21 april 2017, hebben de leden van de fractie van de **PvdD** nog enkele aanvullende vragen inzake het Ontwerpbesluit elektronische gegevensverwerking door zorgaanbieders.

Deze vragen staan ook in relatie tot de aangenomen moties Tan c.s.[11] (na verwerping van wetsvoorstel 31.466[12]), Bredenoord c.s.[13] en Teunissen c.s.[14] (bij de behandeling van het wetsvoorstel 33.509[15]).

Op de vraag of eerdergenoemd besluit niet in strijd is met de hier bovengenoemde motie-Tan c.s. (31 466, X) en of de subsidie geen verkapte vorm van staatsteun inhoudt, omdat er expliciet als eis is opgenomen dat een AORTA(LSP)-standaard gebruikt moet worden als voorwaarde voor de subsidie, wordt ontkennend geantwoord. Daarbij wordt gerefereerd aan de MedMij-standaarden, waarbij de patiënt op een gestandaardiseerde manier zelf gegevens kan gaan uitwisselen met andere zorgverleners, zonder dat hier een landelijk of regionaal schakelpunt voor nodig is. In het *Programma patiënt en medicatie* van het Besluit vaststelling beleidskader subsidiëring Versnellingsprogramma Informatie-uitwisseling Patiënt en professional (VIPP) [16] wordt expliciet een standaard genoemd waaraan voldaan moet worden: de standaard medicatieproces v6.12.2. De standaard v6.12.2 is een AORTA-standaard, dat wil zeggen, een LSP-standaard. Ook onder de *Subsidievoorwaarden* van het Besluit, worden op pagina 7 deze standaarden genoemd, met betrekking tot het opvragen van het actuele medicatieoverzicht, in het kader van modules A3, B1 een B2. In reactie hierop meldt de Staatssecretaris in de brief van 21 april jl. dat de standaard v6.12.2 een «standaard [is] die zorgbreed wordt ingevoerd om een eenduidige uitwisseling van medicatiegegevens mogelijk te maken». Kan de regering bevestigen dat het hier gaat om de zorgbrede invoering van het LSP, zoals benoemd in het «Convenant gebruik landelijke zorginfrastructuur 2016–2020» van de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ)?

In antwoord op de nadere vragen wordt gesteld dat ook van een nieuwere standaard dan v6.12.2 gebruik mag worden gemaakt. Ook stelt de Staatssecretaris dat andere systemen aan de eisen van deze standaard kunnen voldoen, om verderop aan te geven dat het Informatieberaad werkt aan een nieuwe versie van de standaard die infrastructuuronafhankelijk is. In de praktijk is er maar één systeem dat aan de standaard voldoet, het LSP, waar de standaard voor is ontwikkeld. In de wereld van standaarden betekent gebruik van een hoger nummer, dat gebruik mag worden gemaakt van een standaard met een hoger (opvolgend) versienummer van een zelfde soort, dus niet van een andere standaard. Gegeven dat het LSP nu de enige infrastructuur is die aan deze standaard voldoet, wordt dan toch niet de facto via de VIPP voorwaarden een verplichting voor gebruik van het LSP gecreëerd voor het mogen ontvangen van de subsidie?

Als het klopt dat de regering hier de LSP-standaard met bovengenoemd besluit verplicht, en daarmee ook het gebruik van het LSP verplicht voor partijen die aanspraak willen maken op de subsidie, kan zij dan uitleggen hoe deze verplichting zich verhoudt tot de aangenomen motie-Tan c.s., waarin de regering wordt verzocht alles te doen wat in haar vermogen ligt om verdere beleidsinhoudelijke, financiële en organisatorische medewerking aan de ontwikkeling van het Landelijk Schakelpunt te beëindigen?

---

[11] Kamerstukken I 2010/11, 31 466, X.
[12] Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg
[13] Kamerstukken I 2016/17, 33 509, R.
[14] Kamerstukken I 2016/17, 33 509, T.
[15] Wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens).
[16] Staatscourant 2016, nr. 68985, p. 5.

De leden van de fractie van de PvdD vragen ook wat de relatie is tussen het opvragen van medicatiegegevens, en het beschikbaar stellen van (ziekenhuis)gegevens aan patiënten, het beoogde doel van de subsidie.

In hoeverre lost deze subsidie de problemen op met de traag verlopende koppeling van het LSP met de tweedelijns gezondheidszorg? Wat zijn de obstakels voor het koppelen van het LSP met de tweede lijn (ziekenhuizen)? Kan de regering uitsluiten dat de koppeling van het LSP met de tweede lijn door deze subsidie beleidsmatig en financieel wordt gesteund?

