Vervolgonderzoek

Privacy bij Zorgverzekeraars

Opvolging van de verbeterpunten

Juli 2009

Inhoud

Vooraf

De Nederlandse Zorgautoriteit (NZa) heeft in april 2008 de nulmeting privacy gepubliceerd. De zorgverzekeraars is naar aanleiding van deze nulmeting gevraagd zich te verantwoorden over de opvolging van de verbeterpunten. In dit rapport wordt hierover gerapporteerd. De zorgverzekeraars hebben een individuele terugkoppeling over de opvolging van de verbeterpunten ontvangen.

Managementsamenvatting

Voor de verwerking van persoonsgegevens in het verzekeringsstelsel zijn de artikelen 87 van de Zorgverzekeringswet (Zvw), artikel 53 van de Algemene Wet Bijzondere Ziektekosten (AWBZ) en artikel 68a van de Wet marktordening gezondheidszorg (Wmg) van belang. Op basis van deze wetten en de Wet bescherming persoonsgegevens (Wbp) moeten zorgverzekeraars zodanige technische en organisatorische maatregelen treffen dat is gewaarborgd dat onbevoegden zonder toestemming van de verzekerde geen kennis kunnen nemen van (bijzondere) persoonsgegevens. Daarnaast kunnen die gegevens niet voor een ander doel dan de uitvoering van de betreffende verzekering of wet worden gebruikt.

Voor een zorgvuldige omgang met de door zorgverzekeraars ontvangen gegevens, is een gedragscode opgesteld. In de regeling zorgverzekering wordt verwezen naar deze gedragscode en bovendien wordt een verplichting tot naleving opgelegd. Echter, in februari 2008 is de goedkeurende verklaring van het College bescherming persoonsgegevens voor de gedragscode (Gedragscode Verwerking Persoonsgegevens Financiële Instellingen van de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars en het Addendum Zorgverzekeraars van Zorgverzekeraars Nederland) verlopen. Voor de nieuwe gedragscode (die ten tijde van het schrijven van dit rapport in procedure is ter verkrijging van een goedkeurende verklaring van het CBP) geldt dat deze geen addendum meer zal zijn op de gedragscode van de financiële instellingen. Doordat de termijn van de goedkeurende verklaring is vervallen en de procedure ter verkrijging van een goedkeurende verklaring voor een herziene versie nog niet is afgerond, heeft de NZa geen handhavingsbevoegdheden.

De NZa heeft in de tweede helft van 2007 een onderzoek (nulmeting) uitgevoerd naar de verwerking van persoonsgegevens door zorgverzekeraars. In april 2008 is het rapport met de bevindingen gepubliceerd. Dit eerste onderzoek leverde een divers beeld op van de verwerking van persoonsgegevens door zorgverzekeraars. Gezien de verbeterpunten die de zorgverzekeraars moesten doorvoeren, heeft de NZa eind 2008 en begin 2009 een vervolgonderzoek uitgevoerd naar de opvolging van de door de NZa gestelde verbeterpunten.

De zorgverzekeraars hebben zich uiterlijk 1 oktober 2008 verantwoord over de opvolging van de verbeterpunten. De NZa heeft de verantwoordingen van de zorgverzekeraars beoordeeld. Indien noodzakelijk zijn aanvullende vragen gesteld. De uitkomsten van de beoordelingen zijn individueel teruggekoppeld naar de zorgverzekeraars.

Uit het onderzoek naar de opvolging van de verbeterpunten is gebleken dat veel verbeterpunten door de zorgverzekeraars zijn opgevolgd. Wel geldt voor alle zorgverzekeraars dat zij of nog verbeterpunten hebben openstaan of de ingezette verbeteracties nog niet geheel hebben afgerond.

De nog openstaande of niet volledig opgevolgde verbeterpunten hebben voornamelijk betrekking op de onderwerpen: doelbinding, beleid omtrent rechten van betrokkenen; controle op naleving van procedures en maatregelen voor de beginselen van de Wbp; bewaartermijnen; procedure acceptatiebeleid; bepalingen materiële controle en fraudeonderzoeken in aanvullende verzekering.

Deze onderwerpen krijgen in het vervolg van het toezicht op de verwerking van persoonsgegevens bijzondere aandacht. Daarnaast blijkt er bij de verzekeraar nog veel onduidelijkheid te zijn naar het beginsel 'bewerker'. Ook zijn de taken en verantwoordelijkheden van de medisch adviseur van belang voor de waarborging van een zorgvuldige verwerking van persoonsgegevens. Ook deze onderwerpen krijgen bijzondere aandacht in het toezicht van de NZa.

De NZa gaat vanaf 2009 het toezicht op de verwerking van persoonsgegevens structureel vormgeven. Het structurele toezicht valt uiteen in een jaarlijkse review van één of meerdere zorgverzekeraars, onderzoeken naar bepaalde thema's binnen privacy, toezicht gebruik BSN in de zorg en signaaltoezicht.

1. Inleiding

1.1 Aanleiding

De Nederlandse Zorgautoriteit (NZa) heeft in de tweede helft van 2007 een onderzoek (nulmeting) uitgevoerd naar de verwerking van persoonsgegevens door zorgverzekeraars. In april 2008 is het rapport met de bevindingen gepubliceerd. Het onderzoek heeft een divers beeld opgeleverd van de verwerking van persoonsgegevens door zorgverzekeraars (zie paragraaf 1.4). Gezien de verbeterpunten die de zorgverzekeraars moesten doorvoeren, heeft de NZa eind 2008 en begin 2009 een vervolgonderzoek uitgevoerd naar de opvolging van de door de NZa gestelde verbeterpunten.

1.2 Wettelijk kader

Op grond van artikel 6 van de Wet bescherming persoonsgegevens (Wbp) moeten persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Dit geldt ongeacht er sprake is van bijzondere persoonsgegevens.

Voor de verwerking van persoonsgegevens in het verzekeringsstelsel zijn de artikelen 87 van de Zorgverzekeringswet (Zvw), artikel 53 van de Algemene Wet Bijzondere Ziektekosten (AWBZ) en artikel 68a van de Wet marktordening gezondheidszorg (Wmg) van belang. Op basis van de Zvw, AWBZ, Wmg en de Wbp zijn zorgverzekeraars gehouden tot de bouw van Chinese muren. Dat wil zeggen dat zorgverzekeraars zodanige technische en organisatorische maatregelen moeten treffen dat is gewaarborgd dat onbevoegden zonder toestemming van de verzekerde geen kennis kunnen nemen van (bijzondere) persoonsgegevens. Daarnaast kunnen die gegevens niet voor een ander doel dan de uitvoering van de betreffende verzekering of wet worden gebruikt.

Behalve een duidelijke regeling over de te verstrekken persoonsgegevens door zorgaanbieders aan zorgverzekeraars (hoofdstuk 7 *regeling zorgverzekering*[1]), wordt ook groot belang gehecht aan een zorgvuldige omgang met de door de zorgverzekeraar ontvangen gegevens. De door Zorgverzekeraars Nederland (ZN) ontwikkelde gedragscode geeft in dit kader regels. In de regeling zorgverzekering wordt verwezen naar de gedragscode en bovendien wordt een verplichting tot naleving opgelegd.

