Thematisch onderzoek

Nederlandse Zorgautoriteit

Privacy bij Zorgverzekeraars

Onderzoek naar de verwerking van persoonsgegevens door zorgverzekeraars

Thematisch onderzoek

Privacy bij Zorgverzekeraars

Onderzoek naar de verwerking van persoonsgegevens door zorgverzekeraars

april 2008

Inhoud

Vooraf

Zorgverzekeraars verwerken voor de uitvoering van hun werkzaamheden persoonsgegevens, waaronder medische persoonsgegevens. Op grond van de Zorgverzekeringswet (Zvw), de Algemene Wet Bijzondere Ziektekosten (AWBZ) en de Wet bescherming persoonsgegevens (Wbp) zijn zorgverzekeraars ertoe gehouden om de zorgvuldige verwerking van deze persoonsgegevens te waarborgen.

De Nederlandse Zorgautoriteit (NZa) houdt toezicht op de rechtmatige uitvoering van de Zvw. Daaronder valt ook het toezicht op de verwerking van persoonsgegevens onder de Zvw. De NZa en het College bescherming persoonsgegevens (CBP) hebben een protocol opgesteld waarin de samenwerking tussen beide partijen is geregeld.

Voor het toezicht op de verwerking van persoonsgegevens onder de Zvw heeft de NZa inventariserend onderzoek gedaan bij zorgverzekeraars.[1] De uitkomsten van dit onderzoek bieden inzicht in de organisatorische en technische maatregelen die zorgverzekeraars hebben getroffen voor de verwerking van persoonsgegevens, hoe deze maatregelen worden gewaarborgd en of deze voldoen aan wet– en regelgeving. Verder geeft het onderzoek inzicht in hoeverre zorgverzekeraars de naleving van het Addendum Zorgverzekeraars organisatorisch hebben geborgd.

Ten tijde van de uitvoering van het onderzoek was het toezicht van de NZa op de verwerking van persoonsgegevens op grond van de Wet marktordening gezondheidszorg (Wmg) beperkt tot de Zvw. Voor dit onderzoek heeft daarom de medewerking van de zorgverzekeraars voor de aanvullende verzekering en de AWBZ op basis van vrijwilligheid plaatsgevonden. Door wijziging van de Wmg en de AWBZ heeft de NZa vanaf medio december 2007 ook toezicht– en handhavingstaken op het gebied van de verwerking van persoonsgegevens in de aanvullende verzekering en de AWBZ.

Naar aanleiding van de uitkomsten doet de NZa aanbevelingen aan de zorgverzekeraars en voert vervolgonderzoek uit op onderdelen. De uitkomsten van dit onderzoek zal de NZa ook gebruiken bij haar verdere toezicht op de verwerking van persoonsgegevens door zorgverzekeraars.

Voor dit onderzoek maakte de NZa intensief gebruik van reeds beschikbare informatie, aangevuld met een vragenlijst en interviews onder zorgverzekeraars.

de Raad van Bestuur van de Nederlandse Zorgautoriteit,

mw. drs. C.C. van Beek MCM
portefeuillehouder Zorgmarkten Cure

mr. F.H.G. de Grave
voorzitter

[1] Zie voor de definitie van 'zorgverzekeraar' in dit thematisch onderzoek paragraaf 1.2.1

Managementsamenvatting

Het verwerken van persoonsgegevens is onlosmakelijk verbonden met de activiteiten die zorgverzekeraars uitvoeren. Behalve persoonsgegevens zoals naam, adres en woonplaats, gaat het ook om – gevoelige – medische persoonsgegevens. Zorgverzekeraars moeten deze persoonsgegevens zorgvuldig verwerken. Daarvoor zijn waarborgen opgenomen in de Zorgverzekeringswet (Zvw), de Algemene Wet Bijzondere Ziektekosten (AWBZ) en de Wet bescherming persoonsgegevens (Wbp).[2] Daarnaast speelt het Addendum Zorgverzekeraars hierbij een relevante rol. De Nederlandse Zorgautoriteit (NZa) vindt het belangrijk dat zorgverzekeraars persoonsgegevens adequaat verwerken omdat dit de positie van de consument raakt en kan schaden wanneer de verwerking niet juist geschiedt.

In haar werk stelt de NZa het algemeen consumentenbelang (ACB) voorop. De instrumenten die de NZa hiervoor gebruikt, hebben in de eerste plaats betrekking op het vergroten van de zelfredzaamheid van de verzekerde. Onderdeel hiervan is het verbeteren van de rechtspositie van de consument. Dit speelt een grote rol in dit thematisch onderzoek. De consument is zich onvoldoende bewust van zijn rechten die voortkomen uit wet– en regelgeving. Voor het vertrouwen van de consument is het belangrijk dat er prudent wordt omgegaan met zijn privacy.

De NZa houdt toezicht op de rechtmatige uitvoering van de Zvw. Hieronder valt ook het toezicht op de verwerking van persoonsgegevens onder de Zvw. Daartoe heeft de NZa een inventariserend onderzoek verricht naar de verwerking van persoonsgegevens door zorgverzekeraars. In dit onderzoek is gekeken naar de organisatorische en technische maatregelen voor gegevensverwerking bij zorgverzekeraars, hoe deze maatregelen worden geborgd en of deze voldoen aan wet– en regelgeving. Daarnaast is gekeken in hoeverre zorgverzekeraars handelen conform het Addendum Zorgverzekeraars.

De NZa en het College bescherming persoonsgegevens (CBP) hebben een protocol opgesteld waarin de samenwerking tussen beide partijen is geregeld voor een effectieve en efficiënte uitvoering van het toezicht op de verwerking van persoonsgegevens door zorgverzekeraars. Het doel van het protocol is tweeledig. Ten eerste om tot een verdeling te komen van het toezicht daar waar sprake is van een samenloop in taken en bevoegdheden. Ten tweede om elkaar die informatie te verschaffen die van belang kan zijn voor de handhavingsactiviteiten van de ander. In gevallen van wederzijds belang stemmen beide partijen met elkaar af met het oog op een goede en efficiënte handhaving.

De goedkeurende verklaring van het CBP voor de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen en het bijbehorende Addendum Zorgverzekeraars is verlopen op 5 februari 2008. Ten tijde van het schrijven van dit rapport mogen de zorgverzekeraars hierdoor voor de materiële controles geen medische dossiers bij zorgaanbieders inzien zonder uitdrukkelijke toestemming van de verzekerde. De NVB, het VvV en ZN streven ernaar de

[2] Het toezicht van de NZa op de verwerking van persoonsgegevens was ten tijde van het onderzoek beperkt tot de Zvw. Medio december 2007 zijn de Wmg en de AWBZ aangepast. Hierdoor heeft de NZa ook toezicht- en handhavingstaken op het gebied van de verwerking van persoonsgegevens in de aanvullende verzekering en de AWBZ.

geactualiseerde Gedragscode en bijbehorend Addendum uiterlijk 1 juli 2008 aan het CBP voor te leggen. Naar verwachting blijven de uitgangspunten van de Gedragscode en het Addendum ongewijzigd.

Dit onderzoek is uitgevoerd via deskresearch, aangevuld met een vragenlijst onder zorgverzekeraars op grond waarvan interviews zijn gehouden. De resultaten en conclusies zijn gebaseerd op de informatie en antwoorden die zorgverzekeraars hebben verstrekt. De feitelijke naleving van de regels is als zodanig niet door de NZa gecontroleerd.

Het onderzoek levert een divers beeld op van de verwerking van persoonsgegevens door zorgverzekeraars. De meerderheid van de zorgverzekeraars besteedt voor een groot aantal van de getoetste onderdelen aandacht aan de bepalingen uit de Wbp en het Addendum. Er zijn – afgaande op de door de zorgverzekeraars gegeven antwoorden – geen indicaties dat medische persoonsgegevens onzorgvuldig worden verwerkt. Dit neemt niet weg dat belangrijke verbeteringen op een aantal punten nodig zijn. Voor de Wbp geldt voor nagenoeg alle zorgverzekeraars dat het vastleggen van procedures voor gegevensverwerking en de controles op de naleving hiervan aandacht verdienen. Bij het Addendum zijn vooral verbeteringen nodig bij de bewaartermijnen van persoonsgegevens en het opnemen van bepalingen omtrent materiële controle en misbruik en oneigenlijk gebruik in de aanvullende voorwaarden. Ook komen de verantwoordelijkheden van de medisch adviseur bij enkele zorgverzekeraars niet overeen met hetgeen is bepaald in het Addendum.

Wet bescherming persoonsgegevens (Wbp)
Van de getoetste onderdelen uit de Wbp, zoals melding, rechtmatige grondslag, doelbinding, transparantie, kwaliteit, rechten van de betrokkene, beveiliging en bewerker, scoren zorgverzekeraars het beste op de onderdelen kwaliteit van gegevensverwerking en beveiliging. Meer dan 90% van de zorgverzekeraars bevindt zich op deze aspecten op het gewenste niveau. Dit houdt in dat de zorgverzekeraar procedures en maatregelen heeft getroffen om een adequate verwerking van persoonsgegevens te waarborgen, deze procedures en maatregelen bekend zijn binnen de organisatie en de naleving hiervan wordt gecontroleerd. Bij de beveiliging moet worden opgemerkt dat gegeven de toenemende relevantie van informatie– en communicatietechnologie en de hieraan verbonden technische en organisatorische bedreigingen het nodig is dat de zorgverzekeraar regelmatig het beveiligingsbeleid evalueert en zonodig herziet.

Bij slechts dertien zorgverzekeraars (41%) ligt de gegevensverwerking op *alle* onderdelen op het gewenste niveau. Meer dan de helft van de Nederlands ingezetenen – meer dan tien miljoen verzekerden – is bij deze zorgverzekeraars verzekerd. Zes van deze zorgverzekeraars – twee concerns – hebben een functionaris voor gegevensverwerking aangesteld. Dit heeft een positief effect op de organisatie van de gegevensverwerking.

Bij de overige zorgverzekeraars (59%) ligt de verwerking van persoonsgegevens bij één of meer onderdelen niet op het gewenste niveau. Dit betekent dat voor deze onderdelen geen procedures en maatregelen zijn vastgelegd en geen controles plaatsvinden.

Nagenoeg alle zorgverzekeraars dienen aandacht te schenken aan het vastleggen van procedures voor gegevensverwerking en het uitvoeren van controles. Vaak zijn er wel *algemene* procedures en controles aanwezig waarmee privacyaspecten worden geraakt. Toch is het

belangrijk om procedures en *structurele* controles in te voeren die *specifiek* zijn gericht op de verwerking van persoonsgegevens. Slechts een enkele zorgverzekeraar controleert jaarlijks het geheel van verwerkingsmaatregelen en –procedures.

Addendum Zorgverzekeraars
De zorgverzekeraars hebben in grote lijnen de getoetste bepalingen uit het Addendum geborgd. Geen enkele zorgverzekeraar voldoet echter aan alle bepalingen uit het Addendum. Mogelijk hangt dit samen met het invoeringsmoment van het Addendum in 2006, in combinatie met de strekking ervan. Het Addendum is tegelijkertijd met de Zvw ingevoerd en vergt van zorgverzekeraars geen ingrijpende organisatorische aanpassing. Verbeteringen zijn vooral nodig bij de bewaartermijnen van persoonsgegevens en bij – het opnemen van – de bepalingen omtrent materiële controle en misbruik en oneigenlijk gebruik in de aanvullende voorwaarden.

De verantwoordelijkheden van de medisch adviseur komen bij enkele zorgverzekeraars niet overeen met hetgeen is bepaald in het Addendum. Dit is echter wel van belang, aangezien het gaat om het medisch beroepsgeheim van de medisch adviseur. Verder 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.

Ongeveer een kwart van de zorgverzekeraars geeft aan geen beleid of richtlijnen te hebben voor het recht van de betrokkene op inzage, correctie, afscherming of verwijdering van zijn persoonsgegevens. De NZa vindt het belangrijk dat zorgverzekeraars een dergelijk beleid hebben omdat dit direct de positie van de verzekerde raakt.

Een derde van de zorgverzekeraars voert geen acceptatiebeleid voor de aanvullende verzekering. Hierdoor is een aantal bepalingen uit het Addendum niet van toepassing. Dit impliceert dat als zorgverzekeraars de komende jaren wel acceptatievoorwaarden gaan stellen het huidige algemene beeld ten aanzien van het Addendum sterk kan wijzigen. De zorgverzekeraars die wel een acceptatiebeleid hanteren, geven aan vrijwel alle bepalingen hierover uit het Addendum in acht te nemen.

Zorgverzekeraars mogen voor de acceptatie van aspirant–verzekerden voor de zorgverzekering geen medische persoonsgegevens en gegevens over het strafrechterlijk verleden van de aspirant–verzekerde opvragen. Op één na houden de zorgverzekeraars zich hieraan en stellen op het aanmeldformulier geen gezondheidsvragen voor de acceptatie van de zorgverzekering. Wel stelt een beperkt aantal zorgverzekeraars (zeven) vragen over het strafrechterlijk verleden, waarbij niet is aangegeven dat deze uitsluitend moeten worden ingevuld voor het afsluiten van een aanvullende verzekering. Deze zorgverzekeraars moeten hun aanmeldformulieren aanpassen.

Verschillen tussen grote en kleine zorgverzekeraars
Tussen de vijf grootste zorgverzekeraars (> 1.000.000 verzekerden) en de vijf kleinste zorgverzekeraars (< 150.000 verzekerden) bestaan vooral verschillen in de verwerking van persoonsgegevens op de aspecten controle, medisch adviseur en klachtafhandeling. De grote zorgverzekeraars doen het op deze punten beter dan de kleine zorgverzekeraars. De grote zorgverzekeraars voeren vaker controles uit op de geldende procedures en maatregelen dan de kleine zorgverzekeraars. Ook de verantwoordelijkheden van de medisch adviseur en de processen die onder zijn verantwoordelijkheid vallen, komen bij de grote zorgverzekeraars beter overeen met het Addendum

dan bij de kleine zorgverzekeraars. Daarnaast scoren de grote zorgverzekeraars beter bij het informeren van verzekerden over de afhandeling van klachten over de Wbp, de Gedragscode en het Addendum.

Verschillen verzekeraars met en zonder relatie met hypotheken en levens– en pensioenverzekeringen
Tussen zorgverzekeraars die wel en die geen relatie hebben met hypotheekverstrekkers en aanbieders van levens– en/of pensioenverzekeringen bestaan vooral verschillen in de grondslagen van de Wbp. De zorgverzekeraars waarbij deze relatie aanwezig is scoren beter op de controle op een transparante verwerking en de vastlegging en controle met betrekking tot de doelbinding, rechtmatige grondslag en rechten van de betrokkene. Ook is er vaker een interne regeling op grond van artikel 3.0.2 van het Addendum.

Aanbevelingen
Hoewel zorgverzekeraars aandacht besteden aan het privacybewustzijn van de medewerkers dienen de zorgverzekeraars de medewerkers beter te informeren over procedures en maatregelen voor de verwerking van persoonsgegevens.

Het verdient aanbeveling dat zorgverzekeraars structurele controles, specifiek gericht op privacy invoeren om de naleving van maatregelen en procedures te toetsen. Dit kan bijvoorbeeld in de vorm van een jaarlijkse privacy audit.

