Rapport

Zorgverzekeraars, controles en privacyvoorschriften

Onderzoek naar de naleving van privacyregels bij de uitvoering van controles door zorgverzekeraars

augustus 2016

Inhoud

Vooraf

Dit rapport geeft inzicht in de wijze waarop zorgverzekeraars omgaan met medische persoonsgegevens (gegevens betreffende de gezondheid) bij de uitvoering van controles. Als zorgverzekeraars bij de uitvoering van dergelijke controles gebruik moeten maken van medische persoonsgegevens, dienen zij daarmee uiterst zorgvuldig om te gaan. Daarvoor zijn dan ook regels gesteld, waaronder de privacyregeling GGZ, die extra waarborgen biedt voor burgers die gebruik maken van GGZ-zorg.

Aanleiding voor dit rapport vormen signalen over de naleving van de privacyregeling GGZ. Het onderzoek van de NZa laat zien dat zorgverzekeraars deze regeling in zijn algemeenheid goed naleven. De NZa heeft bij één zorgverzekeraar een overtreding vastgesteld, die inmiddels is hersteld.

Naast dit specifieke onderwerp heeft de NZa onderzoek verricht naar het privacybeleid, de organisatie van controles en de communicatie over de uitvoering van controles door zorgverzekeraars. Hoe beter deze zaken geregeld zijn, hoe beter zorgverzekeraars de geldende privacyregels naleven. Ook kan dit bijdragen aan het vertrouwen van zorgaanbieders en verzekerden in de wijze waarop zorgverzekeraars controles uitvoeren. Uit het onderzoek blijkt dat zorgverzekeraars deze zaken in het algemeen op orde hebben.

Dit laat onverlet dat er mogelijkheden tot verbetering bestaan, die wij hebben vastgelegd in algemene aanbevelingen aan alle verzekeraars en in aanbevelingen per zorgverzekeraar.

Alle verzekeraars hebben aangegeven de aanbevelingen met betrekking tot beleid, organisatie en communicatie van controles, te zullen opvolgen. Enkele zorgverzekeraars hebben reeds gedurende de consultatiefase van de bevindingen opvolging gegeven aan enkele aanbevelingen.

De NZa vindt het positief dat zorgverzekeraars in het algemeen hun zaken op orde hebben als het gaat om de omgang met persoonsgegevens. Dit laat onverlet dat de NZa alert zal blijven op signalen over de wijze waarop zorgverzekeraars omgaan met persoonsgegevens en zal (in overleg met de Autoriteit Persoonsgegevens), als daartoe aanleiding bestaat, maatregelen treffen richting de betreffende verzekeraars.

De Nederlandse Zorgautoriteit,

dr. M.J. Kaljouw
voorzitter Raad van Bestuur

Managementsamenvatting

1. Inleiding

Medische persoonsgegevens zijn gevoelige gegevens. Deze gegevens zijn dan ook, indien mogelijk, alleen toegankelijk voor de direct betrokkenen: de patiënt en zijn arts. Inzage in medische persoonsgegevens kan voor zorgverzekeraars noodzakelijk zijn voor de uitvoering van controles – om te controleren of de gedeclareerde zorg is geleverd, onderdeel is van de verzekering en of deze passend is - en aldus bij te dragen aan de betaalbaarheid van zorg. De Zorgverzekeringswet stelt de voorwaarden voor het verwerken van medische gegevens, deels uitgewerkt in de Regeling zorgverzekering. Zorgverzekeraars Nederland heeft hiervoor Uniforme Maatregelen en het Protocol Materiële Controle opgesteld. Een andere waarborg voor verzekerden is de privacyregeling GGZ: deze regeling biedt de mogelijkheid tot het weglaten van diagnose-informatie op de declaratie.
Het onderzoek bestaat uit twee onderdelen: een specifiek deel, gericht op de naleving van de privacyregeling GGZ[1] (hierna ook wel: de privacyregeling), en een algemeen deel (communicatie, organisatie en beleid), over de vraag, in hoeverre de organisatie van een zorgverzekeraar waarborgen biedt voor correcte verwerking van medische persoonsgegevens. Naast dit algemene rapport heeft de NZa (niet-openbare) individuele rapporten, met daarin individuele bevindingen en aanbevelingen, opgesteld per verzekeraar.
De NZa geeft opvolging aan de bevindingen, zoals weergegeven in dit algemeen rapport en in de individuele rapporten. Voor één zorgverzekeraar leidt dat tot een periodieke verantwoordingsplicht over de uitvoering van de privacyregeling. Een andere verzekeraar heeft specifiek moeten rapporteren over de ontwikkeling van zijn privacybeleid.

2. Onderzoek

De NZa houdt toezicht op de wijze waarop zorgverzekeraars omgaan met persoonsgegevens bij - onder meer - de uitvoering van controles, als onderdeel van haar toezicht op de rechtmatige uitvoering door zorgverzekeraars van de Zvw. Voor de verwerking van persoonsgegevens door zorgverzekeraars gaat het daarbij om de normen van artikel 87 Zvw, met betrekking tot de uitvoering van controles uitgewerkt in hoofdstuk 7 van de Regeling zorgverzekering. Daarnaast houdt de NZa toezicht op de privacyregelingen (waaronder: de privacyregeling GGZ) die de NZa heeft vastgesteld. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de verwerking van persoonsgegevens in zijn algemeenheid. Daaronder valt ook de verwerking van medische persoonsgegevens door zorgverzekeraars.

In 2014 heeft de NZa zorgverzekeraars gevraagd naar de naleving van de privacyregeling GGZ, waarop alle zorgverzekeraars antwoordden dat zij deze naleven. Desalniettemin ontving de NZa daarna nog 14 signalen,

[1] De NZa heeft voor de sector medisch specialistische zorg (MSZ) eveneens een privacyregeling opgesteld, die een vrijwaring biedt van de verplichte vermelding van zorgactiviteiten op de nota. Deze regeling is niet afzonderlijk onderzocht, onder meer omdat de NZa daarover vrijwel geen signalen heeft ontvangen.

dat de privacyregeling niet altijd correct zou worden nageleefd. De zorgen van verschillende melders en enkele betrokken organisaties van GGZ-zorgaanbieders gaven de NZa aanleiding voor dit onderzoek.

Het regelgevend kader voor toepassing van de privacyregeling is vastgelegd in de NZa-Regeling Gespecialiseerde Geestelijke Gezondheidszorg (de regeling). Artikel 3.5 van de regeling stelt dat verzekerden en zorgverleners samen kunnen aangeven dat zij geen tot de diagnose herleidbare informatie op de factuur en in het DBC Informatie Systeem (DIS) willen opnemen. Hiertoe tekenen zij een privacyverklaring, die aan de verzekeraar wordt overlegd. De regeling geeft verder de mogelijkheid (artikel 3.5, lid 4) dat de zorgaanbieder een tarief kan declareren dat niet herleidbaar is naar de diagnose.

De privacyregeling vormt een specifiek onderdeel van de bredere vraag, in hoeverre de organisatie van een zorgverzekeraar waarborgen biedt voor een correcte verwerking van persoonsgegevens. Het tweede gedeelte van het onderzoek richt zich op deze vraag. Deze vraag valt uiteen in drie onderwerpen: (1) beleid; (2) organisatie en (3) communicatie.

Voor het onderzoek heeft de NZa, door middel van een informatieverzoek op grond van de Wmg, alle verzekeraars opgedragen om een gedocumenteerde beschrijving te geven van de wijze waarop zij omgaan met de verwerking van persoonsgegevens in het algemeen en, meer in het bijzonder, de privacyregeling GGZ. Onderdeel daarvan was uiteraard hoe vaak er een beroep op deze regeling wordt gedaan en hoe de betreffende declaraties dan worden afgehandeld. Binnen het onderzoek zijn aan een aantal verzekeraars concrete signalen voorgelegd over hun omgang van persoonsgegevens. Zij hebben de NZa gerapporteerd over de afhandeling daarvan.
Op basis van de verkregen informatie hebben wij alle zorgverzekeraars onze algemene concept bevindingen toegestuurd - geldend voor alle zorgverzekeraars – met daarnaast, ter consultatie, de afzonderlijke bevindingen en aanbevelingen per zorgverzekeraar. Vervolgens heeft op 17 juni 2016 een bijeenkomst plaats gehad met vertegenwoordigers van de zorgverzekeraars, waarin zij hun zienswijze op de bevindingen mondeling hebben toegelicht. Daarnaast heeft een consultatie plaatsgevonden met vertegenwoordigende organisaties van GGZ – aanbieders. De opmerkingen van deze organisaties zijn in het rapport verwerkt.

De NZa heeft de inhoud van het rapport voorgelegd voor advies aan de Autoriteit Persoonsgegevens (AP) en heeft het advies in het rapport verwerkt.

3. Bevindingen en conclusies

- Uit het onderzoek volgt dat in 2014 ruim 900 cliënten gebruik maakten van een privacyverklaring in de GGZ (variërend per verzekeraar van 3 tot 518).

- Alle zorgverzekeraars kennen een afzonderlijke werkwijze voor uitvoering van de privacyregeling GGZ. In vier gevallen was deze niet aantoonbaar of niet duidelijk vastgelegd. Op aangeven van de NZa is inmiddels voor die vastlegging gezorgd.

- Eén verzekeraar voerde de privacyregeling GGZ niet goed uit, omdat de verzekeraar diagnose informatie opvroeg waar dat niet

was toegestaan. Om zeker te stellen dat de verzekeraar zich in de toekomst blijvend aan de regels zal houden, heeft de NZa de verzekeraar een periodieke verantwoordingsplicht gedurende een jaar, eindigend op 31 maart 2017, opgelegd over de wijze waarop uitvoering wordt gegeven aan de privacyregeling GGZ.

- Alle zorgverzekeraars bieden de mogelijkheid tot hanteren van een afwijkend tarief, zodat de diagnose op de factuur niet kan worden achterhaald.

- De mogelijkheid tot hanteren van een afwijkend tarief, zoals voorzien in de regeling declaratiebepalingen DBC's in de curatieve GGZ[2], werkt in de praktijk (en de NZa heeft op dit onderdeel dan ook geen overtredingen vastgesteld). Aangezien echter zorgverzekeraars verschillende werkwijzen toepassen, zullen zij duidelijkheid moeten blijven bieden over de werkwijze die ieder van hen toepast.