In februari 2008 is de goedkeurende verklaring van het College bescherming persoonsgegevens voor de gedragscode (Gedragscode Verwerking Persoonsgegevens Financiële Instellingen van de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars en het Addendum Zorgverzekeraars van Zorgverzekeraars Nederland) verlopen. Voor de nieuwe gedragscode (die ten tijde van het schrijven van dit rapport in procedure is ter verkrijging van een goedkeurende verklaring van het CBP) geldt dat deze geen addendum meer zal zijn op de gedragscode van de financiële instellingen.

[1] De regeling zorgverzekering is de ministeriële regeling behorende bij de Zorgverzekeringswet. Vooralsnog is er alleen een ministeriële regeling op de Zvw. De ministeriële regeling voor de AWBZ en Wmg zijn nog in ontwikkeling.

Doordat de termijn van de goedkeurende verklaring is vervallen en de procedure ter verkrijging van een goedkeurende verklaring voor een herziene versie nog niet is afgerond, heeft de NZa geen handhavingsbevoegdheden.

1.3 Definities

1.3.1 Verwerking van persoonsgegevens

In de Wbp is 'verwerking van persoonsgegevens' omschreven als: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in elk geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Ook in dit vervolgonderzoek wordt aangesloten bij deze definitie van verwerking van persoonsgegevens.

1.3.2 Zorgverzekeraars

In de Wmg is een 'ziektekostenverzekeraar' omschreven als: een zorgverzekeraar, een AWBZ–verzekeraar, een particuliere ziektekostenverzekeraar, zijnde een financiële onderneming die ingevolge de Wet op het financieel toezicht in Nederland het bedrijf van verzekeraar mag uitoefenen. In het Addendum Zorgverzekeraars wordt bij deze omschrijving de definitie 'zorgverzekeraar' gehanteerd. Aangezien dit thematisch onderzoek zich ook richt op het Addendum Zorgverzekeraars is voor de eenduidigheid aangesloten bij de definitie uit het Addendum.

In dit vervolgonderzoek verstaat de NZa onder zorgverzekeraar:

Een verzekeraar die zorgverzekeringen in de zin van de Zorgverzekeringswet of andere ziektekostenverzekeringen aanbiedt of uitvoert. Dit betekent dat hij de Zvw, de AWBZ en andere ziektekostenverzekeringen, met name aanvullende verzekeringen, kan uitvoeren.

1.4 Uitkomst nulmeting

Zoals in paragraaf 1.1 is beschreven, leverde de nulmeting naar de verwerking van persoonsgegevens door zorgverzekeraars een divers beeld op. In deze paragraaf worden de resultaten kort weergegeven.

Uit het onderzoek is gebleken dat de meerderheid van de zorgverzekeraars voor een groot aantal van de in dat onderzoek getoetste onderdelen aandacht besteedt aan de bepalingen uit de Wbp en het Addendum Zorgverzekeraars. Voor nagenoeg alle zorgverzekeraars geldt dat voor de Wbp het vastleggen van procedures voor gegevensverwerking en de controles op de naleving hiervan meer aandacht verdienen. Bij het Addendum zijn vooral verbeteringen nodig bij de bewaartermijnen van persoonsgegevens, het opnemen van bepalingen over materiële controle, misbruik en oneigenlijk gebruik in de aanvullende voorwaarden en de interne regeling. Daarnaast komen de verantwoordelijkheden van de medisch adviseur bij enkele

zorgverzekeraars niet overeen met hetgeen is bepaald in het Addendum. Ten slotte diende een aantal zorgverzekeraars hun aanmeldformulieren voor de basisverzekering aan te passen in verband met vragen rondom de strafrechtelijke gegevens.

De NZa heeft bij de terugkoppeling van de bevindingen naar de zorgverzekeraar verbeterpunten geformuleerd. De zorgverzekeraars moesten uiterlijk 1 juni 2008 verantwoording aan de NZa afleggen over de opvolging van de verbeterpunten met betrekking tot de aanmeldformulieren. De zorgverzekeraars waar dit verbeterpunt betrekking op had, hebben de aanmeldformulieren conform de gestelde eisen aangepast. Over de opvolging van de overige verbeterpunten moeten de zorgverzekeraars zich uiterlijk 1 oktober 2008 verantwoorden.

1.5 Doelstelling

De door de NZa geformuleerde verbeterpunten in de nulmeting dienden er voor om de opzet van de verwerking van persoonsgegevens bij zorgverzekeraars op een goed basisniveau te krijgen. In de nabije toekomst kan de NZa dan ook de werking van de geldende maatregelen en procedures worden onderzocht.

Doelstelling van dit vervolgonderzoek is dan ook vaststellen of en in hoeverre de zorgverzekeraars de door de NZa geformuleerde verbeterpunten uit de nulmeting hebben opgevolgd. In dit vervolgonderzoek blijft de werking van de geldende procedures en maatregelen vooralsnog buiten beschouwing. Dit is een logisch gevolg van het feit dat wanneer de NZa de werking van de geldende maatregelen en procedures wil controleren, deze eerst op een basisniveau moeten liggen. In de komende jaren gaat de NZa aandacht besteed aan de werking van de geldende maatregelen en procedures.

1.6 Algemeen consumentenbelang

De persoonsgegevens van verzekerden mogen in principe alleen worden gebruikt voor het doel waarvoor deze zijn verstrekt. Sommige gegevens, zoals gegevens omtrent gezondheid, moeten zodanig vertrouwelijk worden behandeld, dat ze uitsluitend worden vastgelegd door de persoon of afdeling die ze nodig heeft voor de uitvoering van de zorgverzekering en dat ze niet verder worden verspreid dan noodzakelijk. Dit follow-up onderzoek richt zich, eveneens als het eerste onderzoek, op de zorgvuldige behandeling van persoonsgegevens en dient daarmee het consumentenbelang.

1.7 Uitvoering vervolgonderzoek

De nulmeting is in 2007 uitgevoerd bij 32 zorgverzekeraars. Met ingang van 1 januari 2009 zijn 30 zorgverzekeraars actief op de zorgverzekeringsmarkt. Bij deze zorgverzekeraars is het vervolgonderzoek uitgevoerd.

Zoals eerder beschreven moesten de zorgverzekeraars zich uiterlijk 1 oktober 2008 verantwoorden over de opvolging van de verbeterpunten. Daarbij is de zorgverzekeraars gevraagd de opvolging te onderbouwen met nieuw opgestelde procedures, memo’s, beleidsnotities en eventueel overige stukken.

De NZa heeft de verantwoordingen van de zorgverzekeraars beoordeeld. Indien noodzakelijk heeft de NZa aanvullende vragen gesteld. De uitkomsten van de beoordelingen worden individueel teruggekoppeld naar de zorgverzekeraars.