De leden van de PvdD-fractie vernemen graag hoe de steun voor het LSP zich verhoudt tot het gebruik van andere systemen voor gegevensuitwisseling, om met name uitwisseling van medicatiegegevens vanuit de eerste lijn naar de tweede lijn mogelijk te maken; bijvoorbeeld via IHE-XDS of het Whitebox-systeem, dat naar verluidt werkt aan een mogelijkheid om een (geautoriseerd) medicatieoverzicht ter beschikking te stellen van specialisten.[17] Kan voor gebruik van deze standaarden ook subsidie worden aangevraagd in het kader van het VIPP, als zij het mogelijk maken om een medicatieoverzicht op te vragen? Is de regering bereid het subsidiebesluit op dit punt te verduidelijken richting potentiële deelnemers?

De subsidie betreft exclusief de tweede lijn (ziekenhuizen). De eerste lijn krijgt geen subsidie voor e-health, terwijl daar veel winst te verwachten valt met het uitwisselen van gegevens van patiënten. Een investering in e-health voor koppelingen met/tussen patiënt en eerstelijnszorgverleners, zoals apotheker en huisarts, leidt tot meer keuzevrijheid voor de patiënt om gegevens decentraal uit te kunnen wisselen. Waarom strekt het VIPP zich niet (ook) uit tot dergelijke e-health? Kan dit worden verklaard doordat de communicatie van gegevens in de eerste lijn met de patiënt reeds afdoende afgedekt wordt door deze via het LSP te laten lopen, waar inmiddels veel huisartsen en apothekers op zijn aangesloten en waarmee in Nijmegen een pilot loopt?[18] De leden van de PvdD-fractie krijgen hierop graag een reactie.

Vorig jaar is een set afspraken gemaakt en is een website gelanceerd met betrekking tot het MedMij-programma.[19] Dit wordt ondersteund door het Ministerie van VWS, en mede door VWS en de zorgverzekeraars gefinancierd.[20] In het subsidiebesluit wordt op pagina 6 aan MedMij gerefereerd.

Uit de documentatie van MedMij wordt duidelijk dat bij MedMij wordt gewerkt met een LSP- standaard: «The following medication standards are in scope for MedMij: Medicatieproces 6.12 – dispense query/response (LSP). [...] At the time of writing this document, healthcare providers (prescribers, pharmacists) typically make use of Medicatieproces 6.12 using the Landelijk Schakelpunt (LSP) as health network. [...] In the future healthcare providers may choose to make use of the new FHIR standard for exchanging medication information, however, this is not foreseen within the timescales of MedMij. FHIR is more likely to be used in the personal health domain.»[21]

---

[17] https://whiteboxsystems.nl/nieuws/

[18] http://www.medmij.nl/patienten-in-regio-nijmegen-krijgen-door-medmij-inzage-in-hun-huisartsendossier/

[19] www.medmij.nl

[20] http://www.medmij.nl/faqs/ («Het Ministerie van Volksgezondheid Welzijn en Sport en de brancheorganisatie van zorgverzekeraars, Zorgverzekeraars Nederland, betalen het programma.»)

[21] https://informatiestandaarden.nictiz.nl/wiki/MedMij:V1.0_Standards

Klopt het dat bij de ontwikkeling van MedMij wordt uitgegaan van het LSP als de manier bij uitstek voor het opvragen van medicatiegegevens? De leden van deze fractie informeren hoe de uitwisseling van medicatiegegevens werkt voor patiënten die geen toestemming hebben gegeven, of willen geven, voor gebruik van het LSP. Zij krijgen dit graag toegelicht, ook in relatie tot de reportage van EenVandaag, van 12 mei 2017, waaruit blijkt dat patiënten onder druk gezet worden om zich aan te melden voor het LSP, omdat zij anders geen medicatie meekrijgen. Heeft de regering ideeën voor alternatieve manieren om medicatiegegevens beschikbaar te maken voor de (dienst)apotheker als patiënten géén toestemming geven voor het LSP?

In het subsidiebesluit worden voor het kunnen opvragen van medicatiegegevens door ziekenhuizen geen alternatieven voor het LSP meegenomen, waarmee actuele medicatiegegevens van huisarts of apotheek beschikbaar kunnen worden gesteld. Hoe verhoudt zich dit tot de aangenomen motie-Teunissen c.s. (33 509, T), waarin de regering wordt verzocht ervoor zorg te dragen dat toegang tot het medisch dossier niet alleen gecentraliseerd, maar ook decentraal via bij de zorgaanbieder vastgelegde toestemmingen en autorisaties mogelijk zal blijven?

De aangenomen motie-Bredenoord c.s. (33 509, R) verzoekt de regering *dataprotectie-by-design* verder uit te werken als het uitgangspunt voor de elektronische verwerking van medische gegevens en de Kamer daarover te informeren. In de bijlage van het Besluit vaststelling beleidskader subsidiering versnellingsprogramma informatie-uitwisseling patiënt en professional wordt een aantal uitgangspunten vermeld, maar *dataprotectie-by-design* niet. Hoe verhoudt dit besluit zich tot de aangenomen motie-Bredenoord c.s.? Op welke manier past de regering dit uitgangspunt wel toe?