- Alle verzekeraars besteden beleidsmatig aandacht aan privacy.[3] Waar verzekeraars hun privacybeleid op één plaats of in één document beschrijven, bleek het eenvoudiger om de naleving van privacyregelgeving aantoonbaar te maken en het beleid te kunnen evalueren.
  De verschillen tussen verzekeraars in organisatie en inrichting van de verplichte formele en materiële controles kunnen zorgen voor onduidelijkheid bij zorgaanbieders over de vraag, wat verzekeraars van hen verwachten bij de uitvoering van controles. Die onduidelijkheid kan leiden tot terughoudendheid in de medewerking aan controles.

- In enkele gevallen hanteert de verzekeraar niet een strikt onderscheid tussen formele en materiële controles. Enkele verzekeraars hanteren een aanvullende vorm van controles waarvan niet expliciet duidelijk is welke vorm dit betreft: formeel of materieel. De kwalificatie van een controle, als een materiële of formele controle, is bepalend voor de vraag in hoeverre de verzekeraar (persoons-)gegevens mag opvragen. Het is daarom belangrijk dat verzekeraars duidelijkheid bieden over de benaming of kwalificatie van de controles die zij uitvoeren.

- Bij de uitvoering van controles werken alle verzekeraars met één of meer zogenoemde Functionele Eenheden. Een Functionele Eenheid is een eenheid van deskundige medewerkers binnen de organisatie van een zorgverzekeraar, die voor specifieke doeleinden en onder verantwoordelijkheid van de medisch adviseur betrokken zijn bij de verwerking van persoonsgegevens betreffende iemands gezondheid.[4] De positie van de medisch adviseur binnen de organisatie is verschillend geregeld. Behalve zijn positie, varieert ook de rol van de medisch adviseur in het controleproces: die kan adviserend, verantwoordelijk (bijvoorbeeld voor de verwerking van persoonsgegevens bij de uitvoering van detailcontroles) of uitvoerend zijn. Die onderlinge verschillen kunnen bij

[2] Artikel 10.4 van Regeling NR/CU-524, Regeling declaratiebepalingen DBC's in de curatieve GGZ.
[3] Het vastleggen van privacybeleid is nog niet voorgeschreven, maar de in april 2016 door de EU vastgestelde Algemene verordening gegevensbescherming zal daar regels over stellen. De Algemene verordening gegevensbescherming (2016/679) is formeel aangenomen op 27 april 2016 en gepubliceerd in Pb EU L119. De implementatietermijn van twee jaar verstrijkt op 25 mei 2018.
[4] Deze definitie volgt uit de Gedragscode.

zorgaanbieders leiden tot terughoudendheid in de medewerking aan controles.

- Verzekeraars maken bij het opvragen van informatie wisselend gebruik van standaarden. Met name de kleinere verzekeraars maken hiervan minder gebruik. Het werken met standaard teksten is niet verplicht, maar kan wel nuttig zijn voor een heldere voorlichting en uniformiteit.

- Bijna alle zorgverzekeraars laten zien op welke wijze en met welke resultaten zij de effectiviteit en kwaliteit van de privacy-organisatie bewaken. Ook dat kan leiden tot terughoudendheid bij zorgaanbieders in hun relatie met zorgverzekeraars.

4. Aanbevelingen aan verzekeraars

Met betrekking tot de onderdelen communicatie, organisatie en beleid van controles is het de verantwoordelijkheid van zorgverzekeraars zelf om deze in te richten, zodanig dat zij voldoen aan de daarvoor geldende privacyregels. De NZa heeft op deze onderdelen geen overtredingen vastgesteld en concludeert dan ook dat verzekeraars hun verantwoordelijkheid op deze onderdelen nemen. Desalniettemin bieden de bevindingen aanleiding voor de NZa om aan verschillende zorgverzekeraars individuele aanbevelingen te doen teneinde de organisatie, communicatie en beleid met betrekking tot de naleving van privacyregels, verder te versterken. De aanbevelingen zijn niet in gelijke mate van toepassing op iedere zorgverzekeraar; zij geven niettemin een algemeen beeld van verdere verbeteringen die zorgverzekeraars in zijn algemeenheid zouden moeten doorvoeren.

Samengevat betreft het de volgende aanbevelingen:

1. Privacyregeling GGZ: Zorg voor een heldere en voor zorgaanbieders kenbare beschrijving van de wijze waarop de privacyregeling GGZ wordt uitgevoerd. De werkwijze ten aanzien van (het bepalen van) afwijkende tarieven maakt daar deel van uit.

2. Privacybeleid: Zorg voor vastlegging van privacybeleid in één document. Een dergelijk document dient ook voor buitenstaanders kenbaar en begrijpelijk te zijn. Neem daarin periodieke monitoring en evaluatie van dit beleid op. Verantwoording over de noodzaak en de wijze van het uitvoeren van controles is beter mogelijk wanneer verzekeraars tevoren hun beleid terzake bepalen en vastleggen.

3. Organisatie van controles: Beschrijf en borg een adequate privacyorganisatie. Creëer daarin duidelijk onderscheid in de doelen van controles: gericht op de formele aspecten van de declaratie (waaronder bijvoorbeeld de vraag: valt de zorg onder het verzekerde pakket) of op de vraag of de zorg is geleverd en/of deze het meest was aangewezen? Dit is van belang voor de vraag in hoeverre de zorgverzekeraar (persoons-)gegevens mag verwerken. Een beschrijving van de positie en verantwoordelijkheden van de medisch adviseur en de Functionele Eenheden maakt hier deel van uit.

4. Communicatie over controles: Kies een open en aanspreekbare opstelling richting zorgaanbieders bij de uitvoering van controles. Hanteer waar mogelijk standaarden voor het opvragen van informatie. Dit creëert meer duidelijkheid voor de zorgaanbieder over de vraag, waarom de informatie wordt opgevraagd en wat van de zorgaanbieder wordt verwacht.

Bij de afronding van dit onderzoek en deze rapportage zijn de verschillende (individuele) aanbevelingen aan alle verzekeraars gepresenteerd. Zij hebben deze ter hand genomen en een deel ervan is reeds ten tijde van de publicatie van dit rapport uitgevoerd. De reeds uitgevoerde aanpassingen zien bijvoorbeeld op het actualiseren van het 'privacy statement', het publiceren van een publieksvriendelijke versie van het controleplan en aanpassing van de werkwijze bij detailonderzoeken (door standaard de informatie uitvraag te laten ondertekenen door de medisch adviseur).
De individuele aanbevelingen, waarvan de zorgverzekeraars hebben verklaard deze te zullen opvolgen, zien op de borging van beleid en processen (door betere vastlegging ervan), het verhelderen van de interne positie van de medisch adviseur en het verbeteren van de communicatie richting verzekerden en zorgaanbieders.
Met betrekking tot de uitvoering van de privacyregeling GGZ heeft de NZa vastgesteld dat deze regeling in zijn algemeenheid (zie onder "bevindingen") adequaat wordt uitgevoerd. In een enkel geval echter heeft de NZa vastgesteld dat een zorgverzekeraar de regeling onjuist uitvoerde, omdat de verzekeraar diagnose informatie opvroeg waar dat niet was toegestaan. Om zeker te stellen dat de verzekeraar zich in de toekomst blijvend aan de regels zal houden, heeft de NZa de verzekeraar een periodieke rapportageplicht opgelegd over de wijze waarop uitvoering wordt gegeven aan de privacyregeling GGZ.

5. Vervolg

De NZa heeft één verzekeraar opgedragen zich periodiek te verantwoorden. De verantwoording ziet op de wijze waarop deze verzekeraar omgaat met de privacyregeling GGZ. Daarnaast heeft de NZa één verzekeraar opgedragen, te rapporteren over de ontwikkeling van privacybeleid door het opstellen van een zelfstandig beleidsdocument. Aan deze verplichting heeft de zorgverzekeraar inmiddels voldaan.

De NZa heeft voor zijn onderzoek de signalen tot en met 1 augustus 2016 meegenomen. De NZa zal daarnaast alert blijven op signalen over de wijze waarop zorgverzekeraars omgaan met persoonsgegevens. De NZa zal eventuele signalen onderzoeken en zal, als daartoe aanleiding bestaat, maatregelen treffen richting verzekeraars.

1. Inleiding

1.1 Persoonsgegevens

Dit onderzoek richt zich op de wijze waarop zorgverzekeraars omgaan met de privacyregeling GGZ en – meer algemeen - de manier waarop de organisatie voor verwerking van persoonsgegevens is ingericht.

Medische persoonsgegevens zijn gevoelige gegevens. Voor het omgaan met deze gegevens gelden dan ook strenge, wettelijke vereisten. Organisaties mogen deze gegevens alleen verwerken als aan bijzondere voorwaarden wordt voldaan.

Met medische persoonsgegevens worden bedoeld: persoonsgegevens betreffende iemands gezondheid in de zin van artikel 16 van de Wet bescherming persoonsgegevens (Wbp). Het begrip "gezondheid" moet ruim worden opgevat, het gaat om alle gegevens over iemands geestelijke of lichamelijke gezondheid.[5] Zo is ook het enkele gegeven dat iemand in behandeling is bij een bepaalde zorgaanbieder een persoonsgegeven betreffende de gezondheid.[6]

Voor de uitoefening van hun taken beschikken verzekeraars over medische persoonsgegevens en verwerken zij deze gegevens. Voor de verwerking van persoonsgegevens geldt in zijn algemeenheid dat – op grond van de Wbp - een organisatie alleen persoonsgegevens mag verwerken als dat noodzakelijk is voor een bepaald doel.
Medische persoonsgegevens zijn bovendien bijzondere persoonsgegevens: omgang daarmee is aan extra voorwaarden onderworpen. Welke voorwaarden dat zijn, wordt uitgewerkt in het regelgevend kader (zie verder onder hst. 2.2).

1.2 Toezicht op de naleving van privacyvoorschriften zorgverzekeraars

De NZa heeft als taak, op grond van artikel 16, eerste lid, van de Wmg, om toezicht te houden op de rechtmatige uitvoering door zorgverzekeraars van de Zvw. Voor de verwerking van persoonsgegevens door zorgverzekeraars gaat het daarbij om de normen zoals vastgelegd in artikel 87 Zvw, met betrekking tot de uitvoering van controles uitgewerkt in hoofdstuk 7 van de Regeling zorgverzekering. Dat leidt ertoe dat de NZa in haar toezicht rekening houdt met de wijze waarop zorgverzekeraars omgaan met persoonsgegevens bij - onder meer - de uitvoering van controles. Daarnaast houdt de NZa toezicht op de naleving van privacyregelingen (waaronder de privacyregeling GGZ) die de NZa heeft vastgesteld.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de verwerking van persoonsgegevens in zijn algemeenheid. Daaronder valt ook, de verwerking van medische persoonsgegevens door zorgverzekeraars.