1.8 Leeswijzer

In het tweede en derde hoofdstuk wordt de opvolging van de verbeterpunten beschreven van de beginselen van de Wbp en het Addendum Zorgverzekeraars. In het vierde hoofdstuk volgen de conclusies en het vervolg van het toezicht op de verwerking van persoonsgegevens door de NZa.

2. Wbp: regelgeving en resultaten

2.1 Inleiding

De Wbp stelt regels en voorwaarden aan de verwerking van persoonsgegevens door organisaties ter bescherming van de privacy van de betrokkenen. De algemene bepalingen van de Wbp zijn samen te vatten in zes beginselen:
- rechtmatige grondslag;
- doelbinding;
- transparantie;
- kwaliteit van de gegevens;
- beveiliging;
- bewaartermijnen.[2]

Verder zijn belangrijke onderdelen van de Wbp de melding, rechten van betrokkenen en bewerker. In de nulmeting zijn de beginselen en onderdelen van de Wbp uitgebreid beschreven. In dit rapport wordt dit beperkt tot de opvolging van de verbeterpunten bij de hoofdpunten uit de Wbp.

2.2 Inhoud Wbp

2.2.1 Melding

De zorgverzekeraar moet de verwerking van persoonsgegevens *melden* bij het CBP (artikel 27 lid 1 Wbp). Het doel van de melding van de gegevensverwerking is dat deze zorgt voor openheid en daarmee controleerbaarheid voor de betrokkenen, in dit geval de verzekerden.

Dertien zorgverzekeraars bleken geen procedure te hebben voor de melding van de verwerking van persoonsgegevens bij het CBP. Uit dit onderzoek blijkt dat tien zorgverzekeraars naar aanleiding van de verbeterpunten de procedure voor de melding op orde hebben. Twee zorgverzekeraars hebben dit verbeterpunt opgepakt, maar nog niet afgerond.

Wijzigingen in de melding moeten binnen een jaar na de voorafgaande melding worden doorgegeven voor zover deze van meer dan incidentele aard blijken te zijn (artikel 28 lid 3 Wbp). Dit hangt ermee samen dat de organisatie eens per jaar moet controleren of de gegevensverwerking nog overeenkomt met de voorafgaande melding.[3]

Uit de nulmeting bleek dat 24 zorgverzekeraars niet periodiek de juistheid van de melding beoordelen. Uit dit onderzoek blijkt dat 22 zorgverzekeraars de periodieke beoordeling van de juistheid van de melding op orde hebben. Een zorgverzekeraar heeft het verbeterpunt opgepakt, maar nog niet afgerond. Een zorgverzekeraar heeft dit verbeterpunt niet opgevolgd.

Naast de periodieke beoordeling van de juistheid van de melding, moet de zorgverzekeraar de juistheid ook beoordelen bij gelegenheid van wijziging in het verwerkingsproces. Hiervoor moesten negen zorgverzekeraars verbeteringen uitvoeren. Uit dit onderzoek blijkt dat

[2] Zie voor het beginsel bewaartermijnen paragraaf 3.2.6
[3] Memorie van Toelichting op de Wbp, pagina 139

vijf zorgverzekeraars het verbeterpunt hebben opgevolgd en drie hebben het opgepakt, maar nog niet afgerond.

Een zorgverzekeraar heeft het verbeterpunt meegekregen om de medewerkers informeren over de procedure over de melding van de verwerking van persoonsgegevens. Deze zorgverzekeraar heeft het verbeterpunt opgevolgd.

Naast het informeren van de medewerkers moet de zorgverzekeraar ook controles uitvoeren op de naleving van de procedures en maatregelen. Uit dit onderzoek blijkt dat zes zorgverzekeraars het verbeterpunt hebben opgevolgd. Vier zorgverzekeraar hebben het verbeterpunt opgepakt, maar nog niet afgerond. Een zorgverzekeraar heeft het verbeterpunt niet opgevolgd.

2.2.2 Transparantie

Bij transparantie gaat het erom dat de persoonsgegevens in overeenstemming met de wet, behoorlijk en zorgvuldig moeten worden verwerkt (artikel 6 Wbp).

Zes zorgverzekeraars moesten de procedures voor een transparante verwerking van persoonsgegevens verbeteren. Uit dit onderzoek blijkt dat vijf zorgverzekeraars dit verbeterpunt hebben opgevolgd en een heeft het opgepakt, maar nog niet afgerond.

Ook heeft de zorgverzekeraar een informatieplicht. Dit houdt in dat de zorgverzekeraar de verzekerde voorafgaande aan de verkrijging van de gegevens moet informeren over de identiteit van de organisatie en het doel waarvoor de gegevens worden verwerkt (artikel 33 Wbp).

De zorgverzekeraar die het verbeterpunt omtrent de informatieverplichting moest opvolgen, heeft dit opgevolgd.

Twaalf zorgverzekeraars moesten de controle op de naleving van de procedures voor de transparante gegevensverwerking moesten verbeteren. Uit dit onderzoek blijkt dat zeven zorgverzekeraars het verbeterpunt hebben opgevolgd en twee zorgverzekeraars niet. Drie zorgverzekeraars hebben het verbeterpunt opgepakt, maar nog niet afgerond.

2.2.3 Doelbinding

Doelbinding duidt erop dat het verzamelen en het verdere gebruik van persoonsgegevens mogelijk is voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7 Wbp). De verzamelde persoonsgegevens worden alleen verder verwerkt als dit verenigbaar is met het doel waarvoor ze zijn verkregen (artikel 9 Wbp). De zes zorgverzekeraars die verbeterpunten hebben meegekregen met betrekking tot de doelbinding, hebben dit verbeterpunt opgevolgd.

Achttien zorgverzekeraars moesten verbeteringen aanbrengen in de procedures om het verenigbaar gebruik van de gegevens vast te stellen. Factoren die een rol spelen bij de vaststelling of de verwerking verenigbaar is met het oorspronkelijke doel, zijn de *verwantschap* tussen het oorspronkelijke doel en het doel van de verdere verwerking, de *aard* van de betreffende gegevens, de *gevolgen* van de beoogde – verdere – verwerking voor de betrokkene en de *wijze* waarop de gegevens zijn verkregen en de mate waarin passende waarborgen voor de betrokkene zijn genomen.

Uit dit onderzoek blijkt dat dertien zorgverzekeraars dit verbeterpunt hebben opgevolgd en vijf zorgverzekeraars niet.

Voor het verwerken van persoonsgegevens voor historisch, statistisch en wetenschappelijk onderzoek geldt een bijzondere regeling. Deze verwerking wordt niet als onverenigbaar beschouwd op voorwaarde dat de verantwoordelijke de nodige voorzieningen heeft getroffen om te waarborgen dat de verdere verwerking uitsluitend geschiedt voor deze specifieke doeleinden. De uitkomsten van het historisch, statistisch en wetenschappelijk onderzoek moeten worden geanonimiseerd.