Zorgverzekeraars dienen voor zichzelf helder te krijgen in hoeverre zij gebruik maken van 'bewerkers'. Uit het onderzoek is gebleken dat er bij zorgverzekeraars onduidelijkheid bestaat over het begrip bewerker uit de Wbp. Ook dient aandacht uit te gaan naar de controle op het beveiligingsniveau bij de bewerker.

Het is van belang dat zorgverzekeraars de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen en het bijbehorende Addendum Zorgverzekeraars langs hun organisatie leggen om te bepalen waar (organisatorische) aanpassingen nodig zijn. In elk geval dienen de bepalingen over de bewaartermijnen en het opnemen van bepalingen omtrent materiële controle en misbruik en oneigenlijk gebruik in de aanvullende voorwaarden goed te worden nagelopen.

Als zorgverzekeraars – verdere – acceptatievoorwaarden voor de aanvullende verzekering gaan invoeren moeten zij hierbij rekening houden met de bepalingen uit het Addendum.

Vervolgactiviteiten
De NZa heeft bij de terugkoppeling van de bevindingen naar de zorgverzekeraar verbeterpunten geformuleerd. De zorgverzekeraars moeten uiterlijk 1 juni 2008 verantwoording aan de NZa afleggen over de opvolging van de verbeterpunten met betrekking tot de aanmeldformulieren. Over de opvolging van de overige verbeterpunten moeten de zorgverzekeraars zich uiterlijk 1 oktober 2008 verantwoorden. De NZa zal scherp toezien op de opvolging van de verbeterpunten en hierover in 2009 rapporteren.

Daarnaast monitort de NZa de ontwikkelingen in de verwerking van persoonsgegevens via de maatschappelijk verslagen van de zorgverzekeraars en door signaaltoezicht.

1. Inleiding

1.1 Aanleiding

In het ziektekostenverzekeringssysteem en het declaratieverkeer is het verwerken van persoonsgegevens onontbeerlijk. Het gaat behalve om persoonsgegevens zoals naam, adres en woonplaats (NAW–gegevens), ook om – zeer gevoelige – medische persoonsgegevens. Medische persoonsgegevens behoren tot de hoogste categorie van gevoeligheid en vinden in het recht bijzondere bescherming. In het kader van de privacywetgeving staat voorop dat de verwerking van persoonsgegevens over iemands gezondheid door zorgverzekeraars is toegestaan voor zover dit noodzakelijk is voor de beoordeling van het te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt of voor de uitvoering van de verzekeringsovereenkomst. Een verzekeringsovereenkomst is een zorgverzekering, een aanvullende verzekering en een AWBZ–verzekering. Verder kan een ontheffing op het verbod om bijzondere persoonsgegevens te verwerken gelden als de betrokkene uitdrukkelijke toestemming heeft gegeven. Of wanneer de verwerking noodzakelijk is met het oog op een zwaarwegend algemeen belang en er in het belang van de persoonlijke levenssfeer passende waarborgen worden gecreëerd.

De Nederlandse Zorgautoriteit (NZa) houdt toezicht op de rechtmatige uitvoering van de Zorgverzekeringswet (Zvw). Hieronder valt ook het toezicht op de verwerking van persoonsgegevens onder de Zvw. Om invulling te geven aan deze wettelijke toezichtstaak heeft de NZa in de tweede helft van 2007 onderzoek verricht naar de verwerking van persoonsgegevens door zorgverzekeraars. Dit onderzoek heeft het karakter van een nulmeting en dient om een eerste beeld te krijgen van de verwerking van persoonsgegevens door zorgverzekeraars. De resultaten en conclusies zijn gebaseerd op de informatie en antwoorden die zorgverzekeraars hebben verstrekt. De NZa heeft de feitelijke naleving van de regels als zodanig niet gecontroleerd. Bij de interpretatie van de resultaten en conclusies dient hiermee rekening te worden gehouden. Op grond van de resultaten formuleert de NZa verbeterpunten voor de individuele zorgverzekeraar. De NZa zal scherp toezien op de opvolging van de verbeterpunten.

Het toezicht van de NZa op de verwerking van persoonsgegevens was ten tijde van het onderzoek beperkt tot de Zvw. Medio december 2007 zijn de Wet marktordening gezondheidszorg (Wmg) en de Algemene Wet Bijzondere Ziektekosten (AWBZ) aangepast. Door deze wijzigingen heeft de NZa ook toezicht– en handhavingstaken op het gebied van de verwerking van persoonsgegevens in de aanvullende verzekering en de AWBZ. Gezien de wettelijke bevoegdheden van de NZa ten tijde van de uitvoering van het onderzoek is door de zorgverzekeraars voor de aanvullende verzekeringen en de AWBZ medewerking verleend op vrijwillige basis.

Het thematisch onderzoek is uitgevoerd onder alle 32 zorgverzekeraars. Daarvan bieden er 30 tevens aanvullende verzekeringen aan en voeren 13 zorgverzekeraars ook de AWBZ uit (32 zorgkantoren). De peildatum van het onderzoek is september 2007. De resultaten weerspiegelen de situatie op dat moment. Waar het gaat om polisvoorwaarden en aanmeldformulieren is gekeken naar de situatie voor 2008.

1.2 Verwerking persoonsgegevens door zorgverzekeraars

1.2.1 Verwerking van persoonsgegevens

In de Wet bescherming persoonsgegevens (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.

In dit thematisch onderzoek wordt aangesloten bij deze definitie van verwerking van persoonsgegevens.

1.2.2 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 thematisch onderzoek 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.

1.3 Doelstellingen

Het doel van dit thematisch onderzoek is om inzicht te krijgen in de organisatorische en technische maatregelen die zorgverzekeraars treffen voor de verwerking van persoonsgegevens, hoe de zorgverzekeraars deze maatregelen waarborgen en of de getroffen maatregelen voldoen aan wet– en regelgeving. Kortom, kunnen de zorgverzekeraars een zorgvuldige verwerking van de (medische) persoonsgegevens van de verzekerden waarborgen? Voor dit deel van het onderzoek is gekozen voor een systeembenadering. De onderwerpen worden op basis van verschillende toetspunten beoordeeld.

Verder geeft het onderzoek inzicht in hoeverre zorgverzekeraars handelen conform de bepalingen in het Addendum Zorgverzekeraars. De naleving van de getroffen maatregelen en het onderdeel van het Addendum "Protocol Materiële Controle", valt buiten de reikwijdte van dit thematisch onderzoek. Voor dit deel van het onderzoek is per bepaling

uit het Addendum bekeken in hoeverre de zorgverzekeraars de naleving organisatorisch hebben geborgd.[3]
Gezien het verschillende karakter van de beide onderdelen trekt de NZa zowel conclusies voor het onderdeel over de Wbp als voor het Addendum.

Op basis van de uitkomsten van dit thematisch onderzoek definieert de NZa risico's voor het RisicoAnalyseModel betreffende de verwerking van persoonsgegevens door zorgverzekeraars.[4] Hierdoor ontstaat een kader voor verder toezicht van de NZa op de verwerking van persoonsgegevens bij zorgverzekeraars. Voorbeelden hiervan zijn signaaltoezicht en eventuele vervolgonderzoeken.

1.4 Algemeen Consumentenbelang

De NZa stelt in haar werk het algemeen consumentenbelang (ACB) voorop. De instrumenten die de NZa hiervoor gebruikt hebben in de eerste plaats betrekking op het vergroten van de zelfredzaamheid van de verzekerde. Onderdeel hiervan is het verbeteren van de rechtspositie van de consument. Dit speelt een grote rol in dit thematisch onderzoek. De consument is zich onvoldoende bewust van zijn rechten die voortkomen uit wet– en regelgeving. Voor het vertrouwen van de consument is het belangrijk dat er prudent wordt omgegaan met zijn privacy. De geldende regels dienen door de zorgverzekeraars strikt te worden nageleefd. Dit versterkt de rechtspositie van de consument.

1.5 Uitvoering onderzoek

Het onderzoek is langs drie lijnen uitgevoerd:
– vragenlijst zorgverzekeraars;
– interview zorgverzekeraars;
– deskresearch.

Onder alle 32 zorgverzekeraars is een vragenlijst uitgezet in de periode juli tot september 2007. Zij konden de vragenlijst digitaal invullen om de medewerking aan het onderzoek te vergemakkelijken en de administratieve lasten van het onderzoek te beperken. De vragenlijst bestond uit vragen over de Wbp en over het Addendum Zorgverzekeraars. De vragen over de Wbp zijn afgeleid van de audit–producten van het College bescherming persoonsgegevens (CBP). Aan de zorgverzekeraars is gevraagd de vragen te beantwoorden en zo mogelijk te onderbouwen met geldende procedures.

Naar aanleiding van de vragenlijsten zijn interviews gehouden met de zorgverzekeraars. In een enkel geval was de aard en omvang van de bespreekpunten zodanig beperkt dat resterende openstaande punten schriftelijk zijn afgehandeld in plaats van door een interview. De bevindingen uit de vragenlijsten heeft de NZa teruggekoppeld aan de individuele zorgverzekeraars. Op basis van deze bevindingen heeft de NZa tevens voor alle zorgverzekeraars afzonderlijk een aantal verbeterpunten geformuleerd en deze aan hen gecommuniceerd. De zorgverzekeraars moeten zich uiterlijk 1 juni 2008 verantwoorden over de opvolging van de verbeterpunten met betrekking tot de aanmeldformulieren. Over de opvolging van de overige verbeterpunten

[3] Dit protocol heeft betrekking op de wijze waarop de materiële controle van declaraties plaats dient te vinden. De naleving van dit protocol wordt al bij andere onderzoeken van de NZa betrokken.
[4] Voor een nadere uitleg over het RisicoAnalyseModel van de NZa zie www.nza.nl

moeten de zorgverzekeraars zich uiterlijk 1 oktober 2008 verantwoorden.

Om de administratieve lasten bij de zorgverzekeraars zoveel mogelijk te beperken, heeft de NZa voor dit thematisch onderzoek zoveel mogelijk gebruik gemaakt van bestaande informatie. Hierbij moet worden gedacht aan polisvoorwaarden, aanmeldformulieren, informatie op de websites van de zorgverzekeraars en uitvoeringsverslagen.

De informatie uit de vragenlijst, het interview en de reeds bestaande informatie is geanalyseerd en de bevindingen worden in dit rapport gepresenteerd.

1.6 Leeswijzer

Hoofdstuk twee behandelt het toezichtskader voor dit thematisch onderzoek. Ook is in dit hoofdstuk aandacht besteed aan de afbakening van het toezicht op de verwerking van persoonsgegevens tussen de NZa en het CBP. In het derde hoofdstuk staat de Wbp centraal en in het vierde hoofdstuk het Addendum Zorgverzekeraars. In zowel het derde als het vierde hoofdstuk is de wet– en regelgeving beschreven, waarna de resultaten uit het onderzoek worden gepresenteerd. Het rapport wordt afgesloten met de conclusies en aanbevelingen (hoofdstuk vijf).

2. Toezichtskader

2.1 Wettelijk kader

Op grond van artikel 6 van de Wbp moeten persoonsgegevens, inclusief bijzondere persoonsgegevens, in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. [5] Het is verboden om persoonsgegevens betreffende iemands gezondheid (hierna: medische persoonsgegevens) te verwerken (artikel 16 Wbp), tenzij aan specifieke voorwaarden is voldaan. De Wbp kent een ruime opvatting van het begrip 'gezondheid'. Het gaat niet alleen om gegevens die in het kader van een medisch onderzoek of behandeling door een arts worden verwerkt, maar om alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen.

Uitzonderingsbepalingen op het verbod in artikel 16 Wbp staan in de artikelen 21 en 23 Wbp. Artikel 87 van de Zvw biedt een wettelijke basis voor het gebruik van persoonsgegevens bij de uitvoering van de Zvw en de zorgverzekering. Hoofdstuk 7 van de regeling zorgverzekering biedt helderheid over de door zorgaanbieders aan zorgverzekeraars of verzekerden te verstrekken gegevens en over het noodzakelijkheidcriterium.[6] Zo mogen zorgverzekeraars in het kader van de Zvw medische persoonsgegevens verwerken voor zover dit noodzakelijk is voor de uitvoering van de verzekeringsovereenkomst.[7] Verder biedt de regeling helderheid over de doelen die met de verstrekking van persoonsgegevens worden gediend.

Op basis van de Zvw en de Wbp zijn zorgverzekeraars gehouden tot de bouw van de zogenaamde Chinese muren.[8] 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. Ook mogen 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, wordt ook groot belang gehecht aan een zorgvuldige omgang met de door de zorgverzekeraar ontvangen gegevens. Zorgverzekeraars Nederland (ZN) heeft hiervoor een gedragscode ontwikkeld. De regeling zorgverzekering verwijst naar deze gedragscode en legt bovendien de verplichting tot naleving op. Deze gedragscode is uitgewerkt en vormgegeven als een Addendum op de bestaande Gedragscode Verwerking Persoonsgegevens Financiële Instellingen (hierna: Gedragscode) van de Nederlandse Vereniging van Banken (NVB) en het Verbond van Verzekeraars (VvV).

Het Addendum Zorgverzekeraars (hierna: Addendum) heeft betrekking op de verstrekking van persoonsgegevens van verzekerden aan

---

[5] Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke gezindheid, godsdienst of levensovertuiging en strafrechtelijke gegevens. Bij persoonsgegevens is te denken aan naam, adres, geslacht etc.
[6] De regeling zorgverzekering is de ministeriële regeling behorende bij de Zvw.
[7] Voor de uitvoering van de aanvullende verzekeringsovereenkomst mogen zorgverzekeraars de gegevens ook verwerken voor zover dat noodzakelijk is voor de beoordeling van het te verzekeren risico en de verzekerde geen bezwaar heeft gemaakt.
[8] Vanaf medio december 2007 ook op basis van de Wmg en de AWBZ.

zorgverzekeraars en op de zorgvuldige verwerking en beveiliging van de persoonsgegevens waarover de zorgverzekeraars de beschikking krijgen.

De goedkeurende verklaring van het CBP voor de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen en het bijbehorende Addendum Zorgverzekeraars is verlopen op 5 februari 2008. Op 19 februari maakte het CBP bekend dat de zorgverzekeraars voor de materiële controles hierdoor geen medische dossiers bij zorgaanbieders mogen inzien zonder uitdrukkelijke toestemming van de verzekerde. Hiervoor bestaat geen grondslag meer. Ten tijde van het schrijven van dit rapport zijn de NVB, het VvV en ZN de Gedragscode en bijbehorend Addendum aan het actualiseren. Het CBP heeft in dat kader expliciete aandacht van ZN gevraagd voor de problemen bij de GGZ–declaraties. ZN streeft ernaar het geactualiseerde Addendum uiterlijk 1 juli 2008 aan het CBP voor te leggen. Naar verwachting blijven de uitgangspunten van de Gedragscode en het Addendum ongewijzigd.

2.1.1 Het CBP

Het CBP ziet sinds 1 september 2001 toe op de naleving van de Wbp. Wanneer een organisatie zich niet houdt aan de wet, kan het CBP maatregelen nemen. Eén daarvan is uitoefening van bestuursdwang zoals neergelegd in artikel 65 Wbp. Dat betekent dat het CBP van de overtreder kan eisen dat hij de overtreding van de wettelijke regels binnen een bepaalde termijn ongedaan maakt. Daarnaast kan het CBP een last onder dwangsom opleggen (artikel 5:32 lid 1 Algemene Wet Bestuursrecht (Awb)). Het CBP kan slechts in bepaalde gevallen een boete opleggen, bijvoorbeeld wanneer de verwerking van persoonsgegevens niet, onjuist of te laat is gemeld.