Dit betekent dat de bevoegdheden van de AP en NZa, voor zover die betrekking hebben op de verwerking van persoonsgegevens door zorgverzekeraars bij de uitvoering van controles op grond van hoofdstuk

[5] Kamerstukken II, 1997/98, 25 892, nr. 3, p. 109.
[6] Kamerstukken II, 1997/98, 25 892, nr. 3, p. 101; Handelingen II, 2004/05, 29441, p. 821. Zie ook Hoge Raad 3 maart 2009.

7 Regeling zorgverzekering (Rzv), elkaar kunnen overlappen. Om overlap van werkzaamheden in de praktijk te voorkomen, hebben de NZa en de AP afspraken gemaakt over de onderlinge samenwerking op dit terrein.[7] Wegens de algemene taak van de AP als toezichthouder op de verwerking van persoonsgegevens, is dit rapport voorafgaande aan de bekendmaking, aan de AP voorgelegd en heeft zij hierop haar advies gegeven. Het advies van de AP is in het rapport verwerkt.

[7] https://www.nza.nl/organisatie/overdenza/samenwerking/

2. Onderzoek

2.1 Concrete aanleiding onderzoek

Aanleiding van het onderzoek vormen signalen die de NZa heeft ontvangen in de periode van 2014 tot eind 2015 over de naleving van de privacyregeling. Naar aanleiding van eerdere signalen in 2014 heeft de NZa destijds een informatieverzoek (op grond van artikel 61 Wmg) gedaan bij de zorgverzekeraars met de vraag in hoeverre zij de privacyregeling naleven. In reactie daarop hebben alle zorgverzekeraars gesteld dat zij de privacyregeling naleefden. Desalniettemin ontving de NZa daarna nieuwe signalen, die erop wezen dat de privacyregeling niet in alle gevallen werd nageleefd. Dit leidde tot onzekerheid over de vraag, of de privacyregeling door zorgverzekeraars correct werd uitgevoerd en op welke wijze zorgverzekeraars omgaan met deze regeling. De signalen vormden dan ook aanleiding voor de NZa om een onderzoek in te stellen.

In december 2015 heeft de Autoriteit Persoonsgegevens (destijds nog CBP geheten) bovendien een uitvraag gedaan bij vier zorgverzekeraars over het opvragen van verwijsbrieven en behandelplannen bij verzekerden met een privacyverklaring. De zorgverzekeraars verklaarden in een reactie op deze beide uitvragen dat zij handelden conform de regelgeving. Ook na deze verklaring heeft de NZa echter nog vragen ontvangen over de naleving van de privacyregeling, wat de noodzaak van een onderzoek heeft onderstreept. Deze vragen hadden voornamelijk betrekking op het mogelijk door verzekeraars opvragen van meer informatie dan noodzakelijk is voor controles die zij op grond van de Zorgverzekeringswet uitvoeren. In een geval was er zelfs sprake van een privacyverklaring, waarbij de NZa een overtreding heeft vastgesteld met betrekking tot de uitvoering van deze privacyregeling. De verzekeraar heeft - op aangeven van de NZa en in samenspraak met de AP - de overtreding beëindigd. De NZa heeft de verzekeraar een verantwoordingsplicht opgelegd (zie ook verderop). Uit een aantal vragen bleek ook, dat voor zorgverleners niet altijd duidelijk is welke controles verzekeraars met welke diepgang kunnen doen.

2.2 Regelgevend kader

2.2.1 Persoonsgegevens

Zorgverzekeraars zijn bij de uitvoering van de Zorgverzekeringswet (Zvw) gebonden aan de privacyregels.

In de Wet bescherming persoonsgegevens (Wbp) is bepaald dat persoonsgegevens alleen verwerkt mogen worden als dit noodzakelijk is voor één van de in de Wbp genoemde grondslagen voor verwerking (artikel 8 Wbp). Bovendien mogen persoonsgegevens alleen worden verwerkt als zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn. Bij het verenigbaar gebruik speelt de vraag voor welke doeleinden de verzekeraar de verzekerdengegevens verder mag gebruiken. Persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9 Wbp).

Artikel 16 Wbp definieert medische persoonsgegevens als bijzondere persoonsgegevens en bepaalt dat het verwerken van deze gegevens niet is toegestaan, tenzij sprake is van bepaalde uitzonderingen. De artikelen 21 (in het bijzonder: lid 1 sub b) en 23 (in het bijzonder: lid 1 sub f) Wbp regelen uitzonderingen op dit verbod - en maken het mogelijk dat onder voorwaarden medische persoonsgegevens door zorgverzekeraars, onder andere bij de uitvoering van controles, kunnen worden verwerkt.

Artikel 87 Zvw regelt dat zorgaanbieders aan zorgverzekeraars de (medische) gegevens verstrekken die noodzakelijk zijn voor de uitvoering van de zorgverzekering of de Zorgverzekeringswet. Deze bepaling regelt ook de bevoegdheid om bij de uitvoering van controles inzage te verkrijgen in medische persoonsgegevens. De regels en waarborgen voor de verwerking van persoonsgegevens door zorgverzekeraars bij de uitvoering van controles zijn nader uitgewerkt in hoofdstuk 7 van de Regeling Zorgverzekering. Zorgaanbieders zijn verplicht mee te werken aan het verstrekken van persoonsgegevens als dat noodzakelijk is voor de uitvoering van de Zvw.[8]

Verwerking vindt in de meeste gevallen plaats binnen de organisatie van de verzekeraar. Daarnaast kan de verwerking (waaronder ook: de verwerking ter uitvoering van controles) plaats vinden door andere partijen, in opdracht van de verzekeraar. Daar valt te denken aan het door gevolmachtigd agenten uitvoeren van machtigings- of declaratieprocessen, of aan door de zorgverzekeraars gezamenlijk georganiseerde processen. Het verwerken van persoonsgegevens geschiedt echter steeds onder verantwoordelijkheid van de zorgverzekeraar bij wie men verzekerd is. Die verantwoordelijkheid wordt voor wat betreft het conform de Wbp verwerken van persoonsgegevens onder andere geborgd in bewerkersovereenkomsten.

Vóór de invoering van hoofdstuk 7 Rzv vormde de gedragscode de noodzakelijke basis voor uitvoering van controles door zorgverzekeraars. De Minister van VWS achtte het niet gewenst dat een sluitende wettelijke grondslag voor formele en materiële controle structureel afhankelijk was van zelfregulering en een goedkeuringsprocedure op grond van de Wbp. Derhalve is die noodzakelijke wettelijke grondslag beschreven en nader gespecificeerd in een ministeriële regeling, gebaseerd op artikel 87, zesde lid, van de Zvw.[9] Deze regeling geeft specifieke voorschriften over de uitvoering van controles door zorgverzekeraars.

Bij het afsluiten van dit rapport is nog aanhangig het wetsvoorstel VTO Wmg, waarmee een deel van de bepalingen uit de Regeling zorgverzekering wordt verplaatst naar de Wmg. De verplaatsing voorziet in het geven van een steviger (want: formeel wettelijke) verankering van de controles, aangevuld met aangepaste aanleveringsverplichtingen voor zorgaanbieders.[10] De wijziging heeft geen gevolgen voor het afwegingskader: het blijft van groot belang dat zorgverzekeraars toezicht kunnen uitoefenen op uitgaven voor verzekerde zorg en dat daarbij een zorgvuldige omgang met de persoonsgegevens van verzekerden gewaarborgd is.[11]

[8] Deze verplichting zal worden uitgebreid in de aanpassingen van de Zvw volgens het wetsvoorstel VTO Wmg, Kamerstukken II, 33 980.
[9] Staatscourant 2010, 10581.
[10] Kamerstukken II, 33 980.
[11] Zie: Brief van de Minister aan de Tweede Kamer, "Privacywaarborgen materiële controle", kenmerk 913309-146902-Z (TK 2015-2016, 33980, nr. 10), 8 maart 2016.

2.2.2 Organisatie, beleid en communicatie

Naast de bovengenoemde regels die gelden voor het verwerken van persoonsgegevens voor formele en materiële controles, gelden regels voor de inrichting van de organisatie van een zorgverzekeraar, die gevolgen kunnen hebben voor de verwerking van persoonsgegevens. Het doel van deze regels is het versterken van de beheersing en beveiliging van de organisatie van een zorgverzekeraar. Daaronder valt ook, dat wordt geborgd dat de verwerking van persoonsgegevens (ter uitvoering van controles) in de organisatie in overeenstemming met de Wbp plaatsvindt.

Deze regels zijn onder andere te vinden in de Wet op het financieel toezicht (Wft), het Besluit prudentiële regels Wft (Bpr) en de Wmg.[12] De essentie van deze regelgeving is dat de verzekeraar zichzelf zodanig dient te organiseren dat hij kan voldoen aan de relevante wet- en regelgeving en dat hij de risico's beheerst die het realiseren van zijn doelstellingen kunnen bedreigen. De Wbp is onderdeel van de relevante wet- en regelgeving die op verschillende onderdelen voorschrijft dat zorgverzekeraars passende maatregelen nemen om onrechtmatige verwerking van persoonsgegevens te voorkomen.[13]

De eisen van het inrichten van een adequate administratieve organisatie en interne beheersing maken geen uitzondering voor de verwerking van persoonsgegevens. Dit betekent dat zorgverzekeraars, voor de verwerking van persoonsgegevens, beleid dienen op te stellen voor de inrichting en beheersing van hun administratieve organisatie en dit beleid dienen vast te leggen voor, in elk geval, het risk management, de interne controle, compliance en de interne audit binnen de organisatie. Daarnaast zorgen zij ervoor dat deze beleidslijnen worden toegepast.[14]

Daarnaast is voor het beleid met betrekking tot het verwerken van persoonsgegevens de Algemene verordening gegevensbescherming relevant.[15] Deze verordening verplicht organisaties (waaronder zorgverzekeraars) onder andere tot het vastleggen van beleid ten aanzien van bescherming van gegevensverwerking.[16] Verder introduceert de Algemene verordening gegevensbescherming de verplichting tot het (onder voorwaarden) aanstellen van een functionaris voor de gegevensbescherming. Ten slotte is er de, per 1 januari 2016 in werking getreden, verplichting tot het melden van datalekken. Deze verplichting heeft eveneens gevolgen voor de organisatie van een zorgverzekeraar met betrekking tot de bescherming van persoonsgegevens, omdat deze organisatie in staat moet zijn om datalekken waar te nemen, ze te registreren en waar nodig vervolgmaatregelen op te nemen.[17]

Zoals gezegd hebben bovenstaande regels betrekking op de manier waarop zorgverzekeraars organisatorische maatregelen hebben genomen om de regels na te leven met betrekking tot de verwerking van persoonsgegevens, waaronder - van belang voor dit onderzoek – de uitvoering van controles.