Tweederde van de zorgverzekeraars moesten procedures opstellen voor historisch, statistisch en wetenschappelijk onderzoek. Slechts vier zorgverzekeraars hebben, zo blijkt uit dit onderzoek, een dergelijke procedure opgesteld en vijf zorgverzekeraars hebben dit in ontwikkeling. De overige elf zorgverzekeraars hebben geen procedure opgesteld, omdat zij hiertoe niet de noodzaak zien. Ondanks dat de zorgverzekeraars op dit moment de gegevens niet voor deze doeleinden gebruiken, kan dit op termijn wel aan de orde zijn. Vooruitlopend hierop vindt de NZa het van belang dat zorgverzekeraars deze procedures wel opstellen.

Twee zorgverzekeraars hebben het verbeterpunt meegekregen om de medewerkers informeren over de procedure over de doelbinding van de verwerking van persoonsgegevens. Deze zorgverzekeraars hebben het verbeterpunt opgevolgd.

Naast het informeren van de medewerkers moet de zorgverzekeraar ook controles uitvoeren op de naleving van de doelbinding van de gegevensverwerking. Uit dit onderzoek blijkt dat zeven zorgverzekeraars het verbeterpunt hebben opgevolgd en vier hebben het opgepakt, maar nog niet afgerond. Een zorgverzekeraar heeft het verbeterpunt niet opgevolgd.

2.2.4 Rechtmatige grondslag

Voor het rechtmatig verwerken van persoonsgegevens is een grondslag nodig. Artikel 8 Wbp geeft limitatief aan in welke gevallen persoonsgegevens mogen worden verwerkt. Voor bijzondere persoonsgegevens geldt dat het verwerken verboden is tenzij aan specifieke voorwaarden is voldaan (artikel 16 Wbp).

De rechtmatige grondslag is voor zorgverzekeraars nader gedefinieerd in het Addendum. Voor het leveren van bepaalde diensten en/of producten is het noodzakelijk dat medische persoonsgegevens worden verwerkt (artikel 3.0.6 Addendum). In die situatie moeten deze gegevens strikt vertrouwelijk worden verwerkt. Dit mag uitsluitend gebeuren als dit noodzakelijk is voor de beoordeling van een te verzekeren risico en de verzekerde geen bezwaar heeft gemaakt, of als dit noodzakelijk is voor het uitvoeren van de verzekeringsovereenkomst of de AWBZ.

Acht zorgverzekeraars hebben het verbeterpunt meegekregen om procedures op te stellen om de rechtmatige grondslag voor de verwerking van gegevens vast te stellen. Uit dit onderzoek blijkt dat vier zorgverzekeraars dit verbeterpunt wel hebben opgevolgd en vier hebben dit niet gedaan.

Een zorgverzekeraar heeft het verbeterpunt meegekregen om de medewerkers informeren over de procedure voor het vaststellen van de

rechtmatige grondslag van de gegevensverwerking. Uit dit onderzoek blijkt dat deze zorgverzekeraar het verbeterpunt heeft opgevolgd.

Naast het informeren van de medewerkers moet de zorgverzekeraar ook controles uitvoeren op de naleving van de procedures om de rechtmatige grondslag voor de gegevensverwerking vast te stellen. Uit dit onderzoek blijkt dat zeven zorgverzekeraars het verbeterpunt hebben opgevolgd en twee hebben het opgepakt, maar nog niet afgerond. Twee zorgverzekeraars hebben het verbeterpunt niet opgevolgd.

2.2.5 Kwaliteit

Voor de verwerking van persoonsgegevens gelden bepaalde *kwaliteit*seisen. Persoonsgegevens worden voor een bepaald doel verzameld en verder verwerkt. Voor dat doel behoren de persoonsgegevens toereikend, ter zake dienend en niet bovenmatig te zijn (artikel 11 Wbp). Dit betekent onder meer dat niet méér gegevens mogen worden verzameld dan nodig is en dat de gegevens juist en nauwkeurig moeten zijn. De zorgverzekeraar moet maatregelen nemen om de juistheid van de gegevens te waarborgen en fouten in de invoer en verwerking te voorkomen.

Twee zorgverzekeraars hebben verbeterpunten meegekregen voor de procedures die de kwaliteit van de verwerking van persoonsgegevens waarborgt. Uit dit onderzoek blijkt dat één zorgverzekeraar dit verbeterpunt heeft opgevolgd, de andere zorgverzekeraar niet.

Een zorgverzekeraar moest de controle op de naleving van de procedures over de kwaliteit van de gegevensverwerking verbeteren. Deze zorgverzekeraar heeft, zo blijkt uit dit onderzoek, het verbeterpunt opgepakt, maar nog niet afgerond.

2.2.6 Rechten van de betrokkene

De betrokkene moet weten aan welke organisatie hij zijn gegevens verstrekt en voor welk doel deze gegevens worden verwerkt. Daarom heeft de zorgverzekeraar een informatieplicht (zie paragraaf 2.2.2). Daarnaast heeft de *betrokkene* het recht te verzoeken om inzage, verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens (artikel 5, 35–42 Wbp). Hierop gelden weer uitzonderingen (vooral artikel 43 Wbp) en het is aan de verantwoordelijke om te bepalen of aan het verzoek moet worden voldaan. De zorgverzekeraar moet hiervoor beleid en richtlijnen formuleren (artikel 3.10.1 Addendum). Voor het verkrijgen van inzage in een medisch dossier kan naast de Wbp ook de Wet op de geneeskundige behandelingsovereenkomst (WGBO) van toepassing zijn. Het recht van verzet houdt in dat een betrokkene het recht heeft bezwaar te maken (verzet aan te tekenen) tegen bepaalde vormen van gebruik van zijn gegevens door een organisatie.

Van de zeven zorgverzekeraars die geen beleid en/of richtlijnen voor het recht van de betrokkene hadden opgesteld, hebben drie zorgverzekeraars, zo blijkt uit dit onderzoek, het verbeterpunt opgevolgd en vier zorgverzekeraars niet.

De zorgverzekeraar moet ook controles uitvoeren op de naleving van het beleid en/of richtlijnen voor de rechten van de betrokkene. Uit dit onderzoek blijkt dat vijf zorgverzekeraars het verbeterpunt hebben opgevolgd en drie hebben het opgepakt, maar nog niet afgerond. Twee zorgverzekeraars hebben het verbeterpunt niet opgevolgd.

2.2.7 Beveiliging

De zorgverzekeraar moet zorgen voor passende organisatorische en technische maatregelen tegen verlies van gegevens en tegen iedere vorm van onrechtmatige verwerking (artikel 13 Wbp).

Technische maatregelen zijn de logische en fysieke maatregelen in en rondom de informatiesystemen, zoals toegangscontroles, vastlegging van gebruik en back–up. Bij *organisatorische maatregelen* gaat het om maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens, zoals toekenning en deling van verantwoordelijkheden en bevoegdheden, instructies, trainingen en calamiteitenplannen.

Bij de keuze van de te nemen technische en organisatorische maatregelen moet rekening worden gehouden met de *stand der techniek*, de *kosten* van tenuitvoerlegging en de *risico's* die de verwerking meebrengt (artikel 13 Wbp).[4] Bij het maken van een keuze dient de verantwoordelijke te zoeken naar een balans tussen de hiervoor genoemde criteria. Als op basis daarvan een gemotiveerde keuze is gemaakt, is er sprake van een stelsel van passende technische en organisatorische maatregelen.