Het CBP hanteert een tweedelijn strategie. De privacybescherming moet vooral door het veld zelf worden gerealiseerd. Het CBP heeft hiertoe een aantal audit–producten ontwikkeld voor zelfonderzoek.[9]

2.1.2 De NZa

De NZa is volgens artikel 16 onder b Wmg belast met het toezicht op de rechtmatige uitvoering door de zorgverzekeraars van hetgeen bij of krachtens de Zvw is geregeld. De regeling zorgverzekering verwijst naar het Addendum. In het Addendum is vervolgens opgenomen dat de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen voor de zorgverzekeraars van toepassing is (artikel 3.0.1 Addendum). Deze gedragscode bevat onder andere de beginselen van de Wbp.

Doordat in de regeling zorgverzekering het Addendum verplicht is gesteld, strekt het toezicht van de NZa zich uit tot het Addendum voor zover dat past binnen de toezichtstaken die aan de NZa in artikel 16 onder b Wmg zijn opgedragen. De NZa kan de bepalingen in de Zvw over de verwerking van persoonsgegevens bestuursrechtelijk handhaven door middel van een last onder dwangsom en/of een bestuurlijke boete (artikel 83 respectievelijk artikel 89 Wmg).

Ten tijde van de uitvoering van het onderzoek was het toezicht van de NZa op de verwerking van persoonsgegevens beperkt tot de Zvw (zie paragraaf 1.1).

[9] Quickscan, WBP Zelfevaluatie, Raamwerk Privacy Audit (www.cbpweb.nl)

2.1.3 Afbakening toezicht NZa/CBP

Er is een protocol NZa/CBP opgesteld waarin de samenwerking tussen beide partijen is geregeld voor een effectieve en efficiënte uitvoering van het toezicht op de verwerking van persoonsgegevens door zorgverzekeraars.[10] Het doel van het protocol is tweeledig. Ten eerste om tot een verdeling te komen van het toezicht daar waar sprake is van een samenloop in taken en bevoegdheden. Ten tweede om elkaar die informatie te verschaffen die van belang kan zijn voor de handhavingsactiviteiten van de ander. In gevallen van wederzijds belang stemmen beide partijen met elkaar af met het oog op een goede en efficiënte handhaving. Zowel de NZa als het CBP blijven te allen tijde bevoegd gebruik te maken van hun eigen handhavingsmogelijkheden.

In het protocol is de volgende taakverdeling tussen NZa en CBP vastgelegd:

- voor klachten van burgers over de verwerking van persoonsgegevens is het CBP het eerste aanspreekpunt;
- als één van beide toezichthouders bij de uitoefening van zijn taken een vermoedelijke overtreding constateert van normen op de naleving waarvan slechts de andere toezichthouder toeziet, neemt hij hierover zo spoedig mogelijk contact op met de andere toezichthouder, onder verstrekking van de informatie waaruit de vermoedelijke overtreding blijkt;
- als één van beide toezichthouders bij de uitoefening van zijn taken een vermoedelijke overtreding constateert van normen op de naleving waarvan beide toezichthouders toezien, zodat sprake is van samenloop, stemmen de toezichthouders gezamenlijk af welke toezichthouder het meest geschikt is om op te treden tegen de vermoedelijke overtreding;
- als de toezichthouder, die op grond van lid 3 van het protocol is aangewezen om daadwerkelijk toezicht uit te oefenen, besluit niet op te treden, dan wel als zodanig optreden niet op een redelijke termijn plaatsvindt, kan de andere toezichthouder besluiten in dit geval alsnog zelf op te treden.

Tevens zijn in het protocol bepalingen opgenomen ten aanzien van het uitvoeren van zelfstandig onderzoek door één van de toezichthouders:

- de toezichthouders informeren elkaar in het kader van de beleidscyclus tijdig en in elk geval jaarlijks over voorgenomen onderzoeken waarbij sprake is van samenloop, zodat eventuele wensen van de andere toezichthouder kunnen worden meegenomen in het onderzoek;
- de toezichthouders informeren elkaar indien mogelijk vooraf maar in ieder geval zo spoedig mogelijk over ad hoc onderzoeken waarbij sprake is van samenloop, zodat eventuele wensen van de andere toezichthouder kunnen worden meegenomen in het onderzoek;
- de beslissing of de wensen van de andere toezichthouder worden meegenomen in een onderzoek, wordt genomen door de toezichthouder die de verantwoordelijkheid voor het betreffende onderzoek draagt;
- indien en voor zover sprake is van samenloop, kan de ene toezichthouder de andere toezichthouder verzoeken hem op basis van de eigen deskundigheid te assisteren bij het voorbereiden en/of uitvoeren van een onderzoek dat door hem zelfstandig wordt uitgevoerd.

[10] Zie www.nza.nl

3. Wbp: regelgeving en resultaten

3.1 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.[11]

Verder zijn belangrijke onderdelen van de Wbp de melding, rechten van betrokkenen en bewerker. Deze beginselen en onderdelen zijn ook opgenomen in gedragsregels in de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.

Dit hoofdstuk belicht de hoofdpunten uit de Wbp (paragraaf 3.2), de inrichting van een organisatie (paragraaf 3.3) en de onderzoeksresultaten op deze punten (paragraaf 3.4). Om de borging van de eisen uit de Wbp bij zorgverzekeraars te toetsen zijn in de vragenlijsten de hiervoor genoemde beginselen en onderdelen van de Wbp opgenomen.

3.2 Inhoud Wbp

3.2.1 Melding

De zorgverzekeraar moet de verwerking van persoonsgegevens *melden* bij het CBP (artikel 27 lid 1 Wbp) of een functionaris voor de gegevensbescherming aanstellen (artikel 62 Wbp). In dit laatste geval doet de organisatie melding van de verwerking van persoonsgegevens bij de functionaris voor de gegevensbescherming in plaats van bij het CBP.[12] 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.[13]

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. De melding stelt hen in staat om zo nodig gebruik te maken van hun rechten. Ook maken de meldingen een effectiever toezicht door het CBP mogelijk omdat zij via de meldingen kan controleren of een verantwoordelijke overeenkomstig de vooraf geformuleerde doeleinden gegevens verwerkt.[14]

[11] Zie voor het beginsel bewaartermijnen paragraaf 4.2.3 en 4.3.4
[12] Tenzij een voorafgaand onderzoek wordt aangevraagd of door het CBP wordt ingesteld.
[13] Memorie van Toelichting op de Wbp, pagina 139
[14] Informatieblad CBP, nummer 13, april 2004: Melden en vrijstellingen

3.2.2 Rechtmatige grondslag, doelbinding, transparantie, kwaliteit

Persoonsgegevens mogen uitsluitend voor bepaalde *doelen* worden verzameld en voor de verwerking is een *grondslag* nodig. Als persoonsgegevens worden verwerkt moet dit zorgvuldig gebeuren en moet de verzekerde van de verwerking op de hoogte worden gebracht (*transparantie*). Daarnaast moet de verwerking van persoonsgegevens voldoen aan *kwaliteit*seisen. De onderdelen doelbinding, rechtmatige grondslag, transparantie en kwaliteit hangen dan ook nauw met elkaar samen.

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.

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). 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. In artikel 4.2 en 4.4 van de Gedragscode zijn gedragsregels opgenomen omtrent de doelbinding.

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.

Bij *transparantie* gaat het erom dat de persoonsgegevens in overeenstemming met de wet, behoorlijk en zorgvuldig moeten worden verwerkt (artikel 6 Wbp). 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). Een zorgverzekeraar verkrijgt bijvoorbeeld persoonsgegevens van de betrokkene zelf als bij het aangaan van een verzekeringsovereenkomst op een formulier persoonsgegevens moeten worden ingevuld. De zorgverzekeraar kan dan via het aanmeldformulier voldoen aan zijn informatieplicht. Als de

betrokkene via de website van de zorgverzekeraar zijn gegevens invult, kan de zorgverzekeraar verwijzen naar het privacystatement waarin de zorgverzekeraar aangeeft hoe hij omgaat met persoonsgegevens.

Als de gegevens niet rechtstreeks van de verzekerde worden verkregen moet de zorgverzekeraar de betrokkene informeren op het moment van de vastlegging van zijn gegevens of wanneer de gegevens bestemd zijn om aan een derde te worden verstrekt (artikel 34 Wbp).[15] Als het om een grote groep gaat, bijvoorbeeld het gehele verzekerdenbestand, mag de zorgverzekeraar de betrokkenen algemeen informeren. De zorgverzekeraar moet er wel rekening mee houden dat iedereen van de groep wordt bereikt. De bepalingen omtrent transparantie zijn als gedragsregels opgenomen in de artikelen 4.1 en 4.6 tot en met 4.8 van de Gedragscode.

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. In de Gedragscode zijn gedragsregels omtrent de kwaliteit opgenomen in artikel 4.5.

3.2.3 Rechten van 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 3.2.2). 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. Artikel 7 van de Gedragscode bevat hiervoor gedragsregels en op grond van het Addendum zal de zorgverzekeraar hiervoor beleid en richtlijnen formuleren (artikel 3.10.1 Addendum).

Een betrokkene heeft het recht om inzage te verzoeken in zijn gegevens en het gebruik daarvan door een organisatie. Als de betrokkene hierom verzoekt, moet de organisatie binnen vier weken een overzicht van de gegevens verstrekken. Hij moet ook informatie verstrekken over het doel van de verwerking(en), de ontvangers van de gegevens en, indien beschikbaar, de herkomst van de gegevens. Voor het verkrijgen van inzage in een medisch dossier kan naast de Wbp ook de Wet op de geneeskundige behandelingsovereenkomst (WGBO) van toepassing zijn.

Op basis van de inzage in zijn gegevens kan de betrokkene de organisatie verzoeken de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dat kan als de gegevens die de organisatie gebruikt feitelijk onjuist, onvolledig of niet ter zake dienend zijn voor het doel of de doeleinden van de verwerking. Ook hier moet de organisatie binnen vier weken reageren op het verzoek van de betrokkene.

Het recht van verzet houdt in dat een betrokkene het recht heeft bezwaar te maken (verzet aan te tekenen) tegen bepaalde vormen van

[15] Op het moment van eerste verstrekking.

gebruik van zijn gegevens door een organisatie. Als een betrokkene verzet aantekent tegen het gebruik van zijn gegevens voor direct marketingdoeleinden moet de organisatie dit gebruik altijd meteen beëindigen. Een organisatie die persoonsgegevens gebruikt voor direct marketingdoeleinden moet een betrokkene informeren over het recht van verzet.[16]

3.2.4 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). Een ontoereikende beveiliging van persoonsgegevens kan ongewenste gevolgen hebben voor de persoonlijke levenssfeer van één of meer betrokkenen. In artikel 8.3 van de Gedragscode zijn voor de beveiliging van persoonsgegevens ook gedragsregels opgenomen.

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).[17] 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.

3.2.4.1 Privacybewustzijn

Informatiebeveiliging is alleen effectief als medewerkers de beveiligingsmaatregelen daadwerkelijk uitvoeren. Om dit te bereiken moet de zorgverzekeraar aandacht besteden aan het privacy– en beveiligingsbewustzijn van de medewerkers. Dit moet continu gebeuren, zowel bij indiensttreding van medewerkers als bij de dagelijkse functie–uitoefening door bestaande medewerkers. Uiteraard moeten alle medewerkers regelmatig op de hoogte worden gehouden over de procedures en maatregelen voor de informatiebeveiliging.

3.2.4.2 Beheer en toegangsbeveiliging

Zorgverzekeraars moeten maatregelen nemen en procedures hebben om te voorkomen dat onbevoegden toegang krijgen tot locaties, informatiesystemen en gegevensbestanden. Bij het transporteren van persoonsgegevens via computer– of telefoonnetwerken binnen de organisatie of met externe partijen, ontstaat een belangrijk beveiligingsrisico. Het is mogelijk dat de gegevens tijdens het transport in handen komen van onbevoegden of dat gegevens worden gewijzigd. Bij bijvoorbeeld gebruik van het internet ontstaat een extra risico. Bij

[16] Informatieblad CBP, nummer 12 februari 2007: Rechten van de betrokkene
[17] 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.

ontoereikende beveiliging kan van buitenaf het informatiesysteem worden binnengedrongen, met risico voor de integriteit van persoonsgegevens die zich daarin bevinden.

3.2.4.3 Bewaren en vernietigen

Persoonsgegevens kunnen worden bewaard op verschillende gegevensdragers, zoals papieren dossiers, elektromagnetische media of optische media. Deze gegevensdragers moeten veilig worden bewaard. Wanneer persoonsgegevens niet meer worden gebruikt, moeten ze zorgvuldig worden vernietigd. In het Addendum zijn specifieke bewaartermijnen bepaald. Hierop wordt in paragraaf 4.2.3 nader ingegaan.

3.2.4.4 Calamiteitenplannen

Calamiteiten, zoals brand, ernstige computerstoringen en waterschade, kunnen de continuïteit van de bedrijfsvoering verstoren en ernstige gevolgen hebben voor de in de organisatie aanwezige persoonsgegevens. Iedere organisatie moet een calamiteitenplan hebben waarin precies staat beschreven hoe moet worden opgetreden bij calamiteiten. Het plan heeft echter alleen effect als het bij de medewerkers bekend is en regelmatig wordt geoefend. Bij een calamiteitenplan hoort ook een procedure waarin staat hoe na een calamiteit de gegevensverwerking weer op gang wordt gebracht.

3.2.5 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. Als een persoon ondergeschikt of anderszins in een hiërarchische verhouding of onder rechtstreeks gezag staat van de verantwoordelijke, dan is diegene geen bewerker, maar is sprake van – intern – beheer.

De Wbp stelt eisen aan de vorm en inhoud van de afspraken die de verantwoordelijke met de bewerker maakt:

- de verantwoordelijke moet zekerheid verkrijgen dat de bewerker voldoende waarborgen biedt voor de technische en organisatorische beveiliging;
- de verantwoordelijke moet een overeenkomst met de bewerker sluiten of een andere regeling treffen waardoor afdwingbare verbintenissen ontstaan tussen de verantwoordelijke en de bewerker;
- de verantwoordelijke moet in de overeenkomst – of andere regeling – opnemen dat de bewerker de persoonsgegevens uitsluitend verwerkt in zijn opdracht;
- de verantwoordelijke moet ook bedingen dat de bewerker de beveiligingsverplichtingen nakomt die op de verantwoordelijke rusten op grond van de Wbp;
- de verantwoordelijke moet daadwerkelijk toezien op de naleving van deze beveiligingsverplichtingen. Ook het recht daartoe zal de verantwoordelijke in de overeenkomst (of andere regelingen) moeten opnemen.