Voor de organisatie van de verwerking van persoonsgegevens zijn daarnaast in het bijzonder relevant, de Uniforme Maatregelen (uniforme

[12] Respectievelijk artikel 3:10 Wet op het financieel toezicht, artikel 17 Besluit prudentiële regels Wft en artikel 36 Wet marktordening gezondheidszorg.
[13] Zie bijvoorbeeld artikel 13 en artikel 14 van de Wbp.
[14] Artikel 41 Richtlijn 2009/138 EU, Solvency II.
[15] Pb EU L119.
[16] Artikel 22 concept-verordening gegevensbescherming, 2012/0011 (COD).
[17] Artikel 34a Wbp.

werkwijzen) zoals die door Zorgverzekeraars Nederland (ZN) voor alle zorgverzekeraars zijn opgesteld. Voor dit onderzoek zijn vooral van belang, de Uniforme Maatregelen 01 (over de inrichting van de Functionele Eenheid), 02 (die verplicht tot opstellen van een Privacy Statement), 03 (over informatieverstrekking aan verzekerden) en 06 (Privacy bij afhandeling van declaraties).[18]
De Functionele Eenheid wordt gevormd door een of meerdere groepen medewerkers, die bevoegd zijn tot het verwerken van persoonsgegevens en daarbij vallen onder de verantwoordelijkheid van de medisch adviseur. Deze werkzaamheden kunnen in verschillende fasen van de uitvoering van de verzekeringsovereenkomst plaatsvinden (bijvoorbeeld de zorginkoop en machtigingen). Voor dit onderzoek zijn de activiteiten in de declaratiefase het meest relevant.

De uitvoering van controles vindt plaats binnen de Functionele Eenheid. Binnen de Functionele Eenheid vinden werkzaamheden plaats ten aanzien van medische gegevens die verder gaan dan louter administratieve werkzaamheden. Het gaat dan bijvoorbeeld om de interpretatie, taxatie en het eventueel opvragen van nadere gegevens. De medewerkers van de Functionele Eenheid werken onder de functionele verantwoordelijkheid van de medisch adviseur. De medisch adviseur is coördinator van (en verantwoordelijk voor) de verstrekking van informatie over verzekerden aan de medewerkers van de Functionele Eenheid, voor wie een van de medisch adviseur afgeleide geheimhoudingsplicht geldt. Een medisch adviseur hoeft geen arts te zijn, maar een BIG registratie is wel noodzakelijk.[19]
Aangezien deze werkzaamheden als gezegd verder gaan dan de afhandeling van routinematige administratieve werkzaamheden, is van belang dat zorgverzekeraars adequate maatregelen treffen voor de organisatie van de Functionele Eenheid.

De Uniforme Maatregel over de Functionele Eenheid laat ruimte voor de verzekeraar om naar eigen inzicht het aantal Functionele Eenheden binnen de eigen organisatie te bepalen, en daarbij de formele positie van de verantwoordelijk medisch adviseur te kiezen. Vereiste is in alle gevallen dat de medisch adviseur onafhankelijk moet kunnen adviseren.

2.2.3 Regelgevend kader privacyregeling

Het regelgevend kader voor toepassing van de *privacyregeling* is vastgelegd in, zoals genoemd, de Regeling gespecialiseerde geestelijke gezondheidszorg (de regeling).[20] In artikel 3.5 van de regeling is bepaald dat wanneer de patiënten en zorgverleners gezamenlijk een privacyverklaring hebben getekend, geen naar de diagnose herleidbare informatie op de factuur wordt vermeld. In artikel 6 van de Regeling Verplichte aanlevering minimale dataset gespecialiseerde GGZ is bepaald dat in dat geval ook geen naar de diagnose herleidbare informatie in het DBC Informatie Systeem (DIS) wordt opgenomen.[21] De

[18] Zie: https://www.zn.nl/350584837/Gedragscode. De normen in deze uniforme maatregel zijn geen wettelijke regels maar vormen in de praktijk een belangrijke uitwerking van de manier waarop zorgverzekeraars in de praktijk omgaan met wettelijke voorschriften over persoonsgegevens (in het bijzonder: artikel 87 Zvw). Daarom gaat van deze voorschriften niettemin een sterke (zelf-)bindende werking uit.
[19] Uniforme Maatregel 01: Functionele Eenheid, pag. 4.
[20] Zie artikel 3.5 van de regeling.
[21] Ook indien de cliënt aan de zorgverlener te kennen heeft gegeven de rekening niet aan de zorgverzekeraar ter vergoeding aan te bieden (indien hij deze zelf betaalt), bestaat geen verplichting om de diagnose informatie op de factuur te zetten noch om deze aan te leveren aan DIS (zie artikel 3.5 lid 6 van de Regeling gespecialiseerde geestelijke gezondheidszorg (NR/CU-565) en artikel 6 van de Regeling Verplichte aanlevering minimale dataset gespecialiseerde GGZ (NR/CU-549). Het zevende lid van

privacyverklaring heeft bovendien als gevolg dat controles op de betreffende facturen plaats moeten vinden door of onder verantwoordelijkheid van een medisch adviseur (en, uiteraard, met inachtneming van de daarvoor geldende overige waarborgen, vastgesteld in hoofdstuk 7 van de Rzv).
De bepaling stelt daarnaast (artikel 3.5, lid 4) dat patiënt en zorgaanbieder gerechtigd zijn om een tarief te declareren dat niet herleidbaar is naar de diagnose (een afwijkend tarief). Deze bepaling vindt zijn oorsprong in de bestaande declaratiesystematiek in de GGZ, waarin de hoogte van een tarief afhankelijk kan zijn van de behandelde diagnose. Het doel van deze bepaling is om te voorkomen dat – in aanvulling op het feit dat bij ondertekening van de privacyverklaring de diagnose informatie op de factuur reeds ontbreekt - ook op basis van het gedeclareerde *tarief* niet valt te herleiden, welke behandeling (op basis van welke bijbehorende diagnose) is gegeven. De zorgaanbieder dient in dat geval tot een afwijkende betalingsprocedure te komen. De zorgverzekeraar is gehouden om, binnen redelijke grenzen, zijn medewerking te verlenen bij de totstandkoming van een dergelijke procedure.

De NZa heeft voor de sector medisch specialistische zorg (MSZ) eveneens een privacyregeling opgesteld. Deze regeling biedt een vrijwaring van de verplichte vermelding van zorgactiviteiten op de nota in geval van een privacyverklaring (artikel 35.1 r sub 2, van de nadere regel NR/CU-266).[22] Aangezien de NZa hierover vrijwel geen signalen heeft ontvangen, is deze regeling niet afzonderlijk onderzocht[23].

artikel 3.5 van de privacyregeling GGZ bepaalt vervolgens, dat als de cliënt zich bedenkt en de factuur op een later moment alsnog ter betaling wil indienen bij zijn zorgverzekeraar, dan alsnog een privacyverklaring dient te worden ingevuld en ondertekend.

[22] Vanaf 1 januari 2017 geldt deze mogelijkheid ook voor de per die datum geldende nieuwe verplichting om de indicatie van een add-ongeneesmiddel op de nota te vermelden.

[23] Voor de bevindingen (zoals beschreven in hoofdstuk 5) is overigens met betrekking tot de privacyregeling MSZ geen andere uitkomst te verwachten, omdat de werkwijze van zorgverzekeraars geen onderscheid maakt naar het soort zorg (GGZ of MSZ) waarvoor een privacyverklaring wordt afgegeven.

3. Signalen en meldingen

Directe aanleiding voor het onderzoek vormen, als gezegd, signalen die de NZa heeft ontvangen over de naleving van privacyvoorschriften. Deze signalen zijn afkomstig van zorgaanbieders en verzekerden en hebben betrekking op het opvragen van medische persoonsgegevens bij de uitvoering van controles door zorgverzekeraars van declaraties waarbij sprake was van een privacyverklaring. Het betreft 14 signalen in de periode mei 2013 tot heden. In juni 2014 hebben alle zorgverzekeraars aan de NZa verklaard dat zij de privacyregeling naleefden. De zorgen die verschillende melders na deze datum alsnog kenbaar hebben gemaakt en de nauwe betrokkenheid van enkele organisaties van zorgaanbieders in de GGZ waren aanleiding voor de NZa om een onderzoek in te stellen.

4. Beschrijving van het onderzoek

4.1 Onderzoeksvraag

Het onderzoek richt zich op twee onderdelen, een algemeen deel en een specifiek deel. Het algemeen deel, allereerst, is gericht op de wijze waarop zorgverzekeraars de omgang met persoonsgegevens binnen hun organisatie hebben geborgd bij de uitvoering van controles. De omgang met persoonsgegevens vormt een regulier onderdeel van de inrichting en aansturing van de organisatie van een zorgverzekeraar als geheel. De organisatie van een zorgverzekeraar kan dan ook gevolgen hebben voor de mate waarin wordt voldaan aan de specifieke regels voor het verwerken van persoonsgegevens. Indicatoren die daarbij een rol spelen zijn: het onafhankelijk functioneren van de medisch adviseur en van de ondersteunende medewerkers die een (afgeleid) beroepsgeheim hebben; de manier waarop besluitvorming is vastgelegd; het beschrijven en volgen van vastomlijnde werkwijzen en procedures; de algemene governance waaronder het voldoen aan de privacyregelgeving en de wijze waarop met signalen en fouten wordt omgegaan.
De NZa heeft eerder, in april 2008 en in juli 2009, een onderzoek ingesteld naar de naleving van privacyvoorschriften.[24] Daarnaast heeft de NZa in 2013 de werking van de privacyregeling geëvalueerd.[25] De bevindingen van deze onderzoeken zijn, voor zover mogelijk, in dit onderzoek meegenomen.

Een specifiek onderdeel van het onderzoek is gericht op de vraag, op welke wijze zorgverzekeraars omgaan met de uitvoering van de privacyregeling: hoe vaak wordt een beroep op deze regeling gedaan en hoe worden de betreffende declaraties afgehandeld?