In de brief van 21 april 2017 staat dat er bij grote ICT-systemen een *Privacy Impact Assessment* (PIA) moet worden toegepast en tevens dat *privacy-by-design* principes integraal onderdeel uitmaken van het beleidskader. Kan de regering, gegeven het feit dat het LSP genoemd wordt in een subsidievoorwaarde van de overheid en dus deel uitmaakt van overheidsbeleid, aangeven hoe *privacy-by-design* is toegepast in het LSP?

In het subsidiebesluit staat op pagina 6 dat de informatiestandaarden door het Informatieberaad worden vastgesteld: «Het streven is dat in maart 2017 in het Informatieberaad deze standaarden worden vastgesteld. Door ziekenhuizen […] optie te bieden om, in plaats van de informatiestandaarden zoals uitgeschreven in dit beleidskader, te voldoen aan nieuwere versies van informatiestandaarden, mits deze standaarden zijn vastgesteld in het Informatieberaad en zijn gepubliceerd, wordt de implementatie van de landelijk gekozen standaarden gestimuleerd.» Klopt het dat het Informatieberaad de standaarden mag vaststellen zoals, klaarblijkelijk, de LSP-standaard voor medicatie-uitwisseling? Zijn deze standaarden inmiddels door het Informatieberaad vastgesteld? Zo ja, welke standaarden zijn dat?

De leden van de fractie van de PvdD vernemen graag waaruit de (democratische) legitimiteit van het Informatieberaad bestaat om standaarden te kiezen en vast te leggen voor de sector. Waaraan ontleent het beraad het mandaat om verstrekkende besluiten te nemen over hoe de communicatie in de zorg wordt georganiseerd? Wie benoemt en controleert deze raad? In hoeverre is het besluitvormingsproces binnen het Informatieberaad open en toegankelijk voor partijen van buiten de zorg – gegeven ook dat informatiestandaarden álle burgers raken, en niet alleen zorgaanbieders?

Met dit subsidiebesluit en MedMij lijkt het LSP verder verankerd te worden en een centraal systeem actief te worden gestimuleerd. Tijdens het debat over het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens (33.509) gaf de Minister van VWS te kennen dat de overheid het beleid voert dat toestemmingen en autorisaties decentraal mogelijk blijven. Zij gaf aan dat de overheid geen voorkeur uitspreekt voor een of ander systeem en dat dit aan de sector wordt overgelaten en dat de overheid een neutrale positie inneemt.[22] Op welke manier draagt de regering er, naast het stimuleren van het LSP, zorg voor dat ook andere systemen dan het LSP zich kunnen ontwikkelen? De leden van de PvdD-fractie vernemen dit met name graag ten aanzien van decentrale communicatiesystemen, waarbij rechtstreeks tussen artsen onderling of tussen arts en patiënt, zonder centrale vastlegging van toestemmingen en autorisaties, informatie wordt uitgewisseld, conform de motie-Teunissen c.s.

De leden van de commissie voor Volksgezondheid, Welzijn en Sport zien uw reactie met belangstelling tegemoet en ontvangen deze graag uiterlijk 30 juni 2017.

De voorzitter van de vaste commissie voor Volksgezondheid, Welzijn en Sport,
M.J.T. Martens

[22] Handelingen I 2016/17, nr. 2, item 6, p. 2.

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 27 juni 2017

Met belangstelling heb ik kennis genomen van de nadere vragen die een aantal fracties van de vaste commissie voor Volksgezondheid, Welzijn en Sport heeft gesteld naar aanleiding van mijn reactie van 21 april 2017 op de schriftelijke vragen van de commissie over het bij brief van 14 november 2016 aangeboden ontwerp van het Besluit elektronische gegevensverwerking door zorgaanbieders. Graag beantwoord ik uw vragen. Daarbij merk ik op dat deze nadere vragen en antwoorden niet meer hebben geleid tot aanpassing van het besluit. De wet Cliëntenrechten bij elektronische verwerking van gegevens treedt op 1 juli 2017 in werking. Graag bied ik de belangenorganisaties van zorgprofessionals de duidelijkheid waaraan behoefte is als het gaat om de inwerkingtreding van het onderhavige besluit. Ik zal daarom het besluit verder in procedure brengen.