Als de bewerker gegevens verwerkt, heeft diegene te maken met verplichtingen en beperkingen die de Wbp direct aan de bewerker oplegt. Het gaat om de volgende verplichtingen en beperkingen:

- de bewerker mag de persoonsgegevens alleen bewerken in opdracht van de verantwoordelijke;
- de bewerker is, naast de verantwoordelijke, zelfstandig aansprakelijk voor de schade die iemand lijdt of het nadeel dat iemand ondervindt;
- de bewerker en degenen die onder het gezag van de bewerker handelen, zijn – net als de verantwoordelijke – verplicht om persoonsgegevens waarvan zij kennisnemen, geheim te houden.

3.3 Inrichting organisatie: managementcyclus

De eisen uit de Wbp dienen goed in de organisatie te zijn geïmplementeerd om de persoonsgegevens van de verzekerde op adequate wijze te verwerken. Het is daarom van belang een stelsel van algemene verwerkingsmaatregelen en –procedures op te stellen, deze bekend te maken binnen de organisatie en de naleving hiervan structureel te controleren. In de Gedragscode zijn hiervoor bepalingen opgenomen. Zo is bepaald dat aan de interne accountantsdienst of een andere soortgelijke afdeling moet worden opdragen toe te zien op en te rapporteren over de naleving van de Wbp en de Gedragscode. De interne accountantsdienst moet haar bevindingen ten minste één keer per jaar in een rapport vastleggen (artikel 9.1 Gedragscode). Ter bevordering van de interne controle moeten instructies worden opgesteld waarin is aangegeven op welke wijze de persoonsgegevens worden verwerkt (artikel 9.2 Gedragscode).

Als de organisatie tot een evenwichtig verwerkingsbeleid voor persoonsgegevens wil komen en dit wil onderhouden, zal dat een belangrijke plaats in de managementcyclus moeten innemen. Een dergelijke cyclus bestaat uit drie onderdelen: de organisatie van processen inclusief de beleidsvoering, de processen zelf en een evaluatie en bijsturing van de processen.

3.4 Resultaten Wbp

Om na te gaan waar en op welke wijze de eisen van de Wbp in de operationele organisatie van de zorgverzekeraar zijn geborgd en welke aanvullende maatregelen de zorgverzekeraar eventueel nog moet treffen om een toereikende verwerking van persoonsgegevens te garanderen, zijn in de vragenlijst de onderdelen van de Wbp opgenomen. Het gaat om de volgende aspecten: melding, rechtmatige grondslag, doelbinding, transparantie, kwaliteit, rechten van de betrokkene, beveiliging en bewerker. Bij de beoordeling van deze onderdelen is een indeling in vier niveaus gehanteerd.

Beoordeling	
Niveau 1	Niets vastgelegd en niet bekend
Niveau 2	Niets vastgelegd maar wel bekend
Niveau 3	Vastgelegd en bekend
Niveau 4	Vastgelegd, bekend en gecontroleerd

Het gewenste niveau van gegevensverwerking is niveau vier. Bij dit niveau heeft de zorgverzekeraar procedures vastgelegd en maatregelen getroffen om de verwerking van persoonsgegevens te waarborgen. De procedures en maatregelen zijn bekend bij de medewerkers en de naleving hiervan wordt gecontroleerd. De aanbevelingen in hoofdstuk vijf zijn erop gericht om het gewenste beschermingsniveau vier te bereiken.

Een score op niveau vier betekent echter *niet* dat er geen verbeterpunten zijn.

3.4.1 Overzicht score zorgverzekeraars

3.4.1.1 Algemeen

De verwerking van persoonsgegevens door zorgverzekeraars laat in het algemeen een divers beeld zien. Hierbij moet worden opgemerkt dat de beoordeling is gebaseerd op de antwoorden en informatie van zorgverzekeraars. De feitelijke naleving van de regels als zodanig is niet gecontroleerd door de NZa. Bij de interpretatie van de beoordeling dient hiermee rekening te worden gehouden.

Bij slechts dertien zorgverzekeraars (41%) bevindt de verwerking van persoonsgegevens zich op alle onderdelen op het vierde niveau. Bij zes van deze zorgverzekeraars – twee concerns – is een functionaris voor de gegevensbescherming aangesteld. Dit heeft een positieve invloed op de organisatie van de verwerking van persoonsgegevens. Als wordt gekeken naar het aantal verzekerden dat bij deze dertien zorgverzekeraars is verzekerd, blijkt dat het gaat om meer dan tien miljoen verzekerden. Dit is meer dan de helft van de Nederlands ingezetenen.

Bij de meerderheid van de zorgverzekeraars (59%) ligt de verwerking van persoonsgegevens op één of meerdere onderdelen niet op het gewenste vierde niveau. Dit betekent dat deze zorgverzekeraars op onderdelen geen procedures en maatregelen hebben vastgelegd (niveau 1 en 2) en dat er op deze onderdelen geen controle op de naleving plaatsvindt (niveau 1, 2 en 3).

Tabel 1 geeft een overzicht van de scores van de zorgverzekeraars op de verschillende onderdelen. In de kolommen staan per niveau de aantallen zorgverzekeraars vermeld. Gezien de onduidelijkheid bij zorgverzekeraars over het begrip ‘bewerker’ en de diversiteit van de antwoorden van de zorgverzekeraars, heeft de NZa besloten op dit onderdeel geen indeling in niveaus te maken. In hoofdstuk vijf doet de NZa wel aanbevelingen over het onderwerp ‘bewerker’.

Tabel 1. Score zorgverzekeraars (n=32)

	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Melding	1	12	3	16
Rechtmatige grondslag	-	8	5	19
Doelbinding	2	5	7	18
Transparantie	-	6	6	20
Kwaliteit	-	2	1	29
Rechten van betrokkene	-	7	3	22
Beveiliging	-	-	2	30
Bewerker	-	-	-	-

Uit de tabel blijkt dat over het geheel gezien per onderdeel meer dan de helft van de zorgverzekeraars het gewenste vierde niveau heeft bereikt. Per onderdeel moeten twee tot zestien zorgverzekeraars verbetermaatregelen treffen om ook het vierde niveau te bereiken. De onderdelen waarop het beste wordt gescoord zijn de kwaliteit van de gegevensverwerking en de beveiliging. Meer dan 90% van de zorgverzekeraars bevindt zich op deze onderdelen op het vierde niveau. Bij de beveiliging moet worden opgemerkt dat het nodig is dat de

zorgverzekeraar regelmatig het beveiligingsbeleid evalueert en zonodig herziet.

3.4.1.2 Verschillen grote en kleine zorgverzekeraars[18]

Als onderscheid wordt gemaakt tussen de vijf grootste zorgverzekeraars (> 1.000.000 verzekerden) en vijf kleinste zorgverzekeraars (< 150.000 verzekerden) laat dit verschillen zien in de verwerking van persoonsgegevens (zie tabel 2). In de kolommen staan per niveau de aantallen zorgverzekeraars vermeld. Er zijn vooral verschillen in de controle op de naleving van de geldende procedures en maatregelen. De kleine zorgverzekeraars controleren minder vaak op de geldende procedures en maatregelen dan de grote zorgverzekeraars.

Tabel 2. Verschillen grote en kleine zorgverzekeraars

	Niveau 1		Niveau 2		Niveau 3		Niveau 4	
	Groot	*Klein*	*Groot*	*Klein*	*Groot*	*Klein*	*Groot*	*Klein*
Melding	-	-	1	3	-	1	4	1
Rechtmatige grondslag	-	-	1	1	-	3	4	1
Doelbinding	-	-	1	-	1	3	3	1
Transparantie	-	-	1	1	-	3	4	1
Kwaliteit	-	-	-	1	-	-	5	4
Rechten van betrokkene	-	-	1	2	-	1	4	2
Beveiliging	-	-	-	-	1	-	4	5

3.4.1.3 Verschillen verzekeraars met en zonder relatie met hypotheken en levens– en pensioenverzekeringen

Als onderscheid wordt gemaakt tussen zorgverzekeraars die een relatie hebben met hypotheekverstrekkers, aanbieders van levens– en/of pensioenverzekeringen en zorgverzekeraars die deze relatie niet hebben, laat dit verschillen zien in de verwerking van persoonsgegevens (zie tabel 3). In de kolommen staan per niveau de aantallen zorgverzekeraars vermeld. Bij de zorgverzekeraars waar de bovenstaande relatie aanwezig is, kan onrechtmatige verwerking van persoonsgegevens de verzekerde direct schaden. Deze zorgverzekeraars hebben de verwerking van persoonsgegevens over het algemeen op een beter niveau dan de zorgverzekeraars waar deze relatie niet aanwezig is. In het bijzonder op de controle op een transparante verwerking, de vastlegging en controle met betrekking tot de doelbinding, rechtmatige grondslag en rechten van de betrokkene scoren deze zorgverzekeraars beter.

[18] Peildatum verzekerdenaantallen 1 februari 2007

Tabel 3. Verschillen wel en geen relatie overige verzekeringen

	Niveau 1		Niveau 2		Niveau 3		Niveau 4	
	Wel	*Geen*	*Wel*	*Geen*	*Wel*	*Geen*	*Wel*	*Geen*
Melding	-	1	6	6	-	3	9	7
Rechtmatige grondslag	-	-	2	6	2	3	11	8
Doelbinding	1	1	-	5	1	6	13	5
Transparantie	-	-	1	5	-	6	14	6
Kwaliteit	-	-	1	1	-	1	14	15
Rechten van betrokkene	-	-	1	6	-	3	14	8
Beveiliging	-	-	-	-	-	5	14	10

Voor nagenoeg alle zorgverzekeraars geldt dat het vastleggen van procedures voor de gegevensverwerking en de controles op de naleving hiervan aandacht verdienen. Vaak zijn er wel *algemene* procedures en controles aanwezig. Weliswaar worden hiermee privacyaspecten geraakt, toch is het van belang om procedures en controles in te voeren die specifiek zijn gericht op de verwerking van persoonsgegevens, zoals op grond van artikel 9.2 van de Gedragscode van de zorgverzekeraar wordt verwacht. Ook vindt slechts bij een enkele zorgverzekeraar een jaarlijkse controle plaats op grond van artikel 9.1 van de Gedragscode. Het CBP heeft producten ontwikkeld die zorgverzekeraars hierbij kunnen gebruiken.[19]

De onderdelen uit de tabellen bestaan uit verschillende toetspunten. In de volgende paragrafen wordt per onderdeel nader ingegaan op deze toetspunten.

3.4.2 Melding

Twee concerns – zes zorgverzekeraars – hebben een functionaris voor de gegevensbescherming aangesteld. De overige zorgverzekeraars hebben melding gedaan bij het CBP. Hierbij moet worden opgemerkt dat de NZa de inhoud van de melding niet heeft beoordeeld. Het CBP toetst de binnengekomen meldingen op aannemelijkheid. Onderzoek naar de rechtmatigheid van de – voorgenomen – verwerking door het CBP vindt plaats als een voorafgaand onderzoek is aangevraagd.

Voor dit onderzoek heeft de NZa de meldingen wel globaal bekeken en daaruit blijkt dat de melding in veel gevallen niet meer actueel is. Zo is bij de melding vaak nog 'Ziekenfondswet' geregistreerd in plaats van 'Zorgverzekeringswet' en wordt nog gevraagd naar bijvoorbeeld inkomensgegevens van de verzekerde. Onder de Ziekenfondswet waren deze gegevens nodig om het verzekeringsrecht te kunnen vaststellen, maar onder de Zvw is dit niet meer nodig.

De Wbp bepaalt dat de zorgverzekeraar wijzigingen in de melding binnen een jaar na de voorafgaande melding aan het CBP moet doorgeven. Aangezien de Zvw in 2006 is ingevoerd, hadden de meldingen in het openbare register van het CBP inmiddels actueel moeten zijn. Blijkbaar beoordelen de zorgverzekeraars nauwelijks de juistheid van de melding. Dit komt ook naar voren uit het onderzoek. Driekwart van de zorgverzekeraars heeft geantwoord de juistheid van de melding niet periodiek te beoordelen.

Bijna de helft (41%) van de zorgverzekeraars heeft aangegeven geen procedure te hebben voor de melding bij het CBP. Deze zorgverzekeraars

[19] Quickscan, WBP Zelfevaluatie, Raamwerk Privacy Audit (www.cbpweb.nl)

blijken de melding ook niet periodiek en/of bij wijzigingen te beoordelen. Bij slechts de helft van de zorgverzekeraars vindt naast de vastlegging en bekendmaking in de organisatie ook controle plaats op de naleving van de procedures en maatregelen. Dit betekent dat de overige helft van de zorgverzekeraars verbeteringen moet aanbrengen om bij dit onderdeel het vierde niveau te bereiken.

3.4.3 Rechtmatige grondslag, doelbinding, transparantie, kwaliteit

Zoals eerder vermeld zijn de *rechtmatige grondslagen* voor de verwerking van persoonsgegevens uit de Wbp voor zorgverzekeraars in het Addendum nader gedefinieerd. Persoonsgegevens mogen uitsluitend worden verwerkt 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. Wel moeten zorgverzekeraars de gegevens die zij willen verwerken toetsen aan deze grondslag. Een kwart van de zorgverzekeraars geeft aan geen procedures te hebben om de rechtmatige grondslag voor de gegevensverwerking vast te stellen. Bij een derde van de zorgverzekeraars vindt geen controle plaats op de naleving van – de procedures voor – de verwerking van persoonsgegevens op basis van de rechtmatige grondslag. Om het vierde niveau te bereiken moet 41% van de zorgverzekeraars verbetermaatregelen treffen. Deze liggen op het terrein van het vastleggen van de procedures en de controle op de naleving van de procedures.

Uit de antwoorden blijkt dat veel zorgverzekeraars persoonsgegevens niet voor andere *doeleinden* verwerken dan waarvoor deze gegevens worden verzameld, en daarom geen procedures hebben voor het vaststellen van verenigbaar gebruik (59%). Ook hebben veel zorgverzekeraars (69%) geen voorzieningen getroffen om te waarborgen dat bij het gebruik van persoonsgegevens voor historische, statistische en wetenschappelijke doeleinden de verdere werking uitsluitend geschiedt voor deze specifieke doeleinden. Op termijn kan gegevensverwerking voor andere doeleinden echter wel aan de orde zijn. Daarom vindt de NZa het van belang dat zorgverzekeraars procedures voor verenigbaar gegevensgebruik en voor historisch, statistisch en wetenschappelijk onderzoek opstellen.

Bijna 20% van de zorgverzekeraars geeft aan geen maatregelen te hebben getroffen om te waarborgen dat het verwerken van persoonsgegevens geschiedt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Bij 56% van de zorgverzekeraars vindt behalve de vastlegging en de bekendmaking in de organisatie ook controle plaats op de naleving van de maatregelen. Voor de overige zorgverzekeraars geldt dat zij verbetermaatregelen moeten treffen om het gewenste vierde niveau te bereiken. Deze liggen vooral op het terrein van het vastleggen van de maatregelen en de controle op de naleving van de maatregelen.

Een kwart van de zorgverzekeraars zegt niet over procedures voor transparantie – verwerking in overeenstemming met de wet, behoorlijk en zorgvuldig – te beschikken. Bij 62% van de zorgverzekeraars vindt naast de vastlegging en bekendmaking in de organisatie ook controle op de naleving van de procedures plaats. De overige zorgverzekeraars (38%) moeten verbetermaatregelen treffen om het vierde niveau te bereiken. Deze liggen vooral op het terrein van het vastleggen van de procedures en de controle op de naleving van de procedures.