[24] Zie: https://www.nza.nl/1048076/1048181/Rapport_vervolgonderzoek_privacy_bij_zorgverzekeraars.pdf
[25] Zie: https://www.nza.nl/104107/138040/Rapport_Evaluatie_privacyregeling_GGZ.pdf

4.2 Onderzoeksaanpak

Om de noodzakelijke informatie te verzamelen heeft de NZa een vragenlijst opgesteld over de wijze waarop verzekeraars omgaan met de verwerking van persoonsgegevens in het algemeen en, meer in het bijzonder, de privacyregeling. De inhoud van de vragenlijst is afgestemd met Zorgverzekeraars Nederland (ZN) en de Autoriteit Persoonsgegevens. Bijlage 1 bevat een overzicht van de vragen.
De vragen hebben betrekking op de relevante kaders, processen, klantinformatie, governance en compliance en vallen uiteen in de volgende thema's:

Specifiek deel:
De privacyregeling

Algemeen deel:
Het privacybeleid
Organisatie van controles
Communicatie over controles.

De NZa heeft op 25 november 2015 een informatieverzoek op grond van de Wmg verstuurd aan alle (11) verzekeraars (zie bijlage). De verzekeraars hebben daarop gedocumenteerd antwoord gegeven. Na ontvangst van de antwoorden en de bijgevoegde documentatie, heeft de NZa deze informatie geanalyseerd en, waar nodig, aanvullende vragen gesteld. Vervolgens zijn enkele verzekeraars geïnterviewd. Op basis daarvan zijn conceptbevindingen per verzekeraar vastgesteld en voorgelegd met het verzoek om een zienswijze. Daarnaast heeft een bijeenkomst plaats gevonden met de verzekeraars, waarbij de (voorlopige) bevindingen en aanbevelingen ter consultatie zijn besproken. De uitkomsten van deze bijeenkomst zijn in de eindversie van dit rapport verwerkt.

5. Bevindingen, conclusies en aanbevelingen

De bevindingen, conclusies en aanbevelingen van het onderzoek worden besproken in de hiervoor aangeduide thema's:

5.1 Thema 1: Privacyregeling

Werkwijze privacyverklaring
In november 2015 heeft het CBP (thans: Autoriteit Persoonsgegevens) een vragenlijst verstuurd aan enkele zorgverzekeraars met de vraag of - en zo ja, waarom - zij aan verzekerden met een privacyverklaring standaard om de (volledige) verwijsbrief en behandelplan vroegen. Eén verzekeraar bleek daarbij in strijd met de Wbp te handelen. Deze verzekeraar heeft naar aanleiding van het onderzoek van de AP zijn werkwijze aangepast om te borgen dat dergelijke incidenten niet meer voorkomen. De overige zorgverzekeraars hebben verklaard dat zij reeds conform de regelgeving handelden.

Uit het onderzoek van de NZa is gebleken dat alle zorgverzekeraars beschikken over een afzonderlijke werkwijze voor uitvoering van de privacyregeling. In vier gevallen was deze werkwijze niet aantoonbaar of niet duidelijk schriftelijk vastgelegd. Op aangeven van de NZa is inmiddels de werkwijze schriftelijk en aantoonbaar vastgelegd.

In alle gevallen bleek de werkwijze, zoals vastgelegd, in lijn met de privacyregeling. Eén zorgverzekeraar vroeg incidenteel volledige verwijzingen en behandelplannen op. In juni 2014 heeft de zorgverzekeraar (evenals de overige verzekeraars) verklaard de privacyregeling na te leven. De NZa heeft daarom deze verzekeraar opgedragen aan te tonen, dat zijn werkwijze conform de regels was. Deze zorgverzekeraar heeft daaraan inmiddels opvolging gegeven, waarbij de werkwijze op zichzelf wel, maar de toepassing van de werkwijze niet conform de regels bleek. In reactie daarop heeft de NZa de zorgverzekeraar een periodieke rapportageplicht opgelegd, die inhoudt dat de zorgverzekeraar zich dient te verantwoorden aan de NZa over de wijze waarop hij eventuele klachten over de privacyregeling afhandelt. De verzekeraar dient zich (blijvend) te onthouden van het opvragen van diagnose informatie bij het betalen van de factuur als sprake is van een privacyverklaring.[26]

Machtigingseis (toestemmingsvereiste) en privacyverklaring
De waarborg die de privacyverklaring biedt voor het verwerken van persoonsgegevens kan spanning opleveren met toepassing van een machtigingsvereiste. Het machtigingsvereiste (of toestemmingsvereiste) houdt in dat zorgverzekeraars, voorafgaande aan een behandeling, om toestemming moet worden gevraagd voor vergoeding van de behandeling. Zorgverzekeraars kunnen het toestemmingsvereiste bijvoorbeeld hanteren om zeker te stellen dat de te leveren zorg onder het verzekerde pakket valt. Op deze wijze wordt voorkomen dat zorg, die na levering niet voor vergoeding in aanmerking blijkt te komen, ten onrechte wordt vergoed en moet worden teruggevorderd.

[26] Met dien verstande dat de regelgeving ruimte laat om ter controle van de factuur diagnosegegevens op te vragen door of onder verantwoordelijkheid van een medisch adviseur van de zorgverzekeraar, waarbij uiteraard aan de daarvoor geldende regels (zie hoofdstuk 7 Regeling zorgverzekering) moet worden voldaan.

Alle zorgverzekeraars hebben aangegeven dat bij gebruikmaking van een privacyverklaring, de machtigingseis niet aan de orde was. De reden daarvoor is dat zij de machtigingsvereiste ofwel niet hanteerden, of – wanneer zij deze wel hanteerden - het machtigingsvereiste niet is toegepast indien sprake was van een privacyverklaring. Dit betekent dat de zorgverzekeraar de factuur vergoedde *ongeacht of sprake was van een machtigingsvereiste*. De zorgaanbieder kon dan ook de behandeling starten en de factuur aan de verzekeraar toesturen.

Aantallen privacyregeling
Uit het onderzoek is gebleken dat in 2014 ruim 900 cliënten gebruik maakten van een privacyverklaring in de GGZ. De getallen variëren per verzekeraar (maximaal 518, minimaal 3). De aantallen lopen grotendeels gelijk met de omvang van de verzekerden per verzekeraar en laten geen opvallende verschillen zien per verzekeraar.

Hanteren van afwijkend tarief
Een van de onderzoeksvragen was gericht op het hanteren van een afwijkend tarief, zoals beschreven in hoofdstuk 1. Als gezegd, biedt de Regeling GGZ (artikel 3.5 lid 4) een recht aan patiënt en zorgaanbieder om een tarief te declareren dat niet herleidbaar is naar de diagnose (een afwijkend tarief), om te voorkomen dat op basis van het gedeclareerde tarief op de factuur is vast te stellen, welke behandeling (met bijbehorende diagnose) is gegeven.

Alle zorgverzekeraars bieden de mogelijkheid tot hanteren van een afwijkend tarief. In vrijwel alle gevallen wordt aan het vereiste dat de zorgverzekeraar en zorgaanbieder in overleg tot een afwijkende betalingsprocedure voor een dergelijk tarief dienen te komen, helemaal niet toegekomen, omdat de zorgverzekeraar het tarief (ongeacht de *precieze* hoogte ervan) in alle gevallen uitbetaalt. Het is dan niet nodig om in overleg te treden met de zorgverzekeraar om tot een dergelijke betalingsprocedure voor een afwijkend tarief te komen bij toepassing van de privacyregeling. In deze gevallen kan overigens het tarief evengoed niet worden herleid naar de diagnose. Voor de (digitale) verwerking van de facturen, maken alle verzekeraars namelijk gebruik van een aparte code voor declaraties met een privacyverklaring (een ‘dummycode’) ter vervanging van een behandelcode (DBC). Het ontbreken van een behandelcode op de factuur biedt de zorgaanbieder de mogelijkheid een tarief in rekening te brengen dat afwijkt van een tarief dat is vastgesteld (of overeengekomen) voor een bepaalde behandeling.

De zorgverzekeraars hebben aangetoond dat zij de mogelijkheid bieden tot hanteren van een afwijkend tarief doordat er wordt gewerkt met dummycodes. Dit is een aparte code die is ingesteld voor het declareren van zorg met een privacyverklaring. Deze code maakt het, zoals gezegd, mogelijk dat deze zorg, ondanks het ontbreken van een DBC kan worden ingediend bij de verzekeraar en kan worden vergoed.

Als de factuur digitaal kan worden ingediend door de zorgaanbieder (via de voorziening van Vecozo, die verzekeraars hiervoor gezamenlijk aanbieden) dan geldt dat evenzeer voor een factuur met een privacyverklaring. Als een zorgverzekeraar en zorgaanbieder geen afspraken hebben gemaakt over de digitale indiening van een factuur wordt deze op papier ingediend. De privacyverklaring en de dummycode kunnen daarbij ook worden gebruikt. Deze facturen worden dan eveneens uitbetaald zonder dat zichtbaar is welke diagnose is behandeld.

Eén zorgverzekeraar past de regeling toe, door de mogelijkheid tot het hanteren van een afwijkend tarief expliciet aan te bieden, waarbij in overleg met zorgaanbieders tot een gezamenlijke oplossing voor een betalingsprocedure en een tarief wordt gekomen.

Alle verzekeraars verklaren dat zij, in geval van een geldige privacyverklaring, de nota uitbetalen zonder dat zij de hoogte van het bedrag kunnen koppelen aan een diagnose. Dat kan ook niet anders omdat - gezien de dummycode - niet kan worden vastgesteld welke behandeling is geleverd noch welk bijbehorend tarief zou kunnen gelden. Om mogelijke herkenbaarheid van het gefactureerde bedrag bij een dummycode te voorkomen, staat het de zorgaanbieder in alle gevallen vrij om een tarief te hanteren dat afwijkt van het tarief dat de betreffende behandeling is voorgeschreven.

Zorgaanbieders kunnen dan ook in alle gevallen een afwijkend tarief hanteren, zonder daarom bij de verzekeraar te vragen. De gevallen waarin door zorgaanbieders expliciet wordt verzocht om hanteren van een afwijkend tarief, zijn dan ook zeer gering. Twee verzekeraars verklaren dat zij daartoe expliciete verzoeken hebben ontvangen (12 respectievelijk 3 verzoeken). Deze verzoeken zijn gehonoreerd, door toe te lichten dat geen controle plaats kan vinden op de hoogte van het tarief nu immers sprake is van een dummycode.