De leden van de fractie van de **PVV** vragen nogmaals om verduidelijking over de wijze waarop de opmerkingen van de heer Verheul over (de verwijsindex van) het Landelijk Schakelpunt zijn meegenomen bij het opstellen van het ontwerpbesluit. Zij vragen of het door de expert genoemde risico voldoende is uitgesloten.
Zoals ik ook in mijn brief van 21 april 2017 heb aangegeven zijn de suggesties van de heer Verheul in zijn algemeenheid meegenomen. Het wetsvoorstel en het besluit richten zich immers niet specifiek op het door de heer Verheul genoemde systeem. Met de toevoeging van artikel 6 aan het besluit ben ik van mening dat de AMvB op het gebied van informatieveiligheid en privacy als toereikend kan worden beschouwd. Het biedt kaders en randvoorwaarden zonder tot op de punt en komma voor te schrijven welke technieken moeten worden gebruikt. In mijn brief over Beleidsprioriteiten Informatievoorziening en ICT in de zorg (TK 2016–2017, 27 529, nummer 142) beschreef ik het belang van het scheiden van doel en instrumenten in het licht van haalbaarheid en toekomstvastheid. Het is ook in dit geval belangrijk om ruimte te laten voor implementatie en toepassing van nieuwe technologische ontwikkelingen. Verwacht mag worden dat door naleving van de normen en regelgeving, ook de eisen ten aanzien van privacy voldoende zijn geborgd. Het is aan de toezichthouders hierop toe te zien.

De leden van de fractie van de **PVV** vragen welke maatregelen er in het kader van de uitvoering van dit besluit worden genomen, om te voorkomen dat de stijgende tendens van meldingen van datalekken zich voortzet.
In de zorg worden – in vergelijking met andere sectoren – veel bijzondere persoonsgegevens verwerkt waardoor de sector verhoudingsgewijs meer meldingen zal doen. De meldplicht is recent, ook dat draagt ertoe bij dat het aantal meldingen in eerste instantie toeneemt en dat duidt ook op een toenemend bewustzijn bij medewerkers voor het juist omgaan met gevoelige persoonsgegevens.
Het besluit legt de technische en organisatorische eisen vast voor de beveiliging van gegevens. Het is aan de zorgaanbieders om concreet vast te stellen welke maatregelen zij nemen ter uitvoering van dit besluit.
Ik ben bereid initiatieven op het terrein van informatiebeveiliging te ondersteunen. Op 20 juni 2017 heb ik de leden van de Tweede Kamer een

brief[23] gestuurd over het Actieplan (informatie)beveiliging patiëntgegevens. De activiteiten uit het plan moeten leiden tot een structurele verbeteringen in de dagelijkse werkpraktijk bij ziekenhuizen voor wat betreft informatiebeveiliging en privacybescherming daadwerkelijk verbeteren. Dit actieplan zal spoedig
verbreed worden naar de hele zorgsector. Informatiebeveiliging is een doorlopend punt van aandacht en is een onderwerp waar alle partijen zich voor moeten blijven inzetten.

Een item in de uitzending van EenVandaag van 12 mei 2017 ging over het verstrekken van medicijnen aan patiënten die geen toestemming hebben gegevens voor het delen van hun gegevens via een elektronisch uitwisselingssysteem (i.c het Landelijk Schakelpunt). Naar aanleiding daarvan vragen de leden van de fractie van de **PVV** op welke wijze dit besluit bijdraagt aan het voorkomen dat verstrekking van medicijnen aan degenen die geen toestemming geven voor het mogen delen van hun gegevens via een elektronisch uitwisselingssysteem wordt bemoeilijkt. Ook de leden van de fractie van de **PvdD** vragen om een toelichting over de uitwisseling van medicatiegegevens naar aanleiding van de berichtgeving van EenVandaag.
In de Wet cliëntenrechten bij elektronische verwerking van gegevens is helder vastgelegd dat gegevens niet elektronisch mogen worden uitgewisseld zonder toestemming van de patiënt. De keus is aan de patiënt zelf. Dat staat in de wet en op de website van het in de uitzending genoemde systeem[24]. Natuurlijk scheelt het de zorgaanbieder tijd als hij de gegevens van zijn patiënt met één druk op de knop kan oproepen – dat is nou juist de meerwaarde van elektronische gegevensuitwisseling – maar dat laat onverlet dat de keuzevrijheid van de patiënt om wel of geen toestemming te geven voorop staat. Het mag geen reden zijn hem anders te behandelen als hij geen toestemming voor elektronische gegevensuitwisseling. Dat is in strijd met de wet.
Daarnaast is de zorgaanbieder- of hij zijn gegevens nu elektronisch uitwisselt of niet – altijd verantwoordelijk voor met de cliënt geverifieerde juistheid en actualiteit van de inhoudelijke medische gegevens. De zorgaanbieder heeft een onderzoeksplicht en hij mag nooit volledig of uitsluitend vertrouwen op gegevens die al dan niet elektronisch zijn aangeleverd door andere zorgaanbieders. Dat geldt ongeacht de situatie waarin hij wel of niet is uitgesloten van inzage in een systeem voor elektronische gegevensuitwisseling en ook ongeacht het feit of er veel of weinig gegevens zijn afgeschermd. Daarnaast moet de cliënt op grond van artikel 7:452 BW naar beste weten de inlichtingen en de medewerking geven die de hulpverlener redelijkerwijs voor de uitvoering van de behandelingsovereenkomst behoeft. Ook als de cliënt geen toestemming heeft gegeven voor elektronische gegevensuitwisseling. De informatie en onderzoeksverplichtingen alsmede het recht op het vrijelijk toestemming geven of weigeren, liggen dus allemaal vast op wetsniveau en zijn daarmee afdoende geregeld. In het besluit gaat het om technische en organisatorische eisen voor elektronische uitwisselingssystemen en zorginformatiesystemen en dit ziet niet op het in de genoemde uitzending geschetste probleem.