Behalve de transparante verwerking heeft de zorgverzekeraar ook een informatieplicht. De score op de informatieplicht is overwegend positief. De meerderheid van de zorgverzekeraars (84%) informeert de verzekerde over de identiteit van de organisatie en het doel van de gegevensverwerking via het aanmeldformulier voor de zorgverzekering. Ook hebben bijna alle zorgverzekeraars dit ook in hun polisvoorwaarden opgenomen. Hiermee geeft 97% van de zorgverzekeraars voldoende invulling aan de informatieplicht.

De kwaliteit van de gegevensverwerking is bij de meeste zorgverzekeraars geborgd door algemene controles uit hoofde van de reguliere bedrijfsvoering , zoals systeemcontroles. Hoewel deze controles niet specifiek gericht zijn op privacy, worden met deze reguliere controles wel privacyaspecten geraakt. Niettemin verdient het aanbeveling bij de huidige controles meer aandacht te besteden aan het privacyaspect. Van de zorgverzekeraars moet 9% verbetermaatregelen treffen om het vierde niveau te bereiken. Deze liggen in het bijzonder op het terrein van het vastleggen van de procedures en maatregelen en de controle op de naleving daarvan.

3.4.4 Rechten van betrokkene

Het grootste deel van de zorgverzekeraars (78%) heeft voor de rechten van betrokkenen procedures en maatregelen vastgelegd. Bij 69% van de zorgverzekeraars wordt naast de vastlegging en de bekendmaking ook de naleving van de procedures en maatregelen gecontroleerd. Ongeveer een kwart van de zorgverzekeraars geeft aan geen beleid of richtlijnen te hebben voor het recht van de betrokkene op inzage, correctie, afscherming of verwijdering van zijn persoonsgegevens. Volgens het Addendum (artikel 3.10.1) dienen zorgverzekeraars hierover wel te beschikken. Hoewel zorgverzekeraars aangeven dat verzekerden weinig gebruik maken van deze rechten vindt de NZa het belangrijk dat zorgverzekeraars een dergelijk beleid hebben omdat dit direct de positie van de verzekerde raakt. Om het vierde niveau te bereiken moet bijna een derde van de zorgverzekeraars verbetermaatregelen treffen. Deze liggen vooral op het terrein van het vastleggen van de procedures en maatregelen en de controle op de naleving daarvan.

3.4.5 Beveiliging

De ingrediënten voor een goed beveiligingsbeleid zijn bij vrijwel alle zorgverzekeraars aanwezig. Van de zorgverzekeraars moet 6% controle op de naleving uitvoeren om het vierde niveau te bereiken. Zorgverzekeraars schenken aandacht aan het privacybewustzijn van medewerkers. Verder werken zij onder andere met autorisaties, toegangsbeveiliging en er zijn calamiteitenplannen beschikbaar.

Enige tijd geleden werd bekend dat buitenstaanders een lek in de website van een zorgverzekeraar hadden ontdekt. Hierdoor waren gegevens in te zien van aspirant–verzekerden die via de website een offerte hadden aangevraagd. Een andere zorgverzekeraar verkleint een dergelijk risico doordat deze professionele hackers in dienst heeft die de beveiliging van informatiesystemen continu testen. Deze zorgverzekeraar ziet het beveiligingsbeleid in tegenstelling tot de eerst genoemde zorgverzekeraar als een continu en dynamisch proces.

Beveiliging zal in de toekomst een nog belangrijkere rol gaan spelen omdat zorgverzekeraars steeds meer via het internet gaan werken. Dit stelt eisen aan het beveiligingsbeleid en vergt extra aandacht van de zorgverzekeraars. Gegeven de toenemende relevantie van informatie– en communicatietechnologie en de hieraan verbonden technische en

organisatorische bedreigingen, is het nodig dat de zorgverzekeraar regelmatig het beveiligingsbeleid evalueert en zonodig herziet.

3.4.6 Bewerker

Over de definitie van bewerker bleek bij de zorgverzekeraars onduidelijkheid te bestaan. De antwoorden waren hierdoor te divers om hierover een oordeel te geven. Zo gaf een aantal zorgverzekeraars aan geen bewerker te hebben. In de praktijk zijn er echter altijd één of meer bewerkers zoals Vecozo, Vektis, tussenpersonen of volmachten.[20] Bij de zorgverzekeraars die wel aangeven een bewerker te hebben ligt aan de uitbesteding van de werkzaamheden een contract ten grondslag. In dit contract is opgenomen dat de bewerker gehouden is aan een geheimhoudingsplicht. Ook moet de zorgverzekeraar zich op de hoogte stellen van het werkelijke beveiligingsniveau van de bewerker en hierop controle uitoefenen. Dit blijkt in bijna alle gevallen nog de nodige aandacht te verdienen.

Enige tijd geleden werd in de media gesteld dat zorgverleners in het systeem van Vecozo meer gegevens kunnen raadplegen dan die voor het doel noodzakelijk zijn. Het doel is om de zorgverlener in het kader van de controle van de verzekeringsstatus en de declaratieafhandeling op eenvoudige wijze en op een centrale plaats in staat te stellen na te gaan of en waar een persoon is verzekerd. Declaratieafhandeling door zorgverleners en zorgverzekeraars is niet mogelijk zonder daarbij verzekerdengegevens te verwerken die van de zorgverzekeraar afkomstig zijn. Deze verwerking geschiedt onder verantwoordelijkheid van de zorgverzekeraar. De gegevensverwerking door Vecozo geschiedt niet op basis van een zelfstandige titel, maar in opdracht van zorgverzekeraars.

Voor de raadpleging van het systeem geldt dat de zorgverlener hier alleen gebruik van kan maken als hij van Vecozo daarvoor een digitaal certificaat ontvangt. Dit certificaat wordt alleen verstrekt als de zorgverlener een overeenkomst ‘digitale gegevensuitwisseling’ met de zorgverzekeraar heeft gesloten. Daarnaast is de zorgverlener verplicht tot geheimhouding van de verstrekte gebruikersnaam, wachtwoord en het digitale certificaat. Verder is de zorgverlener verplicht adequate technische en organisatorische maatregelen te treffen in het kader van beveiligde toegangsregistratie en –controle, en ervoor zorg te dragen dat alleen geautoriseerde medewerkers toegang krijgen tot de betreffende gegevens. Bij onrechtmatig gebruik van het systeem moeten adequate maatregelen worden genomen. Van onrechtmatig gebruik is sprake wanneer bijvoorbeeld een zorgverlener persoonsgegevens raadpleegt die niet voor het doel noodzakelijk zijn. De doelbinding is dus bepalend voor de raadpleging. Aangezien de zorgverzekeraar eindverantwoordelijk blijft voor de verwerking van de persoonsgegevens dient deze adequate maatregelen te treffen richting de bewerker. De bewerker dient op zijn beurt adequate maatregelen te treffen richting de zorgverlener.

[20] Vecozo staat voor Veilige Communicatie in de Zorg

4. Addendum Zorgverzekeraars: regelgeving en resultaten

4.1 Inleiding

De gedragscode van Zorgverzekeraars Nederland (ZN) geeft regels voor een zorgvuldige omgang met de door de zorgverzekeraar ontvangen persoonsgegevens. Deze gedragscode is uitgewerkt en vormgegeven als een Addendum op de bestaande Gedragscode Verwerking Persoonsgegevens Financiële Instellingen van de Nederlandse Vereniging van Banken (NVB) en het Verbond van Verzekeraars (VvV).

Het Addendum 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 2.1). Ten tijde van het schrijven van dit rapport zijn de NVB, het VvV en ZN de Gedragscode en bijbehorend Addendum aan het actualiseren. Het CBP heeft in dat kader expliciete aandacht van ZN gevraagd voor de problemen bij de GGZ–declaraties. ZN streeft ernaar het geactualiseerde Addendum uiterlijk 1 juli 2008 aan het CBP voor te leggen. Naar verwachting blijven de uitgangspunten van de Gedragscode en het Addendum ongewijzigd.

Dit hoofdstuk belicht de hoofdlijnen van het Addendum behorende bij de Gedragscode (paragraaf 4.2) en de wijze waarop zorgverzekeraars deze regelingen in de praktijk naleven en borgen (paragraaf 4.3). De beginselen en onderdelen van de Wbp die zijn opgenomen in de Gedragscode zijn reeds in hoofdstuk twee aan de orde gekomen.

4.2 Inhoud Addendum Zorgverzekeraars

4.2.1 Interne regeling, medisch adviseur en acceptatie

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.

De gedragsregel legt de zorgverzekeraar verder de verplichting op om passende maatregelen te treffen die werknemers verplichten tot geheimhouding bij het verwerken van medische persoonsgegevens. Een voorbeeld van een dergelijke maatregel is de contractuele geheimhoudingsplicht van de werknemer.

Medisch adviseur
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.

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. Dit is bijvoorbeeld aan de orde als de medische persoonsgegevens worden verwerkt voor de behandeling van geschillen, misbruik en oneigenlijk gebruik, schadeverhaal, materiële controle en zorgbemiddeling.

Uit het Addendum volgt dat het ontvangen en verwerken van declaratiegegevens niet onder de verantwoordelijkheid van de medisch adviseur valt, omdat de 'span of control' van de medisch adviseur dan erg groot wordt. Daardoor zou de extra bescherming die het beheer door de medisch adviseur biedt gaan verwateren.

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 hiervoor 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. Het Addendum (artikel 3.6) bevat hiervoor gedragsregels.

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 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. De verzekeraar mag bij het keuringsonderzoek geen erfelijkheidsonderzoek verlangen of resultaten uit eerder onderzoek opvragen. Als de aspirant–verzekerde al ziekteverschijnselen heeft, die verbonden zijn aan een erfelijke ziekte, kan de verzekeraar wel van hem verlangen om dit te melden.

Als voor het acceptatieproces voor een aanvullende verzekering medische persoonsgegevens bij zorgaanbieders worden opgevraagd moet de medisch adviseur hiervoor uitdrukkelijke toestemming van de aspirant–verzekerde hebben.

De medisch adviseur verstrekt voor de acceptatie van verzekerden slechts die informatie die strikt noodzakelijk is voor de zorgverzekeraar om gemotiveerd te kunnen besluiten om een verzekerde wel of niet, onder uitsluiting van bepaalde – kosten van – zorg, met hantering van een wachttijd dan wel met een premietoeslag te accepteren. De medisch adviseur geeft de aan zijn advies ten grondslag liggende medische persoonsgegevens niet ter inzage. Voor medische dossiers geldt een bijzondere geheimhoudingsplicht (artikel 7:457 BW). Beslissingen over

acceptatie van verzekerden moeten door of namens de directie van de zorgverzekeraar worden ondertekend.

4.2.2 Zorgplicht, uitwisseling en overig gebruik persoonsgegevens

Zorgplicht
De zorgplicht legt zorgverzekeraars de plicht op tot het verstrekken van – vergoeding van – zorg uit de Zvw.[21] In het kader van de verwerking van persoonsgegevens zijn hierbij machtigingen en zorgbemiddeling van belang.

Zorgverzekeraars zijn vrij om te bepalen of en zo ja voor welke vormen van zorg zij een *machtiging* vereisen. Eventuele machtigingsvereisten zijn vastgelegd in de polisvoorwaarden. Hiervoor geldt dat een zorgverzekeraar uitsluitend informatie van de verzekerde mag verlangen die van rechtstreeks belang is voor het onderwerp waarop de machtigingsprocedure betrekking heeft (artikel 34 lid 1 Wmg).

Als een zorgaanbieder namens een verzekerde om een machtiging verzoekt, mag de zorgverzekeraar de persoonsgegevens niet verwerken als hij weet of redelijkerwijs kan vermoeden dat de zorgaanbieder hiervoor geen uitdrukkelijke toestemming heeft gekregen van de verzekerde. Deze persoonsgegevens zijn dan namelijk in strijd met het medisch beroepsgeheim verstrekt. Als de zorgverzekeraar de zorgaanbieder om een toelichting vraagt, moet voldoende aannemelijk zijn dat de uitdrukkelijke toestemming van de verzekerde zich uitstrekt tot de verstrekking van deze aanvullende informatie (artikel 3.0.4 onder b).

Als de verzekerde zélf om een machtiging vraagt, moet de medisch adviseur uitdrukkelijke toestemming van de verzekerde hebben om informatie bij de zorgaanbieder op te vragen. Ook hier geldt dat voor het opvragen van eventuele aanvullende informatie geen toestemming van de verzekerde nodig is, tenzij de aanvullende informatie buiten de reikwijdte van de oorspronkelijke aanvraag valt of als de informatie bij een andere zorgaanbieder wordt opgevraagd (artikel 3.0.4 onder c). In deze gevallen moet opnieuw toestemming aan de verzekerde worden gevraagd.

De zorgverzekeraar heeft een verantwoordelijkheid om de verzekerde de weg te wijzen voor de toegang tot noodzakelijke, adequate en tijdige zorgverlening (*zorgbemiddeling*). Het Addendum (artikel 3.7) bevat gedragsregels voor zorgbemiddeling. Ook geldt voor zorgbemiddeling dat de zorgverzekeraar uitsluitend informatie van de verzekerde mag verlangen die van rechtstreeks belang is voor het onderwerp waarop het zorgbemiddelingsverzoek betrekking heeft.

Individuele zorgbemiddeling vindt slechts plaats op verzoek van of namens de verzekerde. Hiervoor mag de zorgverzekeraar medische persoonsgegevens van de verzekerde verwerken. Voor het gericht benaderen van individuele verzekerden met een zorgbemiddelingsaanbod mogen alleen algemene criteria worden gebruikt. Diagnoses behoren hier niet toe. De zorgverzekeraar beëindigt het gebruik van persoonsgegevens bij zorgbemiddeling als de verzekerde aangeeft de zorgbemiddeling niet meer op prijs te stellen.

[21] Voor nadere informatie over de zorgplicht wordt verwezen naar het onderzoek zorgplicht van de NZa (augustus 2007). Dit onderzoek is beschikbaar op www.nza.nl.

Voor de machtigingsprocedures en zorgbemiddeling moet de zorgverzekeraar zelf bepalen welke informatie noodzakelijk en proportioneel is voor het doel waarvoor de gegevens worden verzameld. Als een consument, zorgaanbieder of zorgverzekeraar van mening is dat een procedure of formulier omtrent bijvoorbeeld zorgplicht onbegrijpelijk, ingewikkeld of overbodig is, kan hij op grond van artikel 23 Wmg beklag indienen bij de NZa.

Uitwisseling persoonsgegevens
Het Addendum bevat gedragsregels voor de verstrekking van gegevens van verzekerden (artikel 3.0.9). Medische persoonsgegevens mogen niet worden verstrekt aan andere concernonderdelen, niet zijnde ziektekosten – bijvoorbeeld voor het verstrekken van bankproducten, afsluiten van levensverzekeringen, autoverzekeringen, brandverzekeringen – of aan partijen buiten de organisatie. Uitzondering hierop is wanneer het verstrekken van de medische persoonsgegevens is gebaseerd op een wettelijk voorschrift. Adresgegevens mogen binnen een maatschappij of groep worden uitgewisseld voor commerciële doeleinden, tenzij de betrokkene hiertegen bezwaar heeft gemaakt.