Onderdelen van het beveiligingbeleid zijn het privacybewustzijn, beheer en toegangsbeveiliging, bewaren en vernietigen en calamiteitenplannen.

Een zorgverzekeraar moest de beveiliging bij datacommunicatie verbeteren. Deze zorgverzekeraar heeft, zo blijkt uit dit onderzoek, het verbeterpunt opgepakt.

wee zorgverzekeraars de controle op het beveiligingsbeleid moesten verbeteren. Een zorgverzekeraar heeft, zo blijkt uit dit onderzoek, dit verbeterpunt opgevolgd, de andere heeft het opgepakt maar nog niet afgerond.

2.2.8 Bewerker

Zorgverzekeraars kunnen de verwerking van persoonsgegevens geheel of gedeeltelijk uitbesteden aan opdrachtnemers. De Wbp noemt degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder dat diegene onder rechtstreeks gezag van de verantwoordelijke staat, de *bewerker* (artikel 1 sub e Wbp). Voor zorgverzekeraars betekent dit veelal dat Vektis en Vecozo bewerkers zijn.

In de nulmeting hebben de zorgverzekeraars geen individuele verbeterpunten meegekregen voor het onderwerp 'bewerker'.

2.3 Conclusie

In tabel 1 is een overzicht gegeven van de opvolging van de verbeterpunten. Hierin is aangegeven hoeveel zorgverzekeraars het verbeterpunt hebben opgevolgd (+), hoeveel zorgverzekeraars het niet hebben opgevolgd (-) en hoeveel zorgverzekeraars het hebben opgepakt, maar nog niet hebben afgerond (+/-).

[4] Zie voor een verdere uitleg van deze criteria het rapport 'Beveiliging van persoonsgegevens' van het CBP. Deze studie bevat een normatief kader hoe met name de 'exclusiviteit' van persoonsgegevens door maatregelen en procedures kan worden geborgd.

De zorgverzekeraars hebben de meeste verbeterpunten voldoende opgevolgd of hebben het verbeterpunt opgepakt, maar nog niet afgerond. Binnen het beginsel 'doelbinding' zijn twee verbeterpunten door veel zorgverzekeraars niet opgevolgd. Dit gaat om de procedure voor het vaststellen van verenigbaar gebruik van de persoonsgegevens en de procedure voor het gebruik van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden. De NZa kan naar dit onderwerp en de noodzaak van deze procedures een themaonderzoek uitvoeren.

Van de zorgverzekeraars die beleid en/of richtlijnen voor de rechten van betrokkenen moesten opstellen hebben vier zorgverzekeraars hieraan geen opvolging gegeven. Het beleid omtrent de rechten van de betrokkene is belangrijk in het licht van het consumentenbelang. Ook dit is een onderwerp dat de NZa bij een themaonderzoek nader kan onderzoeken.

Ook blijkt dat zorgverzekeraars verbeterpunten hebben meegekregen voor de controle naar de naleving van de procedures en maatregelen die de zorgverzekeraars hebben opgesteld voor de beginselen van de Wbp. Bij een aantal zorgverzekeraars is het verbeterpunt wel opgepakt, maar nog niet afgerond. De controles op de naleving van de procedures en maatregelen zijn belangrijk en geven mogelijk aanleiding om de procedures en maatregelen te herzien. Ook naar dit onderwerp kan de NZa een themaonderzoek instellen.

In de nulmeting hebben de zorgverzekeraars geen individuele verbeterpunten meegekregen voor het onderdeel 'bewerker'. Over dit begrip bestond te veel onduidelijkheid. Wel is in het samenvattende rapport aandacht besteed aan dit thema en zijn algemene verbeterpunten geformuleerd. Aangezien bij de zorgverzekeraars veel onduidelijkheid bestaat over 'de bewerker', zou dit ook een goed onderwerp voor een themaonderzoek zijn.

Tabel 1 Overzicht opvolging verbeterpunten beginselen Wbp

Verbeterpunten	+	-	+/-	n.v.t.
Melding				
*Procedure melding verwerking persoonsgegevens	10	-	2	18
*Periodieke beoordeling juistheid melding	20	1	1	8
*Beoordeling juistheid melding bij gelegenheid van wijziging in het verwerkingsproces	5	-	3	22
*Informeren medewerkers over de procedures van de melding	1	-	-	30
*Controle op naleving van de procedures	6	1	4	19
Transparantie				
*Procedures voor transparante gegevensverwerking	5	-	1	24
*Invulling aan de informatieverplichting	1	1	-	29
*Controle op naleving van procedures en informatieverplichting	7	2	3	18
Doelbinding				
*Maatregelen voor waarborging verwerking voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden	6	-	-	24
*Procedure voor vaststellen verenigbaar gebruik	13	5	-	12
*Procedure voor historische, statistische of wetenschappelijke doeleinden	4	11	5	10
*informeren medewerkers over doelbinding van verwerking persoonsgegevens	2	-	-	28
*Controle op naleving van de doelbinding van de verwerking van persoonsgegevens	7	1	4	18
Rechtmatige grondslag				
*Procedures voor vaststellen rechtmatige grondslag voor de gegevensverwerking	4	4	-	22
*Informeren medewerkers over rechtmatige grondslag van verwerking persoonsgegevens	1	-	-	29
*Controle op naleving van procedures over verwerking van persoonsgegevens op basis van rechtmatige grondslag	7	2	2	19
Kwaliteit				
*Procedures die de kwaliteit van de verwerking van persoonsgegevens waarborgt	1	1	-	28
*Controle op naleving van procedures over kwaliteit van gegevensverwerking	-	-	1	29
Rechten van betrokkene				
*Beleid en/of richtlijnen voor recht van betrokkene	3	4	-	23
*Controle op naleving van beleid en/of richtlijnen over recht van betrokkene	5	2	3	20
Beveiliging				
*Extra beveiligingsmaatregelen bij datacommunicatie m.b.t. persoonsgegevens	1	-	-	29
*Controle op naleving van beveiligingsbeleid persoonsgegevens	1	-	1	28

3. Addendum zorgverzekeraars

3.1 Inleiding

Het Addendum Zorgverzekeraars heeft betrekking op de verstrekking van persoonsgegevens van verzekerden aan zorgverzekeraars en op de zorgvuldige verwerking en beveiliging van de persoonsgegevens door zorgverzekeraars.

De goedkeurende verklaring van het CBP voor het Addendum Zorgverzekeraars horende bij de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen is verlopen op 5 februari 2008 (zie paragraaf 1.2)

Dit hoofdstuk belicht de opvolging van de verbeterpunten bij de hoofdlijnen van het Addendum behorende bij de Gedragscode.