De leden van de fractie van de **SP** vragen hoe de NEN-normen de technische beveiliging borgen.
De NEN-7510 norm beschrijft een managementsysteem voor informatiebeveiliging. Een organisatie moet op basis van risicoanalyse van de dreigingen passende technische, procedurele en organisatorische

[23] https://www.rijksoverheid.nl/documenten/kamerstukken/2017/06/20/kamerbrief-over-actieplan-informatiebeveiliging-patientgegevens-medisch-specialistische-zorg-en-ggz
[24] https://www.vzvz.nl/page/Zorgconsument/Toestemming

maatregelen nemen. Periodiek, of bij iedere grotere wijziging, herhaalt de organisatie (delen van) de risicoanalyse en houdt daarmee de maatregelen op peil (stand van de techniek, wijziging in dreigingen). Hiermee sluit de norm aan op de internationale normen op het vlak van informatiebeveiliging.
Op technisch vlak noemt de norm geen specifieke maatregelen, omdat de risico's die een specifieke maatregel reduceert contextafhankelijk zijn. Wel dekt de NEN-norm specifieke (technische) aspecten waarnaar gekeken moet worden, zoals toegangsbeheer en authenticatie, encryptie, verwerving van programmatuur van derde partijen, etc.
De NEN-7512 norm gaat specifiek over gegevensuitwisseling in de zorg. Ook deze norm gaat uit van risicobeoordeling van dreigingen, op de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid. Afhankelijk van het risico (laag, matig, hoog, zeer hoog) worden bepaalde (technische) maatregelen (zoals te gebruiken authenticatiemiddelen of encryptie) normatief voorgeschreven, of aanbevolen.

De leden van de **SP**-fractie vragen nogmaals dringend een end-to-end encryptie te verplichten.
End-to-end encryptie is een technische maatregel om ervoor te zorgen dat alleen de verzender en de beoogd ontvanger een bericht kunnen lezen. Dit is dus een technische maatregel om de vertrouwelijkheid van berichtuitwisseling te helpen borgen. Bij end-to-end encryptie horen technische en organisatorische maatregelen, zoals het beheren en periodiek vervangen van encryptiesleutels en certificaten, en het verifiëren of certificaten van de communicatiepartner nog geldig zijn. Deze aanpalende maatregelen zorgen voor een bepaalde mate van complexiteit.
Om de door de leden van de **SP** genoemde analogie met sloten op de deur te gebruiken: vier sloten op de deur zouden kunnen worden beschouwd als veiliger dan één slot. Maar als je daarmee bij brand niet op tijd het pand uit kunt komen, dan zorgen de extra sloten op een ander aspect van veiligheid voor problemen. De verschillende veiligheidsrisico's moeten daarom altijd zorgvuldig tegen elkaar worden afgewogen en zijn sterk gerelateerd aan de specifieke situatie.
De daadwerkelijke risico's hangen dus af van de context en de overige technische, procedurele en organisatorische maatregelen die genomen zijn (zoals bijvoorbeeld communicatie over een afgezonderd, besloten netwerk). Deze risico's moeten periodiek worden afgewogen in de context, en deze risicoanalyse moet leiden tot adequate maatregelen. Het verplicht stellen van een specifieke maatregel gaat niet samen met deze systematiek. In zijn algemeenheid kan wel gezegd worden dat daar waar end-to-end encryptie haalbaar is, het gebruik hiervan zeker gewenst is.