Als de zorgverzekeraar ook een AWBZ–verzekering aanbiedt mag hij de medische persoonsgegevens, die bij de uitvoering van de AWBZ–verzekering zijn verkregen, niet gebruiken voor de uitvoering van de zorgverzekering of aanvullende verzekering, tenzij een wettelijk voorschrift dit vereist.

Verder mag de zorgverzekeraar medische persoonsgegevens die bij de uitvoering van de zorgverzekering dan wel de AWBZ–verzekering zijn verkregen, niet gebruiken voor het beoordelen en accepteren van een aspirant–verzekerde voor een aanvullende verzekering.

De zorgverzekeraar mag medische persoonsgegevens, verkregen bij de uitvoering van de zorgverzekering respectievelijk aanvullende verzekering, slechts voor de uitvoering van deze beide verzekeringen gebruiken, als dit noodzakelijk is voor de geheel of gedeeltelijke betaling aan een zorgaanbieder, de geheel of gedeeltelijke vergoeding van zorgkosten aan een verzekerde, de vaststelling van de eigen bijdragen, het eigen risico en de no–claim van de verzekerde, het uitoefenen van het verhaalsrecht of het verrichten van formele en materiële controle en fraudeonderzoek (artikel 3.0.9 onder c/d).

Het bovenstaande kan worden geïllustreerd aan de hand van een voorbeeld. Als de verzekerde een behandeling ondergaat die op basis van de zorgverzekering slechts gedeeltelijk voor vergoeding in aanmerking komt, maar waarvoor een aanvullende vergoeding vanuit de aanvullende verzekering mogelijk is, moet de zorgverzekeraar voor een goede uitvoering van de aanvullende verzekering ook toegang hebben tot de declaratiegegevens uit de zorgverzekering. Dit is overigens alleen toegestaan wanneer de verzekerde zowel de zorgverzekering als de aanvullende verzekering heeft ondergebracht bij dezelfde zorgverzekeraar of binnen één concern, handelend onder dezelfde naam.

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. Deze informatie hoeft echter niet op persoonsniveau bekend te zijn. Zorgverzekeraars mogen voor zorginkoop

en voor schadelastbeheersing alleen informatie op geaggregeerd niveau – niet herleidbaar tot individuele personen – gebruiken (artikel 3.1.1 en 3.3). Ook mogen risicoprofielen van verzekerden op geaggregeerd niveau worden verwerkt voor de beoordeling van een aangemeld risico (artikel 3.2.3). Het is niet toegestaan om medische persoonsgegevens voor marketingdoeleinden te gebruiken (artikel 3.5). Gegevens over het betalingsgedrag van verzekerden mogen alleen worden gebruikt voor acceptatie, controle en in– en excasso (artikel 3.4.1).

4.2.3 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.

Bij de Archiefwet gaat het alleen om de 'archiefbescheiden' van de Nederlandse overheid en niet van het bedrijfsleven. De Archiefwet kent geen algemene bewaartermijn, maar schrijft voor dat elk overheidsorgaan over een selectielijst moet beschikken. Hierin staat welke stukken op termijn moeten worden vernietigd en welke voor altijd moeten blijven bewaard. De Archiefwet is voor zorgverzekeraars uitsluitend van toepassing op de archieven die de zorgverzekeraar heeft gevormd bij de zogenaamde openbaar gezagtaken, dat wil zeggen de taken die op grond van de Zvw en de AWBZ worden uitgevoerd. De zorgverzekeraars hebben een privaatrechtelijke rechtsvorm en zijn archiefwettelijk zorgdrager.[22]

De Wbp is een algemene privacywet en stelt regels aan de verwerking van persoonsgegevens. Daarmee bedoelt de wet niet alleen het verzamelen, beheren en ter beschikking stellen van persoonsgegevens, maar ook het vernietigen van persoonsgegevens. De Archiefwet stelt regels aan het beheer van archiefbescheiden bij de overheid. Persoonsgegevens maken vaak deel uit van archiefbescheiden. De Wbp en Archiefwet moeten daarom in onderlinge samenhang worden bekeken. Van belang is dat de Archiefwet op het punt van de verwerking van persoonsgegevens als bijzondere wet ten opzichte van de Wbp geldt. Dit betekent dat de Archiefwet boven de Wbp gaat als de Wbp en de Archiefwet in strijd met elkaar zijn.

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 medisch dossiers die door de medisch adviseur worden beheerd geldt een bewaartermijn van vijftien jaar op grond van artikel 7:454 lid 3 BW (WGBO).

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.

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. Het bewaren van de gegevens na beëindiging van de overeenkomst is

[22] Degene die bij of krachtens de wet belast is met de zorg voor de archiefbescheiden.

noodzakelijk om eventuele vorderingen die hiermee nog samenhangen te beoordelen.

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. 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 (zie ook paragraaf 3.2.3).

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.

4.2.4 Materiële controle en Misbruik/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. Fraudebestrijding is van belang om de integriteit te bewaren en om te voorkomen dat de kosten van onrechtmatige declaraties worden afgewenteld op de premie.

Zorgverzekeraars zijn op grond van artikel 7.4 van de regeling zorgverzekering verplicht de materiële controles uit te voeren op de wijze zoals in het Addendum is vastgelegd. Voor AWBZ–verzekeraars geldt dat zij materiële controles moeten uitvoeren in overeenstemming met de Regeling Controle en Administratie AWBZ–verzekeraars. De zorgverzekeraar gaat bij de controle van persoonsgegevens – ook in relatie tot de zorgaanbieder – zorgvuldig om met deze gegevens en houdt zich daarbij aan het Protocol Materiële Controle.

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.

Als de zorgverzekeraar vaststelt dat de verzekeringnemer essentiële informatie voor de acceptatie van de aanvullende verzekering bij het aangaan van deze verzekering niet heeft medegedeeld, heeft hij het recht om de verzekering binnen twee maanden daarna met onmiddellijke ingang op te zeggen. Reeds uitgekeerde kosten kunnen worden teruggevorderd, als de verzekeringnemer de informatie met opzet heeft verzwegen of als de zorgverzekeraar bij kennis van de ware stand van zaken de verzekering niet zou hebben gesloten. Bij de voor de uitoefening van dit recht noodzakelijke verwerking van persoonsgegevens moet de proportionaliteit in acht worden genomen (artikel 3.9.2).

4.2.5 Omschrijving zorg op nota's en klachten en geschillen

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. Daarbij

wordt verondersteld dat de verzekeringnemer, die een verzekering heeft gesloten voor zijn gezin, ook alle in het gezin vallende ziektekosten voor zijn rekening neemt. Aangezien de verzekeringnemer recht heeft op de schadevergoeding, heeft hij tevens recht op de bijbehorende informatie, voor zover dit noodzakelijk is voor de uitoefening van zijn vorderingsrecht; bijvoorbeeld niet de medicijnnaam, maar een omschrijving als 'farmaceutische middelen'. Bij de informatieverstrekking aan de verzekeringnemer laat de zorgverzekeraar onnodige gegevens over de gezondheid van andere verzekerden achterwege (artikel 3.2).

Klachten en geschillen
Verzekerden kunnen geschillen over de uitvoering van de zorgverzekering en de aanvullende verzekering melden bij de Stichting Klachten en Geschillen Zorgverzekeringen (SKGZ), nadat de verzekerde de zorgverzekeraar heeft verzocht zijn beslissing te heroverwegen en deze niet binnen redelijke termijn of niet naar tevredenheid van de verzekerde heeft gereageerd. Geschillen over de uitvoering van de Wbp, de Gedragscode en het Addendum kunnen worden voorgelegd aan de Ombudsman Zorgverzekeringen (artikel 3.11.1).

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).

De zorgverzekeraar verstrekt bij een klacht of een geschil alleen persoonsgegevens aan de geschilleninstantie of rechter als dit noodzakelijk is voor de geschillenbeslechting en niet meer gegevens dan strikt noodzakelijk. Voor deze gegevensverstrekking mag de toestemming van de verzekerde over het algemeen worden verondersteld. Als het een civiele schadeclaim betreft, is echter de uitdrukkelijke toestemming van de verzekerde nodig, als en voor zover het om gegevens gaat die worden verwerkt onder de verantwoordelijkheid van de medisch adviseur (artikel 3.11.2).

4.3 Resultaten Addendum Zorgverzekeraars

4.3.1 Overzicht score zorgverzekeraars

4.3.1.1 Algemeen

De zorgverzekeraars hebben in grote lijnen de getoetste bepalingen uit het Addendum gewaarborgd. Echter, geen enkele zorgverzekeraar voldoet aan alle bepalingen uit het Addendum. Dit hangt wellicht samen met het tijdstip van de invoering van het Addendum in 2006, tegelijkertijd met de invoering van de Zvw. Het lijkt logisch dat zorgverzekeraars toen prioriteit hebben gegeven aan de invoering van de Zvw en niet aan het Addendum. De onderzoeksresultaten geven de indruk dat zorgverzekeraars het gevoel hebben in grote lijnen wel aan het Addendum te voldoen. Een mogelijke verklaring hiervoor is dat het Addendum geen verregaande organisatorische aanpassingen van de zorgverzekeraars vergt, waardoor al gauw het idee kan ontstaan dat 'het wel goed zit'. Uit het onderzoek blijkt echter dat dit niet op alle punten het geval is. Vooral op het gebied van de bewaartermijnen van persoonsgegevens, het opnemen van bepalingen in de aanvullende voorwaarden omtrent materiële controle en misbruik en oneigenlijk gebruik en de interne regeling conform artikel 3.0.2 van het Addendum moeten zorgverzekeraars verbeteringen doorvoeren om te voldoen aan het Addendum. Daarnaast komen de verantwoordelijkheden van de medisch adviseur bij enkele zorgverzekeraars niet overeen met hetgeen is bepaald in het Addendum.

Een overzicht van de scores van de zorgverzekeraars op de belangrijkste onderdelen is weergegeven in tabel 4. De eerste kolom ('Ja') geeft het aantal zorgverzekeraars aan dat voldoet aan de bepaling van het Addendum. De tweede kolom ('Nee') geeft het aantal zorgverzekeraars aan dat hier niet aan voldoet. De laatste kolom vermeldt het aantal zorgverzekeraars waarvoor een bepaling uit het Addendum niet van toepassing is, bijvoorbeeld wanneer de verzekeraar geen acceptatiebeleid heeft of geen AWBZ uitvoert.

Tabel 4. Score zorgverzekeraars (n=32)

	Ja	Nee	n.v.t.
Interne regeling			
*Interne regeling cf. art. 3.0.2	17	15	-
Medisch adviseur			
*Verantwoordelijkheid en processen medisch adviseur cf. art. 3.0.3	28	4	-
Acceptatie			
*Procedure bij negatieve uitslag voor acceptatie AV is cf. art. 3.6.1	15	6	11
*Gebruik persoonsgegevens voor acceptatie cf. art. 3.0.6	21	-	11
Zorgplicht			
*Machtigingsverzoeken cf. art. 3.0.4	32	-	-
*Individuele zorgbemiddeling cf. art. 3.7.2	32	-	-
Uitwisseling persoonsgegevens			
*Uitwisseling persoonsgegevens cf. art. 3.0.9 a/b en e	32	-	-
*Uitwisseling medische persoonsgegevens tussen zorgverzekering - AV v.v. cf. art. 3.0.9 c/d	31	1	-
Overig gebruik persoonsgegevens			
*Verwerking gegevens voor zorginkoop cf. art. 3.1	28	-	4
*Verwerking gegevens voor risicoprofielen voor acceptatie cf. art. 3.2.3	3	-	29
*Verwerking gegevens voor schadelastbeheersing cf. art. 3.3	10	-	22
*Verwerking gegevens over betalingsgedrag cf. art. 3.4	22	-	10
*Geen medische persoonsgegevens verwerken voor marketing cf. art. 3.5	32	-	-
Bewaartermijnen			
*Bij niet tot stand komen verzekering bewaartermijn medische persoonsgegevens cf. art. 3.0.7	14	10	8
*Na beëindiging verzekering bewaartermijn medische persoonsgegevens cf. art. 3.0.8	19	13	-
*Bewaartermijn gegevens over betalingsgedrag van verzekerden cf. art. 3.4	10	19	3
Materiële controle & Misbruik/Oneigenlijk gebruik			
*Bepaling in AV cf. art. 3.8.1 en 3.9.1	10	22	-
Omschrijving zorg op nota's			
*Omschrijving op nota's cf. art. 3.2.1	30	2	-
Klachten en geschillen			
*Informatie over wijze van afhandeling klachten over uitvoering Wbp, Gedragscode, Addendum	28	4	-
*Verstrekken gegevens aan geschilleninstantie of rechter cf. art. 3.11.2	27	5	-
Aanmeldformulieren			
*Geen gezondheidsvragen bij afsluiten van zorgverzekering	31	1	
*Geen vragen over het strafrechtelijk verleden bij afsluiten van zorgverzekering	25	7	-

Een derde van de zorgverzekeraars heeft aangegeven geen acceptatiebeleid voor de aanvullende verzekering te voeren. Hierdoor is een aantal bepalingen uit het Addendum min of meer niet van toepassing, omdat geen gebruik wordt gemaakt van medische persoonsgegevens voor de acceptatie van een aanvullende verzekering. Dit beeld kan veranderen wanneer de zorgverzekeraars acceptatiebeleid voor de aanvullende verzekering – verder – gaan invoeren.

De meerderheid van de zorgverzekeraars die naast de zorgverzekering ook aanvullende verzekeringen aanbieden stelt op het aanmeldformulier geen gezondheidsvragen. Bij een beperkt aantal zorgverzekeraars dat vragen stelt over het strafrechterlijk verleden is onduidelijk dat deze

vragen alleen beantwoord moeten worden voor het afsluiten van een aanvullende verzekering. Deze zorgverzekeraars moeten hun aanmeldformulieren aanpassen. Uiterlijk 1 juni 2008 moeten de zorgverzekeraars hierover verantwoording afleggen aan de NZa.

4.3.1.2 Verschillen grote en kleine zorgverzekeraars

Evenals bij de Wbp bestaan ook hier verschillen tussen de vijf grootste zorgverzekeraars (> 1.000.000 verzekerden) en vijf kleinste zorgverzekeraars (< 150.000 verzekerden) en de borging van de bepalingen uit het Addendum. De verantwoordelijkheden van de medisch adviseur en de processen die onder zijn verantwoordelijkheid vallen, komen bij de grote zorgverzekeraars beter overeen met het Addendum dan bij de kleine zorgverzekeraars. Daarnaast is er een verschil in het informeren van de verzekerde over de wijze van afhandeling van de klachten over de Wbp, Gedragscode en het Addendum. Ook hier scoren de grote zorgverzekeraars beter dan de kleine zorgverzekeraars.

4.3.1.3 Verschillen verzekeraars met en zonder relatie met hypotheken en levens– en pensioenverzekeringen

Bij de Wbp zijn duidelijke verschillen aanwezig tussen zorgverzekeraars die wel en die geen relatie hebben met hypotheekverstrekkers en aanbieders van levens– en/of pensioenverzekeringen. Bij het Addendum zijn bijna geen verschillen zichtbaar. Alleen zorgverzekeraars met de bovenstaande relatie hebben vaker een interne regeling op grond van artikel 3.0.2 van het Addendum.

In de volgende paragrafen wordt per onderdeel nader ingegaan op de bovenstaande score.