3.2 Inhoud Addendum Zorgverzekeraars

3.2.1 Interne regeling

De zorgverzekeraar moet op grond van artikel 3.0.2 van het Addendum een interne regeling opstellen waarin is gespecificeerd welke medewerkers/functionarissen betrokken zijn bij de verwerking van persoonsgegevens voor de bepaalde doeleinden en over welke gegevens zij gelet op hun functie mogen beschikken. In de nieuwe gedragscode is niet meer bepaald dat de autorisatieschema's onderdeel moeten uitmaken van een interne regeling. Het verbeterpunt van de interne regeling is niet meer meegegeven aan de zorgverzekeraars. Wel moet de zorgverzekeraar natuurlijk beschikken over de autorisatieschema's.

Zeven zorgverzekeraars moesten verbeteringen aanbrengen in de autorisatieschema's van de medewerkers voor de verwerking van persoonsgegevens. Uit dit onderzoek blijkt dat twee zorgverzekeraars dit verbeterpunt hebben opgepakt. Daarnaast moesten dertien zorgverzekeraars in de autorisatieschema's opnemen voor welke doelen de medewerkers de gegevens verwerken. Dit verbeterpunt is, zo blijkt uit dit onderzoek, door acht zorgverzekeraars opgepakt. Tot slot moesten elf zorgverzekeraars in de autorisatieschema's opnemen over welke gegevens de medewerkers gelet op hun functie mogen beschikken. Uit dit onderzoek blijkt dat zes zorgverzekeraars dit hebben opgepakt. Voor de bovenstaande drie verbeterpunten geldt dat uit dit onderzoek blijkt dat vier zorgverzekeraars deze verbeterpunten wel hebben opgepakt maar nog niet hebben afgerond. Voor één zorgverzekeraar geldt dat de verbeterpunten niet voldoende zijn opgepakt.

3.2.2 Medisch adviseur

Het artikel waarin de verantwoordelijkheden van de medisch adviseur[5] zijn beschreven (artikel 3.0.3) is een belangrijk onderdeel van het Addendum. Het gaat om het medisch beroepsgeheim van de medisch adviseur. Daarnaast is het een zeer belangrijke waarborg voor een zorgvuldige verwerking van persoonsgegevens en voor het vertrouwen van verzekerden in een zorgvuldige omgang met hun persoonsgegevens door zorgverzekeraars. Het is daarom van belang dat de verantwoordelijkheden van de medisch adviseur overeen komt met hetgeen is bepaald in het Addendum. De medisch adviseur kan een deel van deze taken delegeren aan medewerkers van de zorgverzekeraar, de functionele eenheid. De medisch adviseur verstrekt hen slechts die medische persoonsgegevens die nodig zijn voor het verrichten van hun werkzaamheden.

Bij twee zorgverzekeraars kwamen de verantwoordelijkheden van de medisch adviseur niet overeen met het Addendum. Uit dit onderzoek blijkt dat beide zorgverzekeraars het verbeterpunt hebben opgepakt, maar bij één zorgverzekeraar is het traject nog niet afgerond.

Bij drie zorgverzekeraars vielen de processen genoemd in artikel 3.0.3 niet onder de verantwoordelijkheid van de medisch adviseur. Dit is inmiddels, zo blijkt uit dit onderzoek, bij twee van deze zorgverzekeraars wel het geval en de andere zorgverzekeraar is er nog mee bezig.

3.2.3 Acceptatie

Voor de vraag of de zorgverzekeraar een verzekeringsovereenkomst wil sluiten met een aspirant–verzekerde zijn verschillende gegevens nodig. Vanwege de wettelijke acceptatieplicht voor de zorgverzekering en de AWBZ–verzekering mag de zorgverzekeraar voor het afsluiten van deze verzekeringen geen medische persoonsgegevens opvragen. Ook mogen zorgverzekeraars voor de zorgverzekering en AWBZ–verzekering geen gegevens over het strafrechtelijke verleden worden opgevraagd (artikel 6.2 Gedragscode). Deze bijzondere persoonsgegevens mogen slechts worden opgevraagd voor beoordeling en acceptatie van de aspirant–verzekerde voor de aanvullende verzekering.

Hiervoor moesten acht zorgverzekeraars het aanmeldformulier aanpassen. Eén zorgverzekeraar moest het aanmeldformulier van de zorgverzekering zo aanpassen dat de gezondheidsvragen alleen moeten worden beantwoord als de verzekerde ook kiest voor een aanvullende verzekering. Uit dit onderzoek blijkt dat al deze zorgverzekeraars de verbeterpunten hebben opgevolgd.

Bij een keuringsonderzoek voor een aanvullende verzekering stelt de medisch adviseur de aspirant–verzekerde op grond van artikel 7:464 Burgerlijk Wetboek (BW) in de gelegenheid mee te delen of hij het – afwijkende – advies als eerste wenst in te zien om te beslissen of de

[5] Werkzaamheden waarbij sprake is van beoordeling, taxatie of interpretatie van medische persoonsgegevens worden verricht onder de verantwoordelijkheid van de medisch adviseur. Hieronder valt in elk geval de verwerking van medische persoonsgegevens die (artikel 3.0.3):
- ter verwerking bij derden worden opgevraagd, zoals ziekenhuizen;
- door of namens de verzekerde ter toelichting zijn verstrekt in het kader van de acceptatie voor de aanvullende verzekering;
- worden verkregen in verband met een verzoek gedaan door of namens de verzekerde om toestemming te krijgen voor het ontvangen van bepaalde zorg (machtigingen);
- worden opgenomen in het medisch dossier dat de medisch adviseur over de verzekerde heeft ingericht.

uitslag al dan niet aan de verzekeraar wordt doorgegeven. De verzekerde moet bovendien op de hoogte worden gesteld van de consequenties van een eventuele weigering. Negen zorgverzekeraars handelden niet volgens deze gedragsregel. Uit dit onderzoek blijkt dat zes zorgverzekeraars dit verbeterpunt hebben opgevolgd, maar drie zorgverzekeraars niet.

3.2.4 Machtiging en zorgbemiddeling

De zorgplicht legt zorgverzekeraars de plicht op tot het verstrekken van – vergoeding van – zorg uit de Zvw. In het kader van de verwerking van persoonsgegevens zijn hierbij machtigingen en zorgbemiddeling van belang. Binnen deze categorie waren geen verbeterpunten opgesteld voor de zorgverzekeraars.

3.2.5 Uitwisseling persoonsgegevens

Het Addendum bevat gedragsregels voor de verstrekking van gegevens van verzekerden (artikel 3.0.9). Uit de nulmeting is niet gebleken dat zorgverzekeraars in strijd handelen met de bepalingen uit dit artikel. Slechts één zorgverzekeraar moest bij de uitwisseling van medische persoonsgegevens tussen de zorgverzekering en de aanvullende verzekering een scheiding aanbrengen tussen de vastlegging van de gegevens voor de beide verzekeringen. Dit is, zo blijkt uit dit onderzoek, inmiddels gerealiseerd.