De leden van de fractie van de **SP** vragen zich – met het oog op de confidentialiteit van medische gegevens – af of end-to-end encryptie verplicht zou kunnen worden om zo schending van de vertrouwelijkheid van een bericht als gevolg van zwakheden in software te voorkomen. Of om het afluisteren van medische gegevens na een inbraak technisch onmogelijk te maken.
In mijn antwoord op de voorgaande vraag, heb ik aangegeven waarom end-to-end encryptie niet algemeen wordt voorgeschreven. Ieder systeem kan, ook bij gebruik van end-to-end encryptie, uiteindelijk zwakheden blijken te bevatten. Iets wat aanvankelijk geen zwakheid was, kan dit door voortschrijdende technieken uiteindelijk wel worden. Op grond van het besluit zullen de verantwoordelijken voor de gebruikte systemen daarom bezig moeten blijven met het up-to-date houden van de informatiebeveiliging en de daarvoor beschikbare technieken. Hier ligt in de eerste plaats de verantwoordelijkheid tegen het voorkomen van kwaadaardige inbreuk. De inlichtingen- en veiligheidsdiensten hebben hun eigen bevoegdheden en verantwoordelijkheden – zoals wordt vastgelegd in de Wet op de

inlichtingen- en veiligheidsdiensten (WIV) – waarbij het uitgangspunt is dat de diensten belangendragers over mogelijke zwakheden informeren. Zoals gezegd houdt de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten hier toezicht op.

De leden van de fractie van de **PvdD** vragen of met het Besluit vaststelling beleidskader subsidiëring Versnellingsprogramma Informatie-uitwisseling Patiënt en professional (VIPP) aansluiting op het Landelijk Schakelpunt (LSP) wordt verplicht c.q. het LSP zorgbreed wordt ingevoerd. Zij leiden dit af uit het feit dat in de VIPP-regeling expliciet een standaard wordt genoemd waaraan voldaan moet worden: de standaard medicatieproces v6.12.2.
Deze aannames van de PvdD-fracties zijn niet juist. Het gebruik van het LSP wordt met de subsidieregeling van het programma VIPP niet verplicht, het LSP wordt niet zorgbreed ingevoerd en de subsidieregeling van het programma VIPP heeft geen relatie met het «Convenant gebruik landelijke zorginfrastructuur 2016–2020» van de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ). Er wordt niet één infrastructuur voorgeschreven. Ter toelichting het volgende.
Voor een veilige uitwisseling van medicatiegegevens is het noodzakelijk om waar mogelijk dezelfde standaarden te gebruiken die nu al in omloop zijn, dit vergroot de interoperabiliteit.
De standaarden waarnaar wordt verwezen zijn openbare standaarden omdat daarmee onafhankelijk van de gebruikte infrastructuur gegevens kunnen worden uitgewisseld.
In de subsidieregeling van het programma VIPP is opgenomen dat minimaal gebruik gemaakt moet worden van bepaalde standaarden, maar dat ook nieuwere standaarden gebruikt mogen worden. Als er een alternatief is dat op gelijke wijze of meer bijdraagt aan eigen regie door de cliënt (uitgangspunt van de regeling) en net zo veilig – of veiliger – is dan de huidige standaard dan kan deze ook worden gebruikt. De aanname dat bedoeld wordt dat alleen een nieuwere standaard gebruikt mag worden met een hoger (opvolgend) versienummer is incorrect. Iedere nieuwere standaard voor medicatie-uitwisseling die veilig is kan worden gebruikt, zolang de medicatiegegevens op een veilige manier kunnen worden uitgewisseld.

De leden van de fractie van de **PvdD** vragen wat de relatie is tussen het opvragen van medicatiegegevens, en het beschikbaar stellen van (ziekenhuis)gegevens aan patiënten, het beoogde doel van de (VIPP-)subsidie.
Het is in het belang van de patiënt dat er een actueel medicatieoverzicht is. In de huidige situatie komt het voor dat patiënten met een tas met medicijndoosjes naar het ziekenhuis komen of dat zij zelf een medicatie-overzicht van de apotheek meenemen. Als de patiënt er toestemming voor geeft kan het ziekenhuis deze gegevens ook via een elektronisch uitwisselingssysteem raadplegen. Dat hoeft niet via het LSP te zijn, dat kan ook via een lokale of regionale infrastructuur.
Ook na ontslag uit het ziekenhuis is het voor de patiënt van belang om een integraal overzicht te hebben van de voorgeschreven medicatie en de eventuele veranderingen daarin als gevolg van de ziekenhuisopname.

Ook de vragen van de leden van de **PvdD**-fractie in hoeverre de koppeling van LSP met de tweede lijn (ziekenhuizen) beleidsmatig en financieel wordt gesteund en hoe de steun voor het LSP zich verhoudt tot het gebruik van andere systemen voor gegevensuitwisseling om met name uitwisseling van medicatiegegevens vanuit de eerste lijn naar de tweede lijn mogelijk te maken, berusten op de verkeerde aanname dat het VIPP-programma verplichte aansluiting op het LSP verlangt.

Het ziekenhuis moet een aantal resultaten behalen om de subsidie te mogen houden. Aansluiting bij het LSP is geen onderdeel van dat resultaat. Zoals aangegeven kan de gegevensuitwisseling, mits veilig, ook via andere systemen plaatsvinden. Dit wordt ook duidelijk gecommuniceerd naar de deelnemende ziekenhuizen. Het is wel van belang dat de patiënt ook toegang krijgt tot de gegevens. Dat is bij bijvoorbeeld het Whiteboxsysteem nu nog niet mogelijk.