Thema 1 Privacyregeling: Conclusies en aanbevelingen aan zorgverzekeraars

De bevindingen laten een stijging zien van het gebruik van het aantal privacyverklaringen. Alle verzekeraars hebben privacyverklaringen ontvangen, in totaal ruim 900 in 2015, waar aanvankelijk (juli 2013) nog sprake was van de situatie waarin enkele zorgverzekeraars geen enkele privacyverklaring ontvingen.[27]

De bevindingen maken duidelijk dat alle zorgverzekeraars met betrekking tot de privacyregeling:

- beschikken over een adequate werkwijze voor de privacyregeling;
- het hanteren van afwijkende tarieven mogelijk maken;

[27] Zie Rapport Evaluatie Privacyregeling GGZ, https://www.nza.nl/104107/138040/Rapport_Evaluatie_privacyregeling_GGZ.pdf. In 2013 is het aantal verzekerden dat gebruik maakte van de privacyregeling niet geteld, maar zijn de ervaringen van zorgaanbieders onderzocht.

- de mogelijkheid tot hanteren van een afwijkend tarief, zoals voorzien in de regeling, in de praktijk aanbieden en uitvoeren; en
- geen machtigingsvereiste hanteren of toepassen bij gebruikmaking van de privacyregeling.

Daarbij passen de verzekeraars verschillende werkwijzen toe bij het hanteren van afwijkende tarieven. Vrijwel alle verzekeraars betalen het tarief (ongeacht de *precieze* hoogte ervan[28]) in alle gevallen uit indien sprake is van een geldige privacyverklaring. Eén verzekeraar past de regeling expliciet toe door de mogelijkheid tot het hanteren van een afwijkend tarief expliciet aan te bieden, waarbij in overleg met zorgaanbieders tot een gezamenlijke oplossing voor een betalingsprocedure en een tarief wordt gekomen. Beide varianten voldoen aan de privacyregeling, maar het is van belang dat zorgverzekeraars duidelijkheid blijven bieden over de werkwijze die zij toepassen.
Bij één zorgverzekeraar bleek de *toepassing van de* werkwijze niet in lijn met de (bedoeling van) privacyregeling, wegens het – incidenteel – opvragen van volledige verwijzingen en behandelplannen. Reeds eerder heeft de verzekeraar (in juni 2014) verklaard de privacyregeling na te leven. De NZa heeft daarom deze verzekeraar een rapportageplicht opgelegd (gedurende een jaar, eindigend op 31 maart 2017) om te controleren of de betreffende verzekeraar de werkwijze in de praktijk conform de regels blijft toepassen.

5.2 Thema 2: Privacybeleid en evaluatie privacybeleid

Bevindingen
Alle verzekeraars besteden aantoonbaar beleidsmatig aandacht aan het onderwerp privacy. Van alle (11) onderzochte verzekeraars hebben er twee hun privacybeleid in een afzonderlijk document vastgelegd. Twee verzekeraars bespreken privacybeleid als onderdeel van een ander (verwant) onderwerp. De overige verzekeraars verdelen hun beleid ten aanzien van privacy over diverse andere beleidsonderwerpen en de daarbij behorende stukken. Verzekeraars hebben beleid ten aanzien van privacy wel in beeld, maar niet altijd even prominent of toegankelijk. Het vastleggen van op zichzelf staand privacybeleid is op dit moment ook niet voorgeschreven. De Algemene verordening gegevensbescherming van de EU stelt vanaf 2018 regels over die vastlegging en toegankelijkheid.[29] Bij verzekeraars waar dit echter wel nu al gebeurt, bleek het eenvoudiger om aantoonbaar te maken hoe met de *naleving* van de betreffende regels wordt omgegaan. Dat geldt ook voor de twee verzekeraars die hun privacybeleid bij een ander (verwant) onderwerp opnemen.
Voor de inrichting van taken, verantwoordelijkheden en bevoegdheden (de governance) rond privacy wijst het merendeel van de verzekeraars op het "three lines of defence" - model voor de naleving van regels. Hierin wordt de verantwoordelijkheid voor de naleving van wet- en regelgeving in de eerste lijn belegd. Monitoring of toezicht op die naleving ligt in de tweede lijn, normaal gesproken bij de

[28] Het afwijkende tarief kan niet hoger zijn dan het geldende maximumtarief.
[29] De Algemene verordening gegevensbescherming (PB EU L119) bepaalt in artikel 11, lid 1 dat "het beleid van de voor de verwerking verantwoordelijke met betrekking tot de verwerking van persoonsgegevens en de uitoefening van de rechten van de betrokkene […] transparant en eenvoudig toegankelijk [dient] te zijn".

compliancefunctie. De derde lijn bestaat doorgaans uit de afdeling Internal Audit en controleert functioneren van (en samenwerking tussen) de eerste en tweede lijn.
Vier verzekeraars melden dat zij een aangewezen functionaris hebben die zich bezig houdt met de naleving van privacyregelgeving: een Functionaris voor de Gegevensbescherming of een Privacy Officer. In één geval bevindt die zich in de eerste lijn, in drie gevallen bij de compliancefunctie.
Niet alle verzekeraars kunnen laten zien op welke wijze en met welke effecten zij de kwaliteit van de privacy-organisatie bewaken. Uiteraard beschikken zij allen over een tweede en derde lijn, maar deze schenken niet altijd aantoonbaar expliciete aandacht aan de verwerking van (medische) persoonsgegevens.

De *evaluatie* van het beleid wordt voornamelijk bepaald door het al dan niet samenhangend beschreven zijn daarvan. Het onderzoek laat zien dat waar privacybeleid als op zichzelf staand onderwerp is beschreven, het eenvoudiger is duidelijkheid te geven over de wijze van naleving van de betreffende regels. Dat kan in combinatie met andere onderwerpen gebeuren. De verzekeraars die kiezen voor een gecombineerde benadering, behandelen privacy binnen de door hen gekozen combinatie wel als zelfstandig onderwerp.

Een enkele verzekeraar, die niet beschikte over een afzonderlijk privacybeleid, toonde onvoldoende concrete uitwerking van de relevante wet- en regelgeving. De verzekeraar heeft vervolgens, na daartoe te zijn opgedragen door de NZa, passend privacybeleid geformuleerd.
In de uitwerking, met name wat betreft de aantoonbaarheid van de evaluaties, zijn wel duidelijke verschillen zichtbaar. Eén verzekeraar evalueert niet in een vaste regelmaat, maar doet dit alleen wanneer hij dat noodzakelijk achtte. Deze verzekeraar heeft op aangeven van de NZa de evaluatie van privacybeleid opgenomen in zijn reguliere monitoring- en auditactiviteiten.

Het niet vastleggen van de vormgeving van evaluaties betekent dat ook de opvolging van de uitkomsten daarvan niet altijd is geborgd. Zo beschikt één verzekeraar over een evaluatiedocument van zijn compliancefunctie, afkomstig uit 2013, zonder ook te kunnen aantonen hoe de daarin geformuleerde aanbevelingen waren opgevolgd.
Bij zeven verzekeraars is evaluatie een regulier onderdeel van de werkzaamheden van de compliance- of auditfunctie. Twee van deze groep voeren daarnaast afzonderlijke evaluaties uit, specifiek gericht op privacy. Eén verzekeraar doet dat gecombineerd met onderzoek naar zijn beheersmaatregelen voor informatiebeveiliging, één voert een volledig op zichzelf staande privacy-evaluatie uit.

Het Verbond van Verzekeraars geeft een model voor zelfevaluatie van de naleving van de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.[30] Geen van de verzekeraars gebruikt dit model integraal voor een zelfevaluatie. Uit de verstrekte informatie blijkt dat dit model bekend is bij verzekeraars en dat zij dit betrekken in de evaluaties die zij zelf opzetten. Zij geven aan hieruit risicogebaseerd elementen op te nemen. Dit model behandelt een breed spectrum van relevante onderwerpen en biedt, als model van eigen branche, de gebruiker de kans zichzelf te toetsen aan een breed gedragen norm. Een (meer)

30

https://www.verzekeraars.nl/overhetverbond/zelfregulering/Documents/Gedragscodes/Zelfevaluatie%20GVPFI.pdf

integraal gebruik van het model voor zelfevaluatie kan daarom de kwaliteit van de zelfevaluaties verder versterken.

Thema 2 Privacybeleid en evaluatie privacybeleid: Conclusies en aanbevelingen aan zorgverzekeraars
Er bestaat geen verplichting het privacybeleid in één (op zichzelf staand) document vast te leggen. Verdeling over verschillende documenten of vindplaatsen achten wij echter niet wenselijk. Centrale vastlegging van privacybeleid verdient aanbeveling omdat het niet alleen bijdraagt aan de inzichtelijkheid hiervan voor interne en externe belanghebbenden, maar ook omdat het efficiënte evaluatie en opvolging daarvan bevordert. Concentratie van privacybeleid brengt een organisatie tot één gedeelde benadering en daarmee tot betere interne beheersing. Dat is niet alleen een algemeen aanvaard beginsel van beheerste bedrijfsvoering, maar ten aanzien van de bescherming van persoonsgegevens stelt de Algemene verordening gegevensbescherming van de EU dat de verantwoordelijke voor betere regelnaleving intern beleid vast dient te stellen en passende maatregelen dient te treffen, die in het bijzonder voldoen aan de beginselen inzake privacy by design en by default.[31]

Het verdient daarom aanbeveling privacybeleid, vooruitlopend op nieuwe regelgeving, (in een enkel geval: verder te ontwikkelen en) herkenbaar vast te leggen. Reguliere periodieke evaluatie en monitoring is daar een onderdeel van. Dat impliceert onzes inziens dat het beleid op één plaats vindbaar is. Ook hier is het zinvol aandacht te besteden aan de werking van interne monitoring en toezicht (bijvoorbeeld door compliance). Deze aanbeveling wordt door een groot deel van de verzekeraars in de praktijk reeds toegepast. Een klein deel van de verzekeraars kan op dit onderdeel echter nog vooruitgang boeken.
De verzekeraar die geen privacybeleid in een zelfstandig document had vastgelegd, heeft dat inmiddels op aangeven van de NZa opgesteld. De overige verzekeraars geven aan deze aanbevelingen ten aanzien van vastlegging, evaluatie en communicatie over te zullen nemen.