3.2.6 Bewaartermijnen

De Wbp regelt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de doeleinden waarvoor ze zijn verzameld of worden gebruikt (artikel 10 Wbp). De Wbp geeft dus geen concrete bewaartermijn voor persoonsgegevens. In bijvoorbeeld de Archiefwet en het BW zijn wel concrete bewaartermijnen voor persoonsgegevens vastgelegd. Bij het bewaren van persoonsgegevens moet de zorgverzekeraar rekening houden met al deze wetten. Voor zorgverzekeraars zijn in het Addendum gedragsregels opgenomen voor de bewaartermijnen van de verwerkte persoonsgegevens (artikel 3.0.7, 3.0.8 en 3.4). Voor de positie van de medisch adviseur en de termijn van bewaring van de in verband daarmee verzamelde gegevens is artikel 7:464 tweede lid BW (voor zover het gaat om handelingen als bedoeld in artikel 7:446 vierde lid BW) en/of artikel 7:464 eerste lid BW (overeenkomstige toepassing voor zover de aard van de rechtsbetrekking zich daartegen niet verzet) van belang. Uit deze artikelen volgt geen (vaste) bewaartermijn, maar moet de bewaartermijn worden gerelateerd aan het specifieke belang gemoeid met verzameling.

Als een verzekeringsovereenkomst niet tot stand komt mag de zorgverzekeraar de medische persoonsgegevens maximaal twaalf maanden bewaren gerekend vanaf het moment dat de gegevens zijn verstrekt. Negen zorgverzekeraars handelden niet volgens deze gedragsregel. Uit dit onderzoek blijkt dat zeven zorgverzekeraars dit hebben aangepast. Eén zorgverzekeraar heeft het wel opgepakt, maar is nog niet afgerond en één zorgverzekeraar heeft het niet opgepakt.

Na beëindiging van de verzekeringsovereenkomst mag de zorgverzekeraar de persoonsgegevens maximaal zeven jaar bewaren, gerekend vanaf het moment van beëindiging. Dit is de bewaartermijn die geldt op grond van artikel 2:10 BW en sluit aan bij artikel 86 Zvw. Twaalf zorgverzekeraars hielden zich niet aan deze bewaartermijn. Van deze verzekeraars hebben, zo blijkt uit dit onderzoek, vijf zorgverzekeraar de bewaartermijn in lijn gebracht met het Addendum. Zes zorgverzekeraars

hebben het verbeterpunt opgepakt, maar is nog niet afgerond. Eén zorgverzekeraar heeft het verbeterpunt niet opgepakt.

De zorgverzekeraar mag zelf een richtlijn opstellen voor het bewaren van naam–, adres– en woonplaats (NAW–)gegevens en geboortedata voor marketingdoeleinden na beëindiging van de verzekeringsovereenkomst. Zeven zorgverzekeraars hadden niet een dergelijke richtlijn opgesteld. Uit dit onderzoek blijkt dat twee zorgverzekeraars dit inmiddels wel hebben gedaan, één zorgverzekeraar is hier nog mee bezig en vier zorgverzekeraar hebben nog steeds geen richtlijn hiervoor.

Als de verzekerde niet wenst dat zijn NAW–gegevens, na beëindiging van de overeenkomst, voor marketingdoeleinden of charitatieve doeleinden worden gebruikt, kan hij recht van verzet aantekenen (artikel 41 Wbp) en moet de zorgverzekeraar hem uit het adressenbestand verwijderen. Eén zorgverzekeraar moest dit punt verbeteren. Deze heeft, zo blijkt uit dit onderzoek, het ook opgepakt, maar nog niet afgerond.

Gegevens over het betalingsgedrag van de verzekerde mogen niet langer worden bewaard dan vijf jaar (artikel 3.4). Deze termijn sluit aan bij de periode gedurende welke de zorgverzekeraar een verzekeringsplichtige voor de Zvw kan weigeren op grond van artikel 3 lid 4 sub b Zvw. Dit is het geval als de verzekerde bij de verzekeraar is geroyeerd wegens het niet betalen van de premie. Achttien zorgverzekeraars bewaarden deze gegevens niet volgens deze termijn. Uit dit onderzoek blijkt dat elf verzekeraars de termijn hebben aangepast, drie zorgverzekeraars zijn er nog mee bezig en vier hebben het niet aangepast.

3.2.7 Omschrijving zorg op nota's

Voor de uitvoering van de verzekeringsovereenkomst moet de verzekerde die schade lijdt, of diens wettelijk vertegenwoordiger, worden geïnformeerd over de afhandeling van de ingediende nota's. Bij de informatieverstrekking aan de verzekeringnemer laat de zorgverzekeraar onnodige gegevens over de gezondheid van andere verzekerden achterwege (artikel 3.2). De zorgverzekeraar die dit verbeterpunt moest oppakken heeft dat gedaan.

3.2.8 Misbruik en oneigenlijk gebruik

Het doel van materiële controle is om voldoende zekerheid te verkrijgen over de juistheid en doelmatigheid van de geleverde prestatie. Daarnaast kan het aanwijzingen voor oneigenlijk gebruik en/of fraude opleveren. In het Addendum (artikel 3.8 en 3.9) is bepaald dat de zorgverzekeraar in zijn polissen voor aanvullende verzekeringen opneemt dat materiële controle en fraudeonderzoek wordt verricht overeenkomstig hetgeen daarover voor de zorgverzekering bij of krachtens de Zvw is bepaald. Van de 30 zorgverzekeraars bleken 21 dit niet in hun voorwaarden van de aanvullende verzekering te hebben opgenomen. Uit dit onderzoek blijkt dat vijftien zorgverzekeraars dit voor 2009 wel hebben gedaan, maar zes zorgverzekeraars niet.

3.2.9 Klachten en geschillen

De zorgverzekeraar moet de verzekerde in kennis stellen over de afhandeling van eventuele klachten over de uitvoering van de Wbp, de Gedragscode en het Addendum (artikel 3.10.2). Drie zorgverzekeraars moesten dit verbeterpunt oppakken en hebben dit ook gedaan.

3.2.10 Overig gebruik persoonsgegevens

Om verzekerden de zorg waarvoor zij zich hebben verzekerd te kunnen aanbieden, moet de zorgverzekeraar voldoende zorg inkopen. De zorgverzekeraar moet daarvoor weten aan welke soort zorg behoefte zal zijn en om hoeveel zorg het gaat. Om de verzekering daarnaast betaalbaar te houden is een goede kostenbeheersing essentieel. Voor deze processen is informatie nodig, maar die hoeft niet op persoonsniveau bekend te zijn. Zorgverzekeraars mogen voor zorginkoop en voor schadelastbeheersing alleen informatie op geaggregeerd niveau – niet herleidbaar tot individuele personen – gebruiken. Ook mogen risicoprofielen van verzekerden op geaggregeerd niveau worden verwerkt voor de beoordeling van een aangemeld risico. Het is niet toegestaan om medische persoonsgegevens voor marketingdoeleinden te gebruiken. Gegevens over het betalingsgedrag van verzekerden mogen alleen worden gebruikt voor acceptatie, controle en in– en excasso.

Voor deze categorie waren geen verbeterpunten opgesteld voor de zorgverzekeraars.