De leden van de fractie van de **PvdD** vragen waarom het VIPP zich niet uitstrekt naar investeringen in eHealth voor koppelingen tussen patiënt en eerstelijns zorgverleners zoals apotheek en huisarts.
Het VIPP-programma is een nadere invulling van de afspraak uit het bestuurlijk hoofdlijnenakkoord medisch specialistische zorg 2014 – 2017 om e-health te stimuleren. Partijen hebben daar gezamenlijk geconcludeerd dat het van belang is dat gestandaardiseerde informatie-uitwisseling cruciaal is voor opschaling van e-health. De NVZ heeft een programma opgesteld om deze gestandaardiseerde informatie-uitwisseling te realiseren. Het vraagt van ziekenhuizen een forse investering om hieraan deel te nemen vanwege de complexe ICT-infrastructuur voor medische gegevens in ziekenhuizen. Er zijn veel verschillende afdelingen met veel verschillende soorten ICT-apparatuur. Ik heb besloten de ziekenhuizen te stimuleren om dit programma uit te voeren, zodat patiënten in 2020 daadwerkelijk over hun medische gegevens kunnen beschikken. De middelen voor VIPP zijn daarbij een onderdeel van de financiële afspraken met de sector voor medisch specialistische zorg.
Ik ben met de partijen in de eerste lijn in gesprek om gegevensuitwisseling onderling en met de patiënt te bevorderen. De opgave in deze sector wijkt af van de opgave in de medisch specialistische zorg. Enerzijds zijn de systemen anders en biedt de meerderheid van de huisartsen al de mogelijkheid tot inzage, anderzijds zijn de organisaties veel kleiner en kunnen zij de benodigde aanpassingen niet altijd zelf implementeren. In het addendum van het bestuurlijk akkoord huisartsenzorg en multidisciplinaire zorg 2018 is hierover het volgende opgenomen: In 2017 en 2018 zal worden onderzocht welke eHealthtoepassingen, procesinnovaties en gerichte investeringen nodig zijn om binnen de eerste lijn de patiënt meer regie te geven over zijn gezondheid, de zorgverleners in hun werk en in de onderlinge samenwerking te ondersteunen en substitutie mogelijk te maken.

De leden van de fractie van de **PvdD** vragen of het klopt dat bij de ontwikkeling van MedMij wordt uitgegaan van het LSP als de manier bij uitstek voor het opvragen van medicatiegegevens.
Deze veronderstelling is niet juist. De vervolgvraag over uitwisseling van gegevens als de patiënt geen toestemming geeft voor elektronische uitwisseling (daarbij verwijzend naar een EenVandaag item van 12 mei 2017) is eerder in deze brief in samenhang met een vraag van de leden van de fractie van de PVV beantwoord.
De missie van MedMij is het mogelijk maken dat iedere Nederlander die dat wil kan beschikken over een persoonlijke gezondheidsomgeving waarin zij hun gezondheidsgegevens kunnen verzamelen, delen en erover beschikken. MedMij stimuleert digitale uitwisseling van gezondheidsgegevens tussen patiënten en zorgverleners en creëert vertrouwen dat dit op een veilige, betrouwbare en gebruikersvriendelijke manier gebeurt. Daartoe is het eerste ontwerp van het MedMij-afsprakenstelsel opgeleverd. MedMij definieert de spelregels waar de uitwisseling aan moet voldoen, maar schrijft niet voor wie of wat die uitwisseling zou moeten uitvoeren.

Zoals hierboven aangegeven wordt het gebruik van het LSP met de subsidieregeling van het programma VIPP niet verplicht en kan de

elektronische gegevensuitwisseling ook, mits veilig, via andere systemen plaatsvinden. De regering laat dus – conform de motie Teunissen c.s. (33 509, T) waarnaar de leden van de **PvdD** twee maal verwijzen – ruimte aan systemen waarbij toestemmingen en autorisaties decentraal worden vastgelegd. In het rapport «Onderzoek zorg-infrastructuur» [25] van Nictiz dat in april 2017 naar de Tweede Kamer is gestuurd blijkt dat in de zorg daadwerkelijk van een breed scala aan infrastructuren voor gegevensuitwisseling gebruikt wordt gemaakt: landelijke en regionale infrastructuren en systemen voor specifieke vormen van samenwerking of ontstaan vanuit één specifieke toepassing.

De leden van de fractie van de **PvdD** vragen aan te geven waarom – conform motie Bredenoord c.s. (33 509, R) – dataprotectie-by-design niet expliciet vermeld staat in de VIPP-regeling.
Op basis van de Wbp ligt er al een verplichting voor zorginstellingen om zowel passende technische als ook organisatorische maatregelen te treffen. Onder die laatste valt ook het meenemen van de dergelijke design-principes. Daarnaast worden organisaties bij de implementatie van de AVG verplicht om de bescherming van persoonsgegevens vanaf het begin in het ontwerpproces van registraties of systemen mee te nemen. De VIPP-regeling is voornamelijk gericht op ontsluiting van informatie naar de patiënt, op zodanige wijze dat de gegevens ook elders in het zorgproces kunnen worden ingezet. Daarom zijn alleen extra eisen ten aanzien van veilige ontsluiting van de informatie opgenomen. Uiteraard geldt daarnaast dat alle geldende wet en regelgeving van toepassing is.

De leden van de **PvdD** vragen of en hoe privacy-by-design is toegepast in het LSP. De achterliggende overtuiging is dat het aansluiting op het LSP een subsidievoorwaarde is en het LSP als zodanig deel uitmaakt van het overheidsbeleid. Ik heb aangegeven dat deze veronderstelling niet juist is. Ik draag geen directe verantwoordelijkheid voor het LSP en ook niet voor enig ander systeem voor elektronische gegevensuitwisseling. De eisen die voortvloeien uit de wet en het onderhavige besluit gelden dus voor alle elektronische uitwisselingssystemen. De verwachting is dat als de verantwoordelijken voor elektronische uitwisselingssystemen de wet en het besluit naleven, privacy voldoende is geborgd.

De leden van de fractie van de **PvdD** vragen of het klopt dat het Informatieberaad de informatiestandaarden mag vaststellen en zo ja, of dat al gebeurd is en om welke standaarden het gaat.
Het Informatieberaad heeft geen zelfstandige bevoegdheid voor het nemen van besluiten, bijvoorbeeld ontleend aan een wettelijke taak of een instellingsbesluit. In een brief aan de Tweede Kamer (TK 2016–2017 27 529 nr. 142) schreef ik dat als de leden van het Informatieberaad standaarden vaststellen, dat betekent dat alle leden zich committeren aan het inzetten van de eigen instrumenten om de standaarden in de zorgpraktijk te laten werken.
Standaarden zijn geen doel op zich. Zij moeten toegevoegde waarde hebben voor de zorg als geheel. Om die reden wordt altijd gekeken of er voor een interoperabiliteitsvraagstuk al een internationale open standaard beschikbaar is, of deze de vrije keuze voor systemen en leveranciers bevordert en daadwerkelijk past in de Nederlandse zorgcontext. Veldnormen zijn leidend voor de interoperabiliteitsvraagstukken waar standaarden voor nodig kunnen zijn. Kandidaten voor vast te stellen standaarden komen uit het veld en volgen een uitgebreid proces met openbare consultatie, advies van experts alvorens de leden van het Beraad tot vaststelling overgaan.

---

[25] https://zoek.officielebekendmakingen.nl/kst-27529–148

Voor medicatie-uitwisseling heeft het Informatieberaad nog geen standaard vastgesteld. Wel is een aantal standaarden als kandidaat-standaard ingediend, die het consultatie-proces nog in moeten gaan.

Daarnaast vraagt de fractie van de PvdD waaruit de (democratische) legitimiteit van het Informatieberaad bestaat om standaarden te kiezen en vast te leggen voor de sector en in hoeverre het besluitvormingsproces binnen het Informatieberaad toegankelijk is voor partijen van buiten de zorg.
Zoals ik al in mijn vorige antwoord aangaf, is het Informatieberaad niets meer en niets minder dan een structureel overleg van partijen in de zorg, en heeft het geen eigenstandige bevoegdheid. Het werkt met het mandaat dat de leden zelf aan tafel meebrengen. Dat mandaat bestaat uit het mandaat dat de leden van de brancheorganisaties en koepels hun vertegenwoordigers in het Informatieberaad hebben gegeven, en niets meer dan dat. De leden van het Informatieberaad zetten de instrumenten die zij hebben in om de afspraken in de praktijk te laten werken. Bijvoorbeeld voorlichting, toezicht en handhaving en inkoopondersteuning. In de vergadering van 20 maart 2017 hebben de leden van het Informatieberaad bekrachtigd dat ze elk hun eigen instrumenten zullen inzetten om tot naleving van de gemaakte afspraken te komen.
De vergaderingen van het Informatieberaad zijn transparant en volledig openbaar, elke vergadering zitten tussen 60 en 80 geïnteresseerden uit allerlei geledingen in de zaal en kunnen zij de beraadslagingen live volgen. Op informatieberaadzorg.nl publiceert het de verslagen van de vergaderingen. Ik heb bewust gekozen voor deze open en transparante aanpak, omdat ik uw mening deel dat de onderwerpen die in de vergadering besproken worden veel partijen raken.

Ik hoop uw vragen hiermee afdoende te hebben beantwoord.

De Minister van Volksgezondheid, Welzijn en Sport,
E.I. Schippers