5.3 Thema 3: Organisatie van controles

Bevindingen
Verzekeraars zijn verplicht om bepaalde controles te doen ten aanzien van gedeclareerde kosten voor zorg. Zij behoren daarvoor plannen te hanteren, om medische persoonsgegevens in deze controles te mogen betrekken. In deze plannen dienen zij voorgenomen controles te beschrijven. Zorgverzekeraars moeten deze plannen zodanig bekend maken dat zij voor verzekerden en zorgaanbieders gemakkelijk verkrijgbaar zijn (artikel 7.7 Regeling zorgverzekering), zonder dat de wijze van bekendmaking is voorgeschreven. Verzekeraars kunnen – uiteraard binnen de grenzen van de daarvoor geldende regelgeving - ook de organisatie en inrichting van deze controles zelf bepalen, zodat daarin verschillende keuzes zijn gemaakt die voor verzekerden en zorgaanbieders niet altijd inzichtelijk zijn.
Deze onbekendheid lijkt een deel van de meldingen en vragen aan de NZa over de controles door verzekeraars te verklaren. Daarom zijn verzekeraars gevraagd te schetsen hoe zij het uitvoeren van deze controles in hun organisatie hebben ingebed.

Zes verzekeraars hebben tevoren uitgewerkt hoe de middelen van materiële controle worden bepaald. Eén van deze zes sluit daarvoor aan

[31] Algemene verordening gegevensbescherming (PB EU L119), overweging 61. Privacy by design en by default zijn beschreven in artikel 23 van deze verordening.

bij de uitwerking die voor een zustervennootschap binnen hetzelfde concern is gemaakt. Deze uitwerkingen bestaan in beslisbomen of uitgeschreven criteria voor het al dan niet hanteren van de gegeven controle-instrumenten.
Bij de andere verzekeraars is weliswaar beschreven welke functionaris de inhoud en diepgang van een controle bepaalt, maar zijn er geen criteria op voorhand zichtbaar. Dit verschil in benadering lijkt niet te worden bepaald door de omvang van de verzekeraar, of de groep waartoe hij behoort. Bepalend lijkt vooral de eigen voorkeur van de betreffende organisatie om meer of minder vrijheid te laten aan de uitvoerders van de controles.

Een belangrijk onderdeel van de bevindingen met betrekking tot de organisatie van controles spitst zich toe op de Functionele Eenheid, die een belangrijke organisatorische waarborg vormt voor de omgang met medische persoonsgegevens. De Functionele Eenheid is ingesteld ter ondersteuning bij de uitvoering van controles onder verantwoordelijkheid van een medisch adviseur, die valt onder het medisch beroepsgeheim.
Alle verzekeraars hebben één of meer Functionele Eenheden ingericht.
Acht verzekeraars leggen de taken en verantwoordelijkheden van de Functionele Eenheid vast in specifiek daarvoor bedoelde documenten.
Twee verzekeraars sluiten ook hier bij zustervennootschappen aan. Bij één verzekeraar is de organisatorische inbedding van de Functionele Eenheid niet eenduidig herkenbaar in de documentatie die voor het onderzoek is overgelegd.
Het medisch beroepsgeheim van de medisch adviseur geldt ook voor de leden van de Functionele Eenheid, zoals dat ook voor ondersteuners van behandelende (para)medici geldt. Op één verzekeraar na laten alle verzekeraars leden van de Functionele Eenheid een afzonderlijke geheimhoudingsverklaring afgeven. De verzekeraar die zonder afzonderlijke verklaringen werkt, wijst op de verplichte eed voor medewerkers van financiële ondernemingen. Deze eed bevat een ongeclausuleerde geheimhoudingsbepaling die dan ook voor een Functionele Eenheid zou werken. Deze verzekeraar wijst leden van de Functionele Eenheid wel in een separate brief op hun positie en de bijzondere gevolgen daarvan. Dit komt echter niet overeen met de door ZN vastgestelde Uniforme Maatregel over de Functionele Eenheid, die stelt dat "zorgverzekeraars, zowel in functiebeschrijvingen van medewerkers die persoonsgegevens betreffende iemands gezondheid verwerken, als in door hen te ondertekenen verklaringen, de geheimhoudingsplicht opnemen".[32] Deze verzekeraar zal naar aanleiding van dit onderzoek de deelnemers in de Functionele Eenheid een afzonderlijke geheimhoudingsverklaring laten ondertekenen.
Een deel van de verzekeraars heeft een afzonderlijke geheimhoudingsplicht opgenomen in de arbeidsovereenkomst. Enkele verzekeraars informeren medewerkers van de Functionele Eenheid over de geheimhouding door middel van cursussen en instructies.

De positie van de medisch adviseurs binnen de organisatie verschilt. Bij drie verzekeraars hebben zij zichtbaar een eigen plaats. Bij de overige verzekeraars maken zij, gelijkelijk verdeeld, onderdeel uit van de afdeling zorginkoop of de afdeling controles. In één geval worden de medisch adviseurs extern ingehuurd.
Behalve zijn positie, varieert ook de rol van de medisch adviseur in het controleproces: adviserend, verantwoordelijk of uitvoerend. Vijf verzekeraars werken de taken en verantwoordelijkheden van de medisch adviseur uit, maar deze verschillen onderling zodanig van elkaar dat zich geen gedeeld beeld aftekent. De zichtbare verschillen gaan vooral over

[32] UM01 Functionele Eenheid, pag. 2 en 11.

de wijze van betrokkenheid van de medisch adviseur bij de controleplannen, instructie van de deelnemers in de Functionele Eenheid en bepaling van de in te zetten controlemiddelen. In veel gevallen is de medisch adviseur betrokken bij het vaststellen van het algemeen controleplan, maar wat die betrokkenheid inhoudt is dan niet vastgelegd. In de uitvoering van controlewerkzaamheden is de medisch adviseur niet altijd zichtbaar. Bij informatieverzoeken wordt bijvoorbeeld wel opgenomen dat deze onder verantwoordelijkheid van de medisch adviseur worden gedaan, maar zij worden niet altijd door hem of haar ondertekend.
Hoe de medisch adviseur dan de verantwoordelijkheid voor de verwerking van bijzondere persoonsgegevens in het kader van de controles waar kan maken, is niet aantoonbaar. Het is voorstelbaar dat deze onderlinge verschillen doorwerken in de wijze waarop de controle-inspanningen van de verschillende verzekeraar zich presenteren aan zorgaanbieders. Daardoor kunnen de controles die verzekeraars doen door zorgaanbieders worden beleefd als onvoorspelbaar en bewerkelijk.

Uit de signalen die mede aanleiding waren voor dit onderzoek (welke betrekking hadden op de privacyregeling) volgde dat het vooral voor zorgaanbieders lastig voorspelbaar is welke controles zij van verzekeraars kunnen verwachten. Het tevoren uitwerken van de keuze van controlemiddelen biedt een zekere mate van voorspelbaarheid en objectiveerbaarheid van deze beslissingen. Althans, in het onderzoek kwamen bij de twee verzekeraars die hierin zichzelf de meeste ruimte laten ook de meeste meldingen of klachten van zorgaanbieders en verzekerden voor. Zonder hier over die meldingen te oordelen, ondersteunt dit het beeld dat duidelijkheid in gedrag ook comfort geeft. Eén verzekeraar legt, naast een plan voor formele en materiële controles, zijn beleid ten aanzien van organisatiebreed onderzoek met persoonsgegevens vast.

Thema 3 Organisatie van controles: Conclusies en aanbevelingen aan zorgverzekeraars
Aangezien niet altijd duidelijk is in welke mate de medisch adviseur bij de controle betrokken is, is het voorstelbaar dat dit voor zorgaanbieders een beeld oproept van een medisch adviseur op (grote) afstand: weliswaar toeziend op het proces, maar zonder directe en zichtbare betrokkenheid bij de betreffende dossiers. De verschillen in inrichting en werkwijze zijn niet in strijd met bestaande brancheregelgeving, maar maken deze praktijk tegelijk toch kwetsbaar, juist omdat die regelgeving veel ruimte voor eigen invulling laat en de handhaving daarvan zacht is. Een meer uitgesproken en beter zichtbare uitvoering daarvan – met een duidelijke inbedding van de positie van de medische adviseur - kan meer vertrouwen bij zorgaanbieders geven. De meerderheid van de zorgverzekeraars biedt voldoende duidelijkheid over de rol van de medisch adviseur binnen de organisatie van de uitvoering van controles. De aanbevelingen die zijn gericht aan een kleine minderheid van de verzekeraars zien op specifieke deelonderwerpen die de positie van de medisch adviseur binnen de organisatie verder moeten verduidelijken. Bovendien geldt dat de medisch adviseur, voor de verwerking van persoonsgegevens bij de uitvoering van de zogenoemde detailcontroles, verantwoordelijk dient te zijn.[33] Dat houdt in dat de medisch adviseur bepaalt welke persoonsgegevens worden opgevraagd bij het uitvoeren van controles.
Duidelijke vastlegging van de positie, taken en bevoegdheden van de medisch adviseur zorgt ervoor dat de medisch adviseur de hierbij behorende verantwoordelijkheden beter kan waarmaken.

[33] Zie artikel 7.8, tweede lid en artikel 7.2b, zesde lid van de Regeling Zorgverzekering.

Eenvoudige aanpassingen, zoals het laten tekenen van correspondentie door de medisch adviseur zelf, kunnen zorgaanbieders duidelijkheid en daarmee vertrouwen geven over behandeling van medische gegevens door verzekeraars. Meer informatie over deze werkwijzen op internet, of op de portal die sommige verzekeraars gebruiken voor zorgaanbieders, kan daar ook aan bijdragen.
Het onderzoek heeft geen aanwijzingen opgeleverd dat medische persoonsgegevens vanuit de controleketen naar buiten zouden zijn gekomen. Tegelijk is voorstelbaar dat zorgverleners terughoudend zijn in hun medewerking aan controles omdat de verzekeraars niet altijd overtuigend kunnen laten zien hoe zij het controleproces hebben ingericht én dat zij dit voldoende beheersen. Verzekeraars kunnen dus vertrouwen (her)winnen door de aantoonbaarheid van hun interne beheersing te verbeteren.