3.3 Conclusie

In tabel 2 is een overzicht gegeven van de opvolging van de verbeterpunten. Hierin is aangegeven hoeveel zorgverzekeraars het verbeterpunt hebben opgevolgd (+), hoeveel zorgverzekeraars het niet hebben opgevolgd (-) en hoeveel zorgverzekeraars het hebben opgepakt, maar nog niet hebben afgerond (+/-).

De zorgverzekeraars hebben de meeste verbeterpunten voldoende opgevolgd of hebben het verbeterpunt opgepakt, maar nog niet afgerond. Veel zorgverzekeraars houden zich echter nog niet aan alle bewaartermijnen. De NZa kan naar dit onderwerp een themaonderzoek instellen.

Veel zorgverzekeraars hanteren geen acceptatiebeleid voor de aanvullende verzekering. Het is wel de verwachting dat dit de komende jaren toe zal nemen. Van de zorgverzekeraars die hun procedure bij een negatieve uitslag van een keuringsonderzoek moesten aanpassen, blijkt dat drie zorgverzekeraars nog niet handelen volgens de gedragsregels. Ook naar richtlijnen omtrent de verwerking van persoonsgegevens bij het acceptatiebeleid kan de NZa een themaonderzoek uitvoeren.

De zorgverzekeraars moeten in hun aanvullende voorwaarden de bepaling opnemen dat zij materiële controle en fraudeonderzoeken worden uitgevoerd conform hetgeen daarover is bepaald in de Zvw. Het blijkt dat in 2009 zes zorgverzekeraars deze bepaling niet hebben opgenomen. De NZa controleert in de aanvullende voorwaarden van 2010 nogmaals of de zorgverzekeraars deze bepaling hebben opgenomen.

Ondanks dat de taken en verantwoordelijkheden van de medisch adviseur overeen komen met het Addendum, is dit wel een belangrijk onderwerp voor een themaonderzoek. De medisch adviseur is namelijk een belangrijke factor in de zorgvuldige verwerking van persoonsgegevens.

Tabel 2 Overzicht opvolging verbeterpunten Addendum

	+	-	+/-	n.v.t.
Interne regeling				
*Interne regeling cf. art. 3.0.2	7	3	4	16
*Autorisatieschema van medewerkers voor verwerking van persoonsgegevens	2	1	4	23
*In autorisatieschema opgenomen voor welke doelen	8	1	4	17
*In autorisatieschema opgenomen welke gegevens	6	1	4	19
Medisch adviseur				
*Verantwoordelijkheid en processen medisch adviseur cf. art. 3.0.3	1	-	1	28
*De processen vallen cf. art. 3.0.3 onder verantwoordelijkheid medisch adviseur	2	-	1	37
Acceptatie				
*Procedure bij negatieve uitslag voor acceptatie AV is cf. art. 3.6.1	6	3	-	21
Uitwisseling persoonsgegevens				
*Uitwisseling medische persoonsgegevens tussen zorgverzekering - AV v.v. cf. art. 3.0.9 c/d	1	-	-	29
Bewaartermijnen				
*Bij niet tot stand komen verzekering bewaartermijn medische persoonsgegevens cf. art. 3.0.7	7	1	1	21
*Na beëindiging verzekering bewaartermijn medische persoonsgegevens cf. art. 3.0.8	5	1	6	18
*Richtlijn voor bewaren van NAW-gegevens na beëindiging	2	4	1	23
*Recht van verzet voor gebruik NAW-gegevens voor marketingdoeleinden	-	-	1	29
*Bewaartermijn gegevens over betalingsgedrag van verzekerden cf. art. 3.4	11	4	3	12
Materiële controle & Misbruik/Oneigenlijk gebruik				
*Bepaling in AV cf. art. 3.8.1 en 3.9.1	15	6	-	9
Omschrijving zorg op nota's				
*Omschrijving op nota's cf. art. 3.2.1	1	-	-	29
Klachten en geschillen				
*Informatie over wijze van afhandeling klachten over uitvoering Wbp, Gedragscode, Addendum	3	-	-	27
*Verstrekken gegevens aan geschilleninstantie of rechter cf. art. 3.11.2	1	-	-	29
Aanmeldformulieren				
*Geen gezondheidsvragen bij afsluiten van zorgverzekering				
*Geen vragen over het strafrechtelijk verleden bij afsluiten van zorgverzekering				

4. Conclusies en acties NZa

4.1 Inleiding

In dit hoofdstuk volgen de conclusies van het onderzoek naar de opvolging van de verbeterpunten die de zorgverzekeraars hebben meegekregen naar aanleiding van de nulmeting in 2007. Daarnaast volgen de vervolgacties van de NZa op het gebied van het toezicht op de verwerking van persoonsgegevens door zorgverzekeraars.

Vanaf februari 2008 is de goedkeurende verklaring van het CBP voor de Gedragscode en bijbehorend Addendum Zorgverzekeraars verlopen. Dit betekent dat, omdat de gedragscode is opgenomen in de regeling zorgverzekering, de NZa geen bevoegdheden heeft ten aanzien van de verwerking van persoonsgegevens voor zover opgenomen in deze gedragscode. De NZa kan, wanneer de zorgverzekeraars de verbeterpunten niet hebben opgevolgd, niet handhavend optreden.

4.2 Conclusies

Uit het onderzoek naar de opvolging van de verbeterpunten is gebleken dat veel verbeterpunten door de zorgverzekeraars zijn opgevolgd. Wel geldt voor alle zorgverzekeraars dat zij of nog verbeterpunten hebben openstaan of de ingezette verbeteracties nog niet hebben afgerond. De nog openstaande of niet volledig opgevolgde verbeterpunten hebben voornamelijk betrekking op de volgende onderwerpen:

- doelbinding: procedure voor vaststellen van verenigbaar gebruik en het gebruik van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden;
- beleid omtrent rechten van betrokkenen;
- controle op naleving van procedures en maatregelen voor de beginselen van de Wbp;
- bewaartermijnen;
- procedure acceptatiebeleid;
- bepalingen materiële controle en fraudeonderzoeken in aanvullende verzekering.

Deze onderwerpen moeten in het vervolg van het toezicht op de verwerking van persoonsgegevens bijzondere aandacht krijgen. Daarnaast blijkt er bij de verzekeraar nog veel onduidelijkheid te zijn naar het beginsel ‘bewerker’. Ook zijn de taken en verantwoordelijkheden van de medisch adviseur van belang voor de waarborging van een zorgvuldige verwerking van persoonsgegevens. Ook deze onderwerpen hebben bijzondere aandacht nodig in het toezicht van de NZa.

4.3 Vervolg toezicht privacy

De NZa gaat vanaf 2009 het toezicht op de verwerking van persoonsgegevens structureel vormgeven. Het structurele toezicht valt uiteen in de volgende activiteiten:

- jaarlijkse review van één of meerdere zorgverzekeraars;
- onderzoeken naar bepaalde thema’s binnen privacy;
- toezicht gebruik BSN in de zorg;
- signaaltoezicht.