4.3.2 Interne regeling, medisch adviseur en acceptatie

Interne regeling
De helft van de zorgverzekeraars (53%) geeft aan een interne regeling te hebben. Dit betekent dat de andere helft geen interne regeling op grond van artikel 3.0.2 van het Addendum heeft. Wellicht bestaat er onduidelijkheid over – de inhoud van – deze regeling of hebben zorgverzekeraars wel een interne regeling maar duiden zij dit anders aan. Voor zover bekend beschikken alle zorgverzekeraars over autorisatieschema's. Aandachtspunt daarbij is dat hierin niet overal is aangeven welke persoonsgegevens en voor welke doeleinden de persoonsgegevens mogen worden verwerkt.

Om de medewerkers bij de zorgverzekeraars te verplichten tot geheimhouding hebben alle zorgverzekeraars in de arbeidsovereenkomst met de medewerkers een geheimhoudingsplicht opgenomen.

Medisch adviseur
De verantwoordelijkheden van de medisch adviseur en de processen die onder zijn verantwoordelijkheid vallen komen bij 87% van zorgverzekeraars overeen met hetgeen is bepaald in het Addendum.[23] De medisch adviseur heeft bij één zorgverzekeraar geen enkele verantwoordelijkheid en bij twee zorgverzekeraars valt enkel het proces van de machtigingen onder de verantwoordelijkheid van de medisch adviseur.

Artikel 3.0.3, waarin de verantwoordelijkheden van de medisch adviseur zijn beschreven, is een belangrijk onderdeel van het Addendum. Het gaat

[23] De verantwoordelijkheden genoemd in het Addendum zijn niet limitatief.

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 bij zorgverzekeraars overeen komt met hetgeen is bepaald in het Addendum. Bij één zorgverzekeraar is een implementatietraject ingezet om de verantwoordelijkheden van de medisch adviseur in lijn te brengen met het Addendum.

De verwerking van declaraties valt bij geen enkele zorgverzekeraars onder de verantwoordelijkheid van de medisch adviseur. Dit is conform het Addendum.

Acceptatie
Met de invoering van de Zvw in 2006 hebben zorgverzekeraars onderling afgesproken geen acceptatievoorwaarden te stellen voor de aanvullende verzekering, met uitzondering van de meest luxe en uitgebreide (tandarts)verzekering. Ook in 2007 vragen zorgverzekeraars nog bijna geen medische persoonsgegevens op van aspirant–verzekerden bij het afsluiten van een aanvullende verzekering. Een zorgverzekeraar voldoet hierdoor automatisch aan de artikel 3.6 van het Addendum.

Door het ontbreken van een acceptatiebeleid was bij een derde van de zorgverzekeraars een groot deel van de vragen niet van toepassing, waardoor geen duidelijk oordeel over de borging van artikel 3.6 van het Addendum is te geven. Echter, het ligt in de lijn der verwachting dat zorgverzekeraars de komende jaren wel acceptatievoorwaarden gaan stellen voor de aanvullende verzekering. Bij de invoering van een dergelijk acceptatiebeleid moet de zorgverzekeraar rekening houden met artikel 3.6 van het Addendum en het acceptatiebeleid hiermee in lijn brengen.

De zorgverzekeraars die wel een acceptatiebeleid hebben, geven aan vrijwel alle bepalingen hierover uit het Addendum na te leven. Bij 19% van de zorgverzekeraars stelt de medisch adviseur de aspirant–verzekerde niet altijd in de gelegenheid mee te delen als eerste de uitslag van het keuringsonderzoek voor de aanvullende verzekering te vernemen en te beslissen of deze uitslag al dan niet aan de zorgverzekeraar wordt meegedeeld. Slechts één zorgverzekeraar stelt de aspirant–verzekerde door een vraag op het aanmeldformulier in de gelegenheid van dit recht gebruik te maken. Dit is een vrij eenvoudige oplossing om de verzekerde gebruik te laten maken van dit recht. Een andere zorgverzekeraar meldt op het aanmeldformulier dat de verzekerde dit recht heeft, maar dat de verzekerde zelf dient aan te geven hiervan gebruik te willen maken.

Geen van de zorgverzekeraars voert voor de acceptatie van een aanvullende verzekering een erfelijkheidsonderzoek uit of vraagt naar de uitkomsten van een – eerder – uitgevoerd erfelijkheidsonderzoek.

Aanmeldformulieren zorgverzekering
Zoals in paragraaf 4.2.1 is vermeld mag de zorgverzekeraar voor de acceptatie van de aspirant–verzekerde voor de zorgverzekering geen medische persoonsgegevens en gegevens over het strafrechtelijk verleden opvragen van de aspirant–verzekerde. De NZa heeft hiertoe de aanmeldformulieren voor de zorgverzekering voor 2008 geanalyseerd. Dit staat los van de vragenlijst die onder de zorgverzekeraars is uitgezet. De resultaten zijn de bevindingen van de NZa en niet de antwoorden van de zorgverzekeraars.

Van de 30 zorgverzekeraars die naast de zorgverzekering ook aanvullende verzekeringen aanbieden, hebben 19 zorgverzekeraars (59%) geen gezondheidsvragen of een verzoek om een tandheelkundige verklaring in het aanmeldformulier opgenomen. Van de elf zorgverzekeraars die in het aanmeldformulier wel gezondheidsvragen hebben opgenomen, is het bij één zorgverzekeraar niet duidelijk of deze vragen ook moeten worden beantwoord als de aspirant–verzekerde alleen een zorgverzekering en geen aanvullende verzekering wenst af te sluiten. Deze zorgverzekeraar moet zijn aanmeldformulier verduidelijken.

Verder hebben acht zorgverzekeraars in het aanmeldformulier vragen opgenomen over het strafrechtelijk verleden van de aspirant–verzekerde. Slechts bij één zorgverzekeraar is duidelijk in het aanmeldformulier opgenomen dat deze vragen alleen hoeven te worden beantwoord wanneer de aspirant–verzekerde – ook – een aanvullende verzekering wil afsluiten. Bij de overige zorgverzekeraars is dit niet opgenomen. Hierdoor kan het voorkomen dat aspirant–verzekerden die geen aanvullende verzekering naast de zorgverzekering wensen af te sluiten, gegevens aan de zorgverzekeraar verstrekken die niet voor het doel noodzakelijk zijn. De zorgverzekeraars zijn immers verplicht de verzekerde voor de zorgverzekering te accepteren, ongeacht het strafrechtelijk verleden. De NZa heeft de zeven zorgverzekeraars waarbij het bovenstaande aan de orde is, verzocht per direct het aanmeldformulier aan te passen.

4.3.3 Zorgplicht, uitwisseling en overig gebruik persoonsgegevens

Zorgplicht: machtigingen en zorgbemiddeling
In het Addendum is bepaald dat de zorgverzekeraar de medische persoonsgegevens die hij heeft ontvangen voor het beoordelen van een machtigingsaanvraag niet mag verwerken als hij signalen heeft die er op wijzen dat de zorgaanbieder hiervoor geen uitdrukkelijke toestemming van de verzekerde heeft verkregen. Aangezien het niet verplicht is gesteld dat de verzekerde schriftelijk zijn toestemming geeft aan de zorgaanbieder voor het verstrekken van zijn gegevens, is het voor de zorgverzekeraars moeilijk invulling te geven aan deze bepaling zo blijkt uit het onderzoek. Er is een discrepantie ontstaan tussen regelgeving en praktijk. Zorgverzekeraars hebben geen signalen gedefinieerd die er op kunnen duiden dat de zorgaanbieder geen uitdrukkelijke toestemming van de verzekerde heeft verkregen. Hierdoor verwerken de zorgverzekeraars altijd de medische persoonsgegevens, verkregen van de zorgaanbieder, voor het beoordelen van een machtigingsaanvraag. Het is de NZa uit het onderzoek niet duidelijk geworden waarom de zorgverzekeraars geen signalen hebben gedefinieerd die hierop kunnen duiden. De NZa adviseert de zorgverzekeraars dergelijke signalen te definiëren, zodat deze in de praktijk kunnen worden herkend.

Alle zorgverzekeraars vragen bij een machtigingsaanvraag van de verzekerde uitdrukkelijke toestemming van de verzekerde conform artikel 3.0.4 onder c om informatie bij een zorgaanbieder op te vragen.

Alle zorgverzekeraars geven aan geen eigen initiatieven te nemen in zorgbemiddeling, maar alleen te bemiddelen als de verzekerde er om verzoekt. Bij individuele zorgbemiddelingsverzoeken handelen alle zorgverzekeraars conform artikel 3.7.2.

Uitwisseling persoonsgegevens
Uit het onderzoek is niet gebleken dat zorgverzekeraars medische persoonsgegevens verstrekken aan andere concernonderdelen – geen ziektekosten – of andere externe partijen. Ook geven de

zorgverzekeraars aan de medische persoonsgegevens, verkregen bij de uitvoering van de zorgverzekering of AWBZ–verzekering, niet te gebruiken voor de beoordeling en acceptatie voor de aanvullende verzekering. Ook hier geldt dat 34% van de verzekeraars heeft aangegeven geen acceptatiebeleid te hebben. Wanneer deze zorgverzekeraars besluiten een acceptatiebeleid in te voeren, moet rekening worden gehouden met artikel 3.0.9 onder b.

De zorgverzekeraars die ook de AWBZ uitvoeren geven aan de medische persoonsgegevens die hiervoor zijn verkregen niet te gebruiken voor de uitvoering van de zorgverzekering en aanvullende verzekering.

De uitwisseling van medische persoonsgegevens tussen de zorgverzekering en aanvullende verzekering en vice versa gaat bij 97% van de zorgverzekeraars conform het Addendum. Bij één zorgverzekeraar is geen scheiding aangebracht tussen de vastlegging van de gegevens uit de zorgverzekering en aanvullende verzekering. Hierdoor kunnen meer gegevens tussen de zorgverzekering en aanvullende verzekering en vice versa worden uitgewisseld dan voor het doel noodzakelijk is.

Overig gebruik persoonsgegevens
Van de zorgverzekeraars verwerkt 88% persoonsgegevens op geaggregeerd niveau voor de zorginkoop. De overige 12% geeft aan hiervoor geen persoonsgegevens te verwerken. Opvallend is dat 69% van de zorgverzekeraars aangeeft geen risicoprofielen op te stellen voor schadelastbeheersing. De zorgverzekeraars die wel risicoprofielen hanteren, gebruiken hiervoor alleen geaggregeerde gegevens. Van de zorgverzekeraars heeft 91% aangegeven geen persoonsgegevens te verwerken voor een risicoprofiel van verzekerden voor de beoordeling van een aangemeld risico voor de aanvullende verzekering. Ook dit hangt samen met het ontbreken van acceptatievoorwaarden voor de aanvullende verzekering. De overige zorgverzekeraars verwerken de gegevens hiervoor op geaggregeerd niveau conform artikel 3.2.3. Gegevens over het betalingsgedrag van verzekerden wordt door 69% van de zorgverzekeraars gebruikt conform artikel 3.4.1. De overige zorgverzekeraars geven aan deze gegevens niet te verwerken. Ten slotte hebben alle zorgverzekeraars aangegeven geen medische persoonsgegevens voor marketingdoeleinden te gebruiken.

4.3.4 Bewaartermijnen

Zorgverzekeraars hebben voor de bewaartermijnen van de persoonsgegevens van verzekerden te maken met verschillende wetten. Dit zijn in ieder geval de Archiefwet, Wbp, WGBO en de Gedragscode en het bijbehorende Addendum. Gezien de bevindingen in dit onderzoek vergen de bewaartermijnen van zorgverzekeraars bijzondere aandacht. Gebleken is dat bij bijna de helft van de zorgverzekeraars de bewaartermijnen niet voldoen aan hetgeen daarover is bepaald in wet– en regelgeving.[24]

Als de verzekeringsovereenkomst niet tot stand is gekomen mogen zorgverzekeraars de medische persoonsgegevens maximaal twaalf maanden bewaren (artikel 3.0.7). Acht zorgverzekeraars geven aan deze gegevens helemaal niet te bewaren, omdat geen medische persoonsgegevens worden opgevraagd bij aanmelding voor een verzekering. Veertien zorgverzekeraars bewaren de betreffende gegevens maximaal twaalf maanden. De overige tien zorgverzekeraars

[24] De Rijksarchiefinspectie ziet toe op de naleving van de Archiefwet 1995

bewaren de medische persoonsgegevens langer dan is toegestaan op grond van artikel 3.0.7 van het Addendum. De bewaartermijn die deze zorgverzekeraars hanteren varieert van drie jaar tot onbeperkt.

Na beëindiging van de verzekering mag de zorgverzekeraar de persoonsgegevens maximaal zeven jaar bewaren (artikel 3.0.8). Dertien zorgverzekeraars hanteren een langere bewaartermijn voor de persoonsgegevens dan in het Addendum is bepaald. Zeven zorgverzekeraars hanteren zelfs een onbeperkte bewaartermijn. De overige negentien zorgverzekeraars voldoen wel aan hetgeen in het Addendum is bepaald. Voor de bewaartermijnen van NAW–gegevens en geboortedata kan een zorgverzekeraar afwijkende richtlijnen opstellen. Vier zorgverzekeraars hebben een afwijkende richtlijn opgesteld. De overige zorgverzekeraars hanteren geen andere bewaartermijn.

Voor gegevens over betalingsgedrag van de verzekerde geldt een maximale bewaartermijn van vijf jaar. Drie zorgverzekeraars geven aan deze gegevens in het geheel niet te bewaren. Tien zorgverzekeraars hanteren de bewaartermijn zoals gesteld in artikel 3.4 van het Addendum. De overige negentien zorgverzekeraars hebben een langere bewaartermijn dan toegestaan. Zeven zorgverzekeraars hanteren zelfs een onbeperkte bewaartermijn.

4.3.5 Materiële controle en Misbruik/Oneigenlijk gebruik

Slechts tien zorgverzekeraars hebben in de polisvoorwaarden van de aanvullende verzekering 2008 opgenomen dat materiële controle en fraudeonderzoek wordt verricht overeenkomstig hetgeen daarover voor de zorgverzekering bij of krachtens de Zvw is bepaald. De NZa heeft de overige zorgverzekeraars verzocht deze bepaling op te nemen in de aanvullende voorwaarden voor polisjaar 2009.

Bij de constatering van fraude bij het *aangaan* van de aanvullende verzekering geven alle zorgverzekeraars aan te handelen volgens het Addendum. Het is echter mogelijk dat deze vraag niet alleen is beantwoord voor fraude bij het *aangaan* van de aanvullende verzekering maar ook gedurende de looptijd van de verzekering. Onbedoeld kunnen de resultaten minder betrouwbaar zijn en kunnen hierover geen conclusies worden getrokken.

4.3.6 Omschrijving zorg op nota's en klachten en geschillen

Omschrijving zorg op nota's
Op een enkeling na blijken de zorgverzekeraars te voldoen aan de voorwaarde uit het Addendum, dat bij de informatieverstrekking aan de verzekeringnemer de zorgverzekeraar onnodige gegevens achterwege laat over de gezondheid van andere verzekerden.

De declaraties van zorgaanbieders aan zorgverzekeraars bevatten medische persoonsgegevens – diagnosegegevens – van de verzekerde. Per 1 januari 2008 is de DBC–systematiek ingevoerd binnen de geestelijke gezondheidszorg (GGZ). Onlangs werd in de media gesteld dat door de invoering van de DBC–systematiek in de GGZ de privacy van de GGZ–patiënten niet goed is geborgd. Echter, het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) stemt bij elke voorgenomen substantiële beleidswijziging af met het CBP of de privacy van de verzekerden is geborgd. Voor de wijziging naar het DBC–systeem is dit ook gebeurd. Met oog op de bescherming van de privacy is een aantal voorwaarden opgenomen betreffende gegevens die beslist niet op de factuur mogen worden vermeld.

De DBC–factuur die vanuit de zorgaanbieder naar de zorgverzekeraar gaat, wordt op naam van de patiënt gedeclareerd. Zou dit niet gebeuren, dan zou voor een zorgverzekeraar niet duidelijk zijn of de factuur wel hoort bij iemand die bij hem is verzekerd. Om de privacy van consumenten te waarborgen is veel aandacht geweest voor de manier van factureren en declareren op het gebied van de GGZ. De belangen van de zorgverzekeraar enerzijds – kunnen uitvoeren van de verzekeringsovereenkomst – en de consument anderzijds zijn goed tegen elkaar afgewogen. Echter, er blijft een spanningsveld bestaan. Ook is de zorgverzekeraar gehouden aan het Addendum waarin restrictieve bepalingen zijn opgenomen over onder andere de uitwisseling van persoonsgegevens (artikel 3.0.9) (zie paragraaf 4.2.2 en 4.3.3). Gezien het bovenstaande is er geen reden aan te nemen dat de privacy van de GGZ–patiënt niet is geborgd.

Klachten en geschillen
Vrijwel alle zorgverzekeraars hebben een algemene klachten– en geschillenprocedure waarmee ook klachten over privacy worden afgehandeld. Echter, 13% van de zorgverzekeraars informeert de verzekerde niet over de wijze van afhandeling van klachten over de uitvoering van de Wbp, Gedragscode en het bijbehorende Addendum. Vijf zorgverzekeraars verstrekken de gegevens niet conform het Addendum aan de geschilleninstantie of rechter.

5. Conclusies en aanbevelingen

5.1 Inleiding

Het thematisch onderzoek van de NZa naar de verwerking van persoonsgegevens bij zorgverzekeraars geeft inzicht in de organisatorische en technische maatregelen die zorgverzekeraars hebben getroffen voor zowel de Wbp als het Addendum, hoe deze maatregelen worden gewaarborgd en of deze voldoen aan wet– en regelgeving. Dit hoofdstuk beschrijft de belangrijkste conclusies en geeft een aantal aanbevelingen voor de zorgverzekeraars. De conclusies zijn gebaseerd op de informatie en de antwoorden die zorgverzekeraars hebben verstrekt.[25] De uitkomsten per zorgverzekeraar zijn teruggekoppeld naar de individuele zorgverzekeraar, waarbij ook verbeterpunten zijn geformuleerd.

5.2 Conclusies

Het onderzoek heeft het onderwerp 'privacy' – verwerking van persoonsgegevens – onder de aandacht gebracht bij zorgverzekeraars. Gebleken is dat van het onderzoek een preventieve werking is uitgegaan. Diverse zorgverzekeraars hebben naar aanleiding van de vragenlijst verbeteringen doorgevoerd of verbeterplannen opgesteld. De NZa vindt het belangrijk dat zorgverzekeraars aandacht besteden aan een adequate verwerking van persoonsgegevens omdat dit het belang en de positie van de consument raakt en kan schaden wanneer de verwerking niet juist geschiedt.

Het onderzoek levert een divers beeld op van de verwerking van persoonsgegevens door zorgverzekeraars. De meerderheid van de zorgverzekeraars besteedt voor een groot aantal van de getoetste onderdelen aandacht aan de bepalingen uit de Wbp en het Addendum. Er zijn – afgaande op de door de zorgverzekeraars gegeven antwoorden – geen indicaties dat medische persoonsgegevens onzorgvuldig worden verwerkt. Dit neemt niet weg dat er een aantal punten is waarop belangrijke verbeteringen nodig zijn. Voor de Wbp geldt voor nagenoeg alle zorgverzekeraars dat het vastleggen van procedures voor gegevensverwerking en de controles op de naleving hiervan 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 dient een aantal zorgverzekeraars hun aanmeldformulieren voor de aanvullende verzekering aan te passen.

Gezien het verschillende karakter van de twee onderdelen in dit onderzoek, heeft de NZa zowel conclusies getrokken voor de bepalingen uit de Wbp als uit het Addendum. Onderstaand zijn de voornaamste conclusies voor de Wbp en het Addendum weergegeven.

[25] De peildatum van het onderzoek is september 2007.

5.2.1 Wet bescherming persoonsgegevens

- Bij slechts dertien zorgverzekeraars (41%) ligt de verwerking van persoonsgegevens op alle onderdelen op het gewenste niveau (niveau vier).[26] Bij deze zorgverzekeraars zijn meer dan tien miljoen personen verzekerd.
- Bij de meerderheid van de zorgverzekeraars (59%) ligt de verwerking van persoonsgegevens bij één of meerdere onderdelen niet op het gewenste niveau. Dit betekent dat deze zorgverzekeraars op deze onderdelen geen procedures en maatregelen hebben vastgelegd (niveau 1 en 2) en dat er op deze onderdelen geen controle op de naleving plaatsvindt (niveau 1, 2 en 3).
- Per getoetst onderdeel heeft meer dan de helft van de zorgverzekeraars het gewenste niveau van gegevensverwerking bereikt (niveau vier). Per onderdeel moeten twee tot zestien zorgverzekeraars verbetermaatregelen treffen om ook het vierde niveau te bereiken.
- De onderdelen waarop het beste wordt gescoord zijn de kwaliteit van de gegevensverwerking en de beveiliging. Meer dan 90% van de zorgverzekeraars bevindt zich op deze onderdelen op het gewenste niveau. Bij de beveiliging moet worden opgemerkt dat gegeven de toenemende relevantie van informatie– en communicatietechnologie en de hieraan verbonden technische en organisatorische bedreigingen het nodig is dat de zorgverzekeraar regelmatig het beveiligingsbeleid evalueert en zonodig herziet.
- Voor nagenoeg alle zorgverzekeraars geldt dat het vastleggen van procedures voor gegevensverwerking en de controles op de naleving hiervan aandacht verdienen. Vaak zijn er wel *algemene* procedures en controles aanwezig waarmee privacyaspecten worden geraakt. Toch is het van belang om *specifieke* procedures en *structurele* controles in te voeren voor de verwerking van persoonsgegevens (artikel 9.2 van de Gedragscode).
- Slechts bij een enkele zorgverzekeraar vindt een jaarlijkse controle van het stelsel van verwerkingsmaatregelen en –procedures plaats op grond van artikel 9.1 van de Gedragscode.

5.2.2 Addendum Zorgverzekeraars

- De zorgverzekeraars hebben in grote lijnen de getoetste bepalingen uit het Addendum gewaarborgd. Echter, geen enkele zorgverzekeraar voldoet aan alle bepalingen uit het Addendum. Een mogelijke verklaring hiervoor is de invoering van het Addendum in 2006, tegelijkertijd met de Zvw. Daar komt bij dat het Addendum geen ingrijpende organisatorische aanpassingen van zorgverzekeraars vergt, waardoor het gevoel kan ontstaan over het algemeen wel aan de bepalingen te voldoen.
- Van de 30 zorgverzekeraars die naast de zorgverzekering ook aanvullende verzekeringen aanbieden, is bij zeven zorgverzekeraars niet duidelijk dat de in het aanmeldformulier opgenomen vragen over het strafrechterlijk verleden uitsluitend moeten worden ingevuld bij het afsluiten van een aanvullende verzekering. Deze zorgverzekeraars moeten hun aanmeldformulieren direct aanpassen.
- Zorgverzekeraars dienen vooral verbeteringen door te voeren bij de bewaartermijnen voor persoonsgegevens en bij het opnemen van bepalingen in de aanvullende voorwaarden omtrent materiële controle en misbruik en oneigenlijk gebruik.

[26] Dit gewenste niveau vier houdt in dat de zorgverzekeraar procedures heeft vastgelegd en maatregelen heeft getroffen om de verwerking van persoonsgegevens te waarborgen. De procedures en maatregelen zijn bekend bij de medewerkers en de naleving hiervan wordt gecontroleerd.

- De verantwoordelijkheden van de medisch adviseur komen bij enkele zorgverzekeraars niet overeen met hetgeen is bepaald in het Addendum. Dit is echter wel van belang, aangezien het gaat om het medisch beroepsgeheim van de medisch adviseur. Ook 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.
- Ongeveer een kwart van de zorgverzekeraars geeft aan geen beleid of richtlijnen te hebben voor het recht van de betrokkene op inzage, correctie, afscherming of verwijdering van zijn persoonsgegevens. De NZa vindt het belangrijk dat zorgverzekeraars een dergelijk beleid hebben omdat dit direct de positie van de verzekerde raakt.
- Een derde van de zorgverzekeraars heeft aangegeven geen acceptatiebeleid voor de aanvullende verzekering te voeren. Hierdoor is een aantal bepalingen uit het Addendum niet van toepassing.
- Belangrijk is dat het algemene beeld ten aanzien van het Addendum sterk kan wijzigingen als zorgverzekeraars de komende jaren wel acceptatiebeleid gaan voeren. Immers, vier van de elf getoetste hoofdonderdelen – acceptatie, uitwisseling – en overig gebruik van persoonsgegevens en aanmeldformulieren – hebben betrekking op het acceptatiebeleid.

5.2.3 Verschillen tussen groepen zorgverzekeraars

Verschillen tussen de grote en kleine zorgverzekeraars
Tussen de vijf grootste zorgverzekeraars (> 1.000.000 verzekerden) en vijf kleinste zorgverzekeraars (< 150.000 verzekerden) zijn verschillen zichtbaar in de verwerking van persoonsgegevens. De grote zorgverzekeraars scoren beter dan de kleine zorgverzekeraars op de volgende punten:
- controles op de geldende procedures en maatregelen;
- de verantwoordelijkheden van de medisch adviseur en de processen die onder zijn verantwoordelijkheid vallen conform het Addendum;
- het informeren van de verzekerde over de wijze van afhandeling van de klachten over de Wbp, Gedragscode en het Addendum.

Verschillen verzekeraars met en zonder relatie met hypotheken en levens– en pensioenverzekeringen
Tussen zorgverzekeraars die wel en die geen relatie hebben met hypotheekverstrekkers en aanbieders van levens– en/of pensioenverzekeringen zijn verschillen zichtbaar. De zorgverzekeraars waarbij deze relatie aanwezig is scoren beter dan de verzekeraars waarbij deze relatie niet aanwezig is op de volgende punten:
- controle op een transparante verwerking;
- vastlegging en controle met betrekking tot de doelbinding, rechtmatige grondslag en rechten van de betrokkene;
- er is vaker een interne regeling op grond van artikel 3.0.2 van het Addendum.

5.3 Aanbevelingen

Naar aanleiding van de onderzoeksbevindingen, zoals verwoord in de conclusies voor de Wbp en het Addendum in paragraaf 5.2, doet de NZa de volgende aanbevelingen:
- hoewel zorgverzekeraars aandacht besteden aan de privacybewustzijn van de medewerkers dienen de zorgverzekeraars de medewerkers beter te informeren over procedures en maatregelen voor de verwerking van persoonsgegevens;

- om deze maatregelen en procedures te borgen is het van belang om structurele controles op de naleving ervan, specifiek gericht op privacy, in te voeren. Dit kan bijvoorbeeld in de vorm van een jaarlijkse privacy audit (conform artikel 9.2 van de Gedragscode);
- de zorgverzekeraars moeten voor zichzelf duidelijkheid krijgen in hoeverre bij hun organisatie sprake is van een 'bewerker' (zie paragraaf 3.2.5). Ook verdient de controle op het beveiligingsniveau bij de bewerker door de zorgverzekeraar de nodige aandacht;
- De Gedragscode Verwerking Persoonsgegevens Financiële Instellingen en het bijbehorende Addendum Zorgverzekeraars langs de organisatie leggen om te bepalen waar de zorgverzekeraar organisatorische aanpassingen moet doorvoeren. In elk geval dient aandacht te worden besteed aan de bepalingen over de bewaartermijnen en het opnemen van bepalingen omtrent materiële controle en misbruik en oneigenlijk gebruik in de aanvullende voorwaarden;
- wanneer zorgverzekeraars – verdere – acceptatievoorwaarden voor de aanvullende verzekering invoeren, moet hierbij rekening worden gehouden met de bepalingen uit het Addendum.

5.4 Vervolgonderzoek

De de NZa heeft bij de terugkoppeling van de bevindingen naar de zorgverzekeraar verbeterpunten geformuleerd. De zorgverzekeraars moeten uiterlijk 1 juni 2008 verantwoording aan de NZa afleggen over de opvolging van de verbeterpunten met betrekking tot de aanmeldformulieren. Over de opvolging van de overige verbeterpunten moeten de zorgverzekeraars zich uiterlijk 1 oktober 2008 verantwoorden. De NZa zal scherp toezien op de opvolging van de verbeterpunten en hierover in 2009 rapporteren.

Daarnaast monitort de NZa de ontwikkelingen in de verwerking van persoonsgegevens via de maatschappelijk verslagen van zorgverzekeraars en door signaaltoezicht.

Postbus 3017
3502 GA Utrecht

T 030 296 81 11
E info@nza.nl
I www.nza.nl

De Nederlandse Zorgautoriteit (NZa) is de toezichthouder op alle zorgmarkten in Nederland en ziet toe op zowel de zorgaanbieders als verzekeraars, op zowel de curatieve markten als op de markten voor langdurige zorg. De NZa heeft een aantal wettelijke taken: het vaststellen van prijzen en budgetten, markttoezicht en waken over goede uitvoering van de Zorgverzekeringswet en de AWBZ. Daarbij staat het belang van de consument voorop: er moet voldoende, toegankelijke, betaalbare en goede zorg zijn.

De NZa is marktmeester voor die delen van de zorgmarkt waar vrije prijzen gelden. Als blijkt dat op een bepaalde deelmarkt geen daadwerkelijke concurrentie tot stand komt, heeft de NZa verschillende instrumenten om in te grijpen. Markttoezicht gaat ook over het bevorderen van inzichtelijkheid (transparantie) van markten en over goede keuze-informatie voor consumenten. Informatie moet helder en vergelijkbaar zijn en mag niet misleidend zijn.

Als er (nog) geen vrije prijzen gelden, stelt de NZa tarieven of prestatiebeschrijvingen vast voor een groot deel van de gezondheidszorg. Het toezicht op de zorgverzekeringswetten bestaat er bijvoorbeeld uit dat de NZa bewaakt dat verzekeraars aan hun zorgplicht en acceptatieplicht voldoen en dat ze zich houden aan het verbod op premiedifferentiatie.
De NZa zet ook in op flinke vermindering van de bureaucratie. Ze neemt haar eigen regels grondig onder de loep, maar spreekt ook beleidsmakers, andere toezichthouders én marktpartijen aan op hun verantwoordelijkheid als dat nodig is om het aantal regels en voorschriften te beperken.