Daarnaast zien wij dat sommige verzekeraars bij gebruik van een privacyverklaring bewust afzien van controles. Het gebruik van een privacyverklaring sluit echter de bevoegdheid tot en noodzaak van controles (uiteraard onder de daarvoor geldende waarborgen[34]) niet uit. Verzekeraars en zorgaanbieders mogen niet uit het oog verliezen dat de rechtmatigheid van gedeclareerde zorgkosten niet ter discussie mag komen te staan. Deze kosten worden uit ingelegde premies en publieke middelen gefinancierd, waarvan de uitgaven verantwoord moeten kunnen worden. Verantwoording over deze noodzaak wordt ondersteund wanneer verzekeraars tevoren bepalen en vastleggen hoe (aan de hand van welke criteria) zij hun controles uitvoeren, waaruit ook blijkt welke de rol van de medisch adviseur daarin is. Dit bevordert bovendien de kwaliteit van en het draagvlak voor de controles, door het hanteren van objectieve en op zijn minst herhaalbare criteria.
Dit betekent niet dat verzekeraars hun volledige controlestrategie en -aanpak op voorhand naar buiten moeten brengen. Dat zou immers tot optimalisatie van gedrag (ook wel: *acting to the test*) kunnen leiden. Het bevordert in onze visie wel de interne beheersing en de uitlegbaarheid in de gevallen waarin een verzekeraar zich in voorkomende gevallen over zijn gedrag dient te verantwoorden. Het (kunnen) afleggen van verantwoording is bovendien, ook los van dit onderzoek, een van kenmerken van een gezonde bedrijfscultuur.[35]

Ook deze aanbevelingen worden door de verzekeraars ter hand genomen, in het bijzonder wat betreft de zichtbaarheid van de medisch adviseur in de controleketen.

5.4 Thema 4: Communicatie van zorgverzekeraars over controles

Opvragen gegevens
De informatie die verzekeraars opvragen kan worden onderscheiden in informatie verkregen ter uitvoering van de formele controle enerzijds en materiële controle anderzijds. In vier gevallen hanteert de verzekeraar niet een strikt onderscheid tussen formele en materiële controles of hanteren verzekeraars een aanvullende vorm van controles waarvan niet

[34] Voor de volledigheid: het enkele feit dat sprake is van privacyverklaringen vormt *op zichzelf* géén rechtvaardiging voor de uitvoering van materiele controles. Zie: standpunt Autoriteit Persoonsgegevens (AP) van 8 februari 2016, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-opvragen-verwijsbrief-verzekerde-met-privacyverklaring-mag-niet.
[35] De 7 Elementen van een integere cultuur, http://www.dnb.nl/binaries/De%207%20Elementen%20van%20een%20Integere%20Cultuur_tcm46-233197.pdf.

duidelijk wordt aangegeven welke vorm (materieel of formeel) het betreft. De kwalificatie van een controle, als een materiële of formele controle, is bepalend voor de vraag in hoeverre de verzekeraar (persoons-)gegevens mag opvragen. Terwijl de formele controle met name ziet op formeel-technische aspecten van de factuur - zoals de vraag of de patiënt is verzekerd bij de betreffende zorgverzekeraar – heeft de materiële controle betrekking op de vraag of de verzekerde redelijkerwijs was aangewezen op de gedeclareerde zorg en/of de zorg is geleverd[36]. Voor uitvoering van de materiële (inhoudelijke) controle is de verwerking van persoonsgegevens betreffende de gezondheid veelal in grotere mate noodzakelijk dan voor de uitvoering van een formele (technisch-administratieve) controle. Voor de materiële controle bestaan dan ook andere, meer uitgebreide regels met betrekking de verwerking van deze persoonsgegevens.

Gezien de verschillen tussen formele en materiële controles, is daarom belangrijk dat verzekeraars duidelijkheid bieden over de benaming of kwalificatie van de controles die zij uitvoeren. De NZa heeft de verzekeraars erop aangesproken, om uitsluitend de formele en materiële controles (en ook fraudeonderzoek) als kader te hanteren bij de uitvoering van controles.

Hanteren van standaarden
Verzekeraars maken wisselend gebruik van een gestandaardiseerde aanpak bij het opvragen van informatie. Met name de kleinere verzekeraars doen dit minder.
Het werken met standaardteksten is niet verplicht, maar kan wel nuttig zijn voor goede informatievoorziening en uniformiteit. Dit voordeel doet zich met name gelden bij het opvragen van informatie in een detailonderzoek, door de betreffende zorgaanbieder te informeren over de vervolgstappen van het onderzoek, de methode die de verzekeraar hanteert en de rol van de medisch adviseur bij de verwerking van de medische persoonsgegevens.

Het opvragen van medische persoonsgegevens geschiedt in alle gevallen onder de verantwoordelijkheid van de medisch adviseur. Niettemin maken twee verzekeraars de keuze om het opvragen van informatie in het kader van een detailcontrole niet rechtstreeks uit te laten voeren door de medisch adviseur, met als gevolg dat de correspondentie niet in alle gevallen door de medisch adviseur zelf (maar door een gemandateerde binnen de Functionele Eenheid) wordt ondertekend.

Informatievoorziening over controles aan verzekerden
Het overgrote deel van de verzekeraars stelt dat verzekerden door middel van de polisvoorwaarden worden geïnformeerd over de verwerking van persoonsgegevens. Daarin is (in veel gevallen) opgenomen dat de verzekerde in beginsel verplicht is om mee te werken aan eventuele controles. In een enkel geval wordt de verzekerde niet middels de polisvoorwaarden voorgelicht. De NZa heeft deze verzekeraars aanbevolen deze informatie in zijn polisvoorwaarden op te nemen. In enkele gevallen wordt verwezen naar de privacyverklaring van de verzekeraar en het algemeen controleplan, dat is gepubliceerd op de website van de verzekeraar. Enkele verzekeraars verwijzen in hun beantwoording van de door de NZa gestelde vragen expliciet naar de wettelijke regelingen op basis waarvan de verzekeraar *niet* verplicht is om de verzekerde te informeren over de uitvoering van een controle.[37]

[36] Zie NZa Nadere Regel Controle en Administratie Zorgverzekeraars (TH/NR-006), met verwijzing naar artikel 1 Regeling Zorgverzekering.
[37] Tenzij sprake is van een *verzoek*, zie artikel 34 vijfde lid Wbp.

Deze informatie is weliswaar voldoende gezien het wettelijke kader, maar dit laat onverlet dat zorgverzekeraars meer voorlichting zouden kunnen bieden over de vraag, waarom en op welke wijze zij controles uitvoeren. Ook hier geldt, dat die uitleg terughoudendheid en onzekerheid kan wegnemen.[38]

Aanwezigheid medisch adviseur bij controles
Op een enkele verzekeraar na, is de medisch adviseur aanwezig bij de uitvoering van de detailcontroles wanneer die ter plaatse van de zorgaanbieder plaats hebben. In geen enkel geval was het dan ook noodzakelijk dat een zorgaanbieder verzocht om de aanwezigheid van een medisch adviseur bij het onderzoek ter plaatse.

Thema 4 Communicatie van zorgverzekeraars over controles: Conclusies en aanbevelingen aan zorgverzekeraars
Bovenstaande bevindingen leiden tot de volgende aanbevelingen aan de zorgverzekeraars op dit onderdeel:

- Breng duidelijk onderscheid aan in de doelen van de controles: is de controle gericht op formele aspecten van de declaratie (bijvoorbeeld: valt de zorg onder het verzekerde pakket) of is deze gericht op de vraag of de zorg is geleverd en/of deze het meest was aangewezen?
- Hanteer, indien mogelijk, standaarden voor het opvragen van informatie. Borg daarin dat niet meer gegevens worden opgevraagd dan noodzakelijk.
- Wees open en aanspreekbaar richting zorgaanbieders bij de uitvoering van controles.
- Geef een toereikende toelichting op het opvragen van informatie in het kader van (detail-)controles, door aan te geven:
  - in welke fase van de controle de uitvraag zich bevindt;
  - welke methodes van onderzoek wordt ingezet en
  - hoe de privacy van de verzekerden is gewaarborgd.
- Leg uit – in aanvulling op de informatie in de polisvoorwaarden – op welke wijze de verzekeraar omgaat met medische persoonsgegevens bij de uitvoering van controles, in de vorm van een standaard toelichting bij het opvragen van informatie ter uitvoering van controles.
- Garandeer (en blijf garanderen) dat de medisch adviseur aanwezig is bij onderzoek ter plaatse in het kader van een detailcontrole.

De zorgverzekeraars hebben aangegeven dat zij deze aanbevelingen onderschrijven en daaraan uitvoering geven. In het bijzonder hebben verzekeraars duidelijk gemaakt dat zij belang hechten aan de aanspreekbaarheid op controles, door duidelijk te communiceren over de uitvoering van deze controles.

[38] Voor de volledigheid merken we op dat ook de Minister van VWS recentelijk aandacht heeft besteed aan dit onderwerp, zie Brief van de Minister aan de Tweede Kamer, "Privacywaarborgen materiële controle", kenmerk 913309-146902-Z (TK 2015-2016, 33980, nr. 10), 8 maart 2016, p. 2; Zie ook: TK 2015-2016, 33980, nr. 14.

6. Vervolg

Zoals genoemd onder hoofdstuk 4, heeft de NZa specifieke aanbevelingen gedaan aan de afzonderlijke verzekeraars met als doel, het beleid, de organisatie en communicatie over controles verder te versterken. Alle verzekeraars hebben aangegeven, de aanbevelingen te zullen opvolgen. Enkele zorgverzekeraars hebben reeds gedurende de consultatiefase van de bevindingen opvolging hebben gegeven aan de aanbevelingen, wat de NZa als positief waardeert.
Als gezegd heeft de NZa een enkele zorgverzekeraar een periodieke verantwoordingsplicht opgelegd over de wijze waarop hij toepassing geeft aan de privacyregeling en heeft de NZa een zorgverzekeraar opgedragen aan de NZa te rapporteren over ontwikkeling van zijn privacybeleid (welke rapportage inmiddels is afgerond).

De NZa zal daarnaast, in zijn algemeenheid, alert blijven op signalen over de wijze waarop zorgverzekeraars omgaan met persoonsgegevens. De NZa zal eventuele signalen onderzoeken (en zal daarover, indien nodig, in overleg treden met AP) en zal, als daartoe aanleiding bestaat, maatregelen treffen richting verzekeraars.

7. Bijlagen

Vragenlijst NZa aan zorgverzekeraars, 25 november 2015

Brief van de Minister aan de Tweede Kamer, "Privacywaarborgen materiële controle", kenmerk 913309-146902-Z (TK 2015-2016, 33980, nr. 10), 8 maart 2016 (https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z04985&did=2016D